Gesellschaft für Informatik e.V. (GI)

publishes this series in order to make available to a broad public recent findings in informatics (i.e. computer science and information systems), to document conferences that are organized in cooperation with GI and to publish the annual GI Award dissertation.

Broken down into
- seminars
- proceedings
- dissertations
- thematics

current topics are dealt with from the vantage point of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure high quality contributions.

The volumes are published in German or English.

Information: http://www.gi.de/service/publikationen/lni/

ISBN 978-3-88579-417-2

This book presents outstanding dissertations in informatics of the year 2012. Every year, the German Gesellschaft für Informatik (GI), the Swiss Informatics Society (SI), the Austrian Computer Society (OCG) and the German Chapter of the ACM (GChACM) jointly give an award for an excellent dissertation that represents an important advance in informatics. The award winner is chosen in a careful selection procedure from candidates proposed by Austrian, Swiss and German universities, where each university may suggest at most one dissertation per year. The series "Ausgezeichnete Informatikdissertationen" presents these outstanding dissertations to the informatics community, as well as to the public in order to support knowledge transfer from universities to industry and society.
This volume is in German.

GI-Dissertationspreis 2012

13

GI-Edition

Lecture Notes in Informatics

Steffen Hölldobler et al. (Hrsg.)

Ausgezeichnete Informatikdissertationen 2012

Dissertations



Steffen Hölldobler et al. (Hrsg.)

Ausgezeichnete Informatikdissertationen 2012

Im Auftrag der GI herausgegeben durch die Mitglieder des Nominierungsausschusses

Abraham Bernstein, Universität Zürich
Wolfgang Effelsberg, Universität Mannheim
Steffen Hölldobler (Vorsitzender), Technische Universität Dresden
Hans-Peter Lenhof, Universität des Saarlandes
Klaus-Peter Löhr, Freie Universität Berlin
Paul Molitor, Martin-Luther-Universität Halle-Wittenberg
Gustaf Neumann, Wirtschaftsuniversität Wien
Rüdiger Reischuk, Universität zu Lübeck
Nicole Schweikardt, Goethe-Universität Frankfurt am Main
Myra Spiliopoulou, Otto-von Guericke-Universität Magdeburg
Harald Störrle, Technical University of Denmark
Sabine Süsstrunk, École Polytechnique Fédérale de Lausanne

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Dissertations
Series of the Gesellschaft für Informatik (GI), Volume D-13
ISBN 978-3-88579-417-2

Dissertations Editorial Board
Prof. Dr. Steffen Hölldobler (Chair), Technische Universität Dresden,
Fakultät für Informatik, Institut für Künstliche Intelligenz, 01062 Dresden

Abraham Bernstein, Universität Zürich
Wolfgang Effelsberg, Universität Mannheim
Steffen Hölldobler (Vorsitzender), Technische Universität Dresden
Hans-Peter Lenhof, Universität des Saarlandes
Klaus-Peter Löhr, Freie Universität Berlin
Paul Molitor, Martin-Luther-Universität Halle-Wittenberg
Gustaf Neumann, Wirtschaftsuniversität Wien
Rüdiger Reischuk, Universität zu Lübeck
Nicole Schweikardt, Goethe-Universität Frankfurt am Main
Myra Spiliopoulou, Otto-von Guericke-Universität Magdeburg
Harald Störrle, Technical University of Denmark
Sabine Süsstrunk, École Polytechnique Fédérale de Lausanne

Series Editorial Board
Heinrich C. Mayr, Alpen-Adria-Universität Klagenfurt, Austria
(Chairman, mayr@ifit.uni-klu.ac.at)
Dieter Fellner, Technische Universität Darmstadt, Germany
Ulrich Flegel, Hochschule für Technik, Stuttgart, Germany
Ulrich Frank, Universität Duisburg-Essen, Germany
Johann-Christoph Freytag, Humboldt-Universität zu Berlin, Germany
Michael Goedicke, Universität Duisburg-Essen, Germany
Ralf Hofestädt, Universität Bielefeld, Germany
Michael Koch, Universität der Bundeswehr München, Germany
Axel Lehmann, Universität der Bundeswehr München, Germany
Peter Sanders, Karlsruher Institut für Technologie (KIT), Germany
Sigrid Schubert, Universität Siegen, Germany
Ingo Timm, Universität Trier, Germany
Karin Vosseberg, Hochschule Bremerhaven, Germany
Maria Wimmer, Universität Koblenz-Landau, Germany

Dissertations
Steffen Hölldobler, Technische Universität Dresden, Germany
Seminars
Reinhard Wilhelm, Universität des Saarlandes, Germany
Thematics
Andreas Oberweis, Karlsruher Institut für Technologie (KIT), Germany

© Gesellschaft für Informatik, Bonn 2013
printed by Köllen Druck+Verlag GmbH, Bonn

Vorwort

Die Gesellschaft für Informatik e.V. (GI) vergibt gemeinsam mit der Schweizer Informatik Gesellschaft (SI), der Österreichischen Computergesellschaft (OCG) und dem German Chapter of the ACM (GChACM) jährlich einen Preis für eine hervorragende Dissertation im Bereich der Informatik. Hierzu zählen nicht nur Arbeiten, die einen Fortschritt in der Informatik bedeuten, sondern auch Arbeiten aus dem Bereich der Anwendungen in anderen Disziplinen und Arbeiten, die die Wechselwirkungen zwischen Informatik und Gesellschaft untersuchen. Die Auswahl dieser Dissertationen stützt sich auf die von den Universitäten und Hochschulen für diesen Preis vorgeschlagenen Dissertationen. Jede dieser Hochschulen kann jedes Jahr nur eine Dissertation vorschlagen. Somit sind die im Auswahlverfahren vorgeschlagenen Kandidatinnen und Kandidaten bereits „Preisträger" ihrer Hochschule.

Die 29 Einreichungen zum Dissertationspreis 2012 belegen die zunehmende Bedeutung und auch die Bekanntheit des Dissertationspreises. Wie jedes Jahr wurden die vorgeschlagenen Arbeiten im Rahmen eines Kolloquiums im Leibniz-Zentrum für Informatik Schloss Dagstuhl von den Nominierten vorgestellt. Für die Mitglieder des Nominierungsausschusses war das persönliche Zusammentreffen mit den Nominierten der Höhepunkt der Auswahlarbeit, und für die Nominierten hat das Kolloquium sicher eine Reihe neuer Erfahrungen und wissenschaftlicher Kontakte geboten. Das wissenschaftlich sehr hohe Niveau der Vorträge, die regen Diskussionen und die angenehme Atmosphäre in Schloss Dagstuhl wurde von allen Teilnehmerinnen und Teilnehmern des Kolloquiums sehr begrüßt.

Wie in jedem Jahr fiel es dem Nominierungsausschuss sehr schwer, eine einzige Dissertation auszuwählen, die durch den Preis besonders gewürdigt wird. Mit der Präsentation aller vorgeschlagenen Dissertationen in diesem Band wird die Ungerechtigkeit, eine aus mehreren ebenbürtigen Dissertationen hervorzuheben, etwas ausgeglichen. Dieser Band soll zudem einen Beitrag zum Wissenstransfer innerhalb der Informatik und von den Universitäten und Hochschulen in die Bereiche Technik, Wirtschaft und Gesellschaft leisten.

Die beteiligten Gesellschaften zeichnen Herrn Dr. sc. ethz. Robin A. Moser für seine hervorragende Dissertation „Exact Algorithms for Constraint Satisfaction Problems" mit dem Dissertationspreis 2012 aus.

Das Local Lemma ist ein starkes Kriterium für die Erfüllbarkeit aussagenlogischer Formeln, oder allgemeiner für die Erfüllbarkeit eines Systems von Einschränkungen. Herr Moser entwickelt erstmals für dieses Lemma einen effizienten konstruktiven Beweis, der sehr überraschend ist. Daneben gelingt es ihm, die lokale Suche bei k-SAT-Problemen mit einer verblüffenden Idee vollständig zu de-randomisieren.

Mit dieser Preisverleihung würdigen die beteiligten Gesellschaften – die Gesellschaft für Informatik e.V. (GI), die Schweizer Informatik Gesellschaft (SI), die Österreichische Computergesellschaft (OCG) und das German Chapter of the ACM (GChACM) – eine herausragende wissenschaftliche Arbeit, in der zwei, seit vielen Jahren offene Probleme mit neuen, bahnbrechenden Ideen elegant gelöst werden.

Ein besonderer Dank gilt dem Nominierungsausschuss, der sehr effizient und konstruktiv zusammengearbeitet hat. Bei Frau Julia Koppenhagen und Herrn Christoph Wernhard möchte ich mich für die Unterstützung bei der Entgegennahme der vorgeschlagenen Dissertationen, für die Organisation des Kolloquiums sowie für die Zusammenstellung und Anpassung der Beiträge an das Format der GI-Edition Lecture Notes in Informatik (LNI) bedanken. Für die finanzielle Unterstützung des Nominierungskolloquiums sei den beteiligten Gesellschaften gedankt. Die Gastfreundlichkeit und die hervorragende Bewirtung in Dagstuhl trugen zum Erfolg des Kolloquiums bei, wofür ich mich an dieser Stelle ebenfalls herzlich bedanke.

Steffen Hölldobler
Dresden im August 2013



Kandidaten für den GI-Dissertationspreis 2012

Dr. Bächle, Sebastian	Technische Universität Kaiserslautern
Dr.-Ing. Bartsch, Steffen	Universität Bremen
Dr. Baumeister, Dorothea	Heinrich-Heine-Universität Düsseldorf
Dr. Brill, Markus	Technische Universität München
Dr. Drews, Paul	Universität Hamburg
Dr. Dvořák, Wolfgang	Technische Universität Wien
Dr. Elberfeld, Michael	Universität zu Lübeck
Dr. Endrass, Birgit	Universität Augsburg
Dr. Fouz, Mahmoud	Universität des Saarlandes
Dr. Geister, Dagi	Leibniz Universität Hannover
Dr. Gieseke, Fabian	Carl von Ossietzky Universität Oldenburg
Dr.-Ing. Göthel, Thomas	Technische Universität Berlin
Dr. Gruber, Thiemo	Universität Kassel
Dr. Hecht, Fabio V.	Universität Zürich
Dr. Kennel, Bastian	Universität Mannheim
Dr. Keßelheim, Thomas	RWTH Aachen
Dr.-Ing. Klüppelholz, Sascha	Technische Universität Dresden
Dr.-Ing. Kober, Jens	Technische Universität Darmstadt
Dr. Kriege, Jan Sören	TU Dortmund, Fakultät für Informatik
Dr. Łabaj, Paweł P.	Universität für Bodenkultur Wien
Dr. Lochbihler, Andreas	Karlsruher Institut für Technologie (KIT)
Dr.-Ing. Lukas, Georg	Otto-von-Guericke-Universität Magdeburg
Dr. Moser, Robin A.	ETH Zürich
Dr.-Ing. Neumann, Christoph P.	Friedrich-Alexander-Universität Erlangen-Nürnberg
Dr. Reinecke, Philipp	Freie Universität Berlin
Dr. Solis Escalante, Teodoro	Technische Universität Graz
Dr. Tegeler, Florian	Georg-August-Universität Göttingen
Dr. Wild, Peter	Universität Salzburg
Dr. Wirth, Henry	Universität Leipzig

Mitglieder des Nominierungsausschusses für den GI-Dissertationspreis 2012



Von links nach rechts:

Prof. Dr.-Ing. Wolfgang Effelsberg	Universität Mannheim
Prof. Dr. Myra Spiliopoulou	Otto-von-Guericke-Universität Magdeburg
Prof. Dr.-Ing. Klaus-Peter Löhr	Freie Universität Berlin
Prof. Dr. Gustaf Neumann	Wirtschaftsuniversität Wien
Prof. Dr. Harald Störrle	Technical University of Denmark
Prof. Dr. Sabine Süsstrunk	École Polytechnique Fédérale de Lausanne
Prof. Dr. Hans-Peter Lenhof	Universität des Saarlandes
Prof. Dr. Steffen Hölldobler (Vorsitzender)	Technische Universität Dresden
Prof. Dr. Paul Molitor	Martin-Luther-Universität Halle-Wittenberg
Prof. Dr. Nicole Schweikardt	Goethe-Universität Frankfurt am Main
Prof. Dr. Abraham Bernstein	Universität Zürich

Nicht im Bild:

Prof. Dr. Rüdiger Reischuk (Fotograf)	Universität zu Lübeck

Inhaltsverzeichnis

Sebastian Bächle
Entkopplung von Kernelementen der Anfrageverarbeitung 11

Steffen Bartsch
Benutzbare Sicherheit für wirksame Berechtigungen in Organisationen 21

Dorothea Baumeister
Berechnungskomplexität von Problemen in der Computational Social Choice 31

Markus Brill
Mengenwertige Lösungskonzepte in Spieltheorie und Social-Choice-Theorie 41

Paul Drews
Branchenspezifische IT-Innovationssysteme: Von der Analyse zur Intervention – Am Beispiel des IT-Innovationssystems für Krankenhäuser in Deutschland 51

Wolfgang Dvořák
Computationale Aspekte der Abstrakten Argumentation 61

Michael Elberfeld
Platz- und Schaltkreiskomplexität von MSO-beschreibbaren Problemen auf baumartig zerlegbaren Strukturen 71

Birgit Endrass
Kulturelle Vielfalt für virtuelle Charaktere 81

Mahmoud Fouz
Randomisiertes Rumor Spreading auf Sozialen Netwerken und Vollständigen Graphen 91

Dagi Geister
Constraint Generierung für domänenspezifische Modellierungssprachen 101

Fabian Gieseke
Von überwachten zu unüberwachten Support-Vektor-Maschinen und Anwendungen in der Astronomie 111

Thomas Göthel
Maschinelle Verifikation von parametrisierten Echtzeitsystemen 121

Thiemo Gruber
Analyse von Zeitreihen unter Verwendung orthogonaler Polynome am Beispiel der Online-Motivsuche und ihrer Anwendungen 131

Fabio Hecht
LiveShift: Ein Ansatz für zeitversetzte P2P Multimedia-Übertragungen 141

Bastian Kennel
Ein Einheitliches Rahmenwerk für Multi-Level Modellierung 151

Thomas Keßelheim
Approximationsalgorithmen für Spektrumsallokation und Power Control in Funknetzwerken 161

Sascha Klüppelholz
Formale Verifikation von exogenen Koodinationsmodellen 171

Jens Kober
Lernen Motorischer Fähigkeiten: Von Algorithmen zu Roboter-Experimenten ... 181

Jan Kriege
Modellierung korrelierter Eingabedaten für Simulationen 191

Paweł P. Łabaj
Messungen und Datenanalyse in Anbetracht von Rauschen und komplexem Bias – Fortschritte aus verbesserten bioinformatischen Algorithmen 201

Andreas Lochbihler
Ein maschinengeprüftes, typsicheres Modell der Nebenläufigkeit in Java: Sprachdefinition, virtuelle Maschine, Speichermodell und verifizierter Compiler . 211

Georg Lukas
Fehlertolerante Industrielle Wireless-Mesh-Network-Infrastruktur 221

Robin A. Moser
Exakte Algorithmen für Erfüllbarkeitsprobleme 231

Christoph P. Neumann
Verteiltes Dokumenten-orientiertes Prozessmanagement im Gesundheitswesen .. 241

Philipp Reinecke
Effiziente Systemevaluation mit stochastischen Modellen 251

Teodoro Solis Escalante
Der Asynchrone Graz Brain Switch 261

Florian Tegeler
Schadsoftwareerkennung auf Netzwerkebene ohne Einzelpaketanalyse 271

Peter Wild
Irisbiometrie in der Überwachung: Innovationen zu Segmentierung und Komparatoren 281

Henry Wirth
Analyse molekularbiologischer Daten mittels Self-organizing Maps 291

Entkopplung von Kernelementen der Anfrageverarbeitung*

Sebastian Bächle
Databases and Information Systems Group
University of Kaiserslautern, Germany
baechle@cs.uni-kl.de

Abstract: Diese Arbeit befasst sich mit der Konzeption, Optimierung und Realisierung einer erweiterbaren deklarativen Anfragesprache zur effizienten Verarbeitung strukturierter und semi-strukturierter Daten. Zur Vereinfachung von Optimierungs- und Übersetzungsprozessen strebt sie eine strikte Trennung von logischen mengenorientierten Konzepten und physischen Aspekten an. Die für diese Trennung sorgfältig abgestimmte Compiler-Architektur kann daher als effiziente Basis für die Implementierung, Erweiterung und Portierung von Anfragesystemen für unterschiedliche Sprachen, Datenmodelle und Systemarchitekturen herangezogen werden. Desweiteren wird ein neuartiges, auf das Operatorkonzept der Sprache abgestimmtes Ausführungsmodell vorgestellt, mit dem Anfragen zur Laufzeit automatisch parallelisiert werden können.

1 Übersicht

Die Bedeutung deklarativer Anfragesprachen als effiziente und produktivitätssteigernde Abstraktion für die Verarbeitung großer Datenmengen nimmt stetig zu. Die mit ihnen erzielte Entkopplung von der physischen Datenrepräsentation ermöglicht es, komplexe Zugriffs- und Verarbeitungsroutinen isoliert von der Anwendung selbst zu optimieren und auszuführen. Die aktuelle Tendenz zur immer tiefgreifenderen Erweiterung und Spezialisierung von Systemen für neue Anwendungsgebiete und deren Datenmodelle wirkt allerdings wie eine Zentrifugalkraft auf diese bislang von klassischen Unternehmens- und Geschäftsanwendungen dominierte Disziplin. Getrieben durch die zusätzlichen Anforderungen schnell wachsender Datenmengen, neuer Hardware und der Forderung nach unmittelbarer Verfügbarkeit, werden immer mehr Systeme, Sprachen und APIs für spezielle Anwendungsszenarien zugeschnitten. Ohne das relationale Modell und SQL als gegebene Kernelemente müssen jedoch bewährte Konzepte und Algorithmen immer wieder aufwändig adaptiert, portiert und implementiert werden.

Gegenstand dieser Arbeit ist die Zusammenfassung der in [Bä12] entwickelten Konzeption und Realisierung einer abstrakten Verarbeitungsprache für strukturierte und semistrukturierte Daten. Diese deklarative Sprache vereint in sich die zentralen Strategien und Techniken aus dem Bereich der Anfrageoptimierung und -auswertung. Sie kann deshalb als solide Basis für die Realisierung neuer Anfragesprachen dienen. Der Vorteil dieses

*Englischer Titel der Dissertation: “Separating Key Concerns in Query Processing”

Ansatzes besteht in der Möglichkeit, die für ein konkretes Anwendungsszenario zugeschnittenen Abstraktionen für Daten und Operationen auf Standardkonzepte abzubilden, zu optimieren und letztendlich effizient auf der konkreten Zielplattform umzusetzen.

Um den vielfältigen Herausforderungen eine Datenverarbeitungsprache auf logischer und physischer Ebene Rechnung tragen zu können, ist es wichtig, deren Komplexität durch eine klare Trennung von Kernzielen beherrschbar zu machen. Am Ausgangspunkt steht daher die Besinnung auf ihre vier Kernaufgaben: das *Filtern*, *Transformieren*, *Kombinieren* und *Aggregieren* von großen Datenmengen. Im Fokus der Betrachtungen liegen hierbei drei zentrale Herausforderungen: die Optimierung mengenorientierter Aspekte, die effiziente Ausnutzung plattformspezifischer Gegebenheiten und eine parallele Verarbeitung.

Anfragen oder Skripte bestehen üblicherweise aus Kombinationen mengenorientierter Operationen, die in einen möglichst effizienten Ausführungsplan übersetzt werden sollen. Art und Reihenfolge der einzelnen Verarbeitungsschritte sind dabei häufig die kritischsten Aspekte, wobei gängige Optimierungen in erster Linie unabhängig von der konkreten Ausprägung der Daten sind. Beim Transformieren und Filtern von Daten ist es beispielsweise sinnnvoll, den Filterschritt als erstes durchzuführen. Konzeptionell spielt es dabei jedoch keine Rolle, ob die Daten als Tabellen homogen-strukturierter Tupel oder Kollektionen semi-strukturierter Dokumente vorliegen. Physische Aspekte, beispielsweise der effiziente Zugriff auf die einzelnen Felder eines Tupels oder das Auswerten von Pfadmustern auf hierarchischen Strukturen, können isoliert davon betrachtet und für die jeweilige Plattform optimiert werden. Die effiziente Parallelisierung einer Anfrage zur gezielten Ausnutzung moderner Mehrkern-Architekturen stellt schließlich eine besondere Herausforderung dar, da neben logischen auch physische Aspekte wie Scheduling und Datenlokalität beachtet werden müssen.

Das Ergebnis dieser Arbeit ist die in Abbildung 1 schematisch dargestellte Compiler-Architektur. Sie ermöglicht es, unterschiedlichste Frontend-Sprachen auf einheitliche Konzepte abzubilden, diese auf rein logischer und konkreter physischer Ebene zu optimieren und schließlich auf unterschiedlichen Speicherungsarchitekturen auszuwerten. Die Laufzeitumgebung baut dazu auf einem Wrapper-Ansatz auf, der zur Effizienzsteigerung teilweise oder vollständig durch native Operationen ergänzt werden kann.

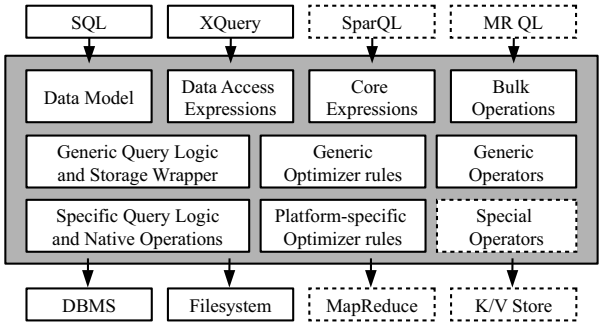


Abbildung 1: Schematischer Aufbau der Compiler Architektur.

2 Anatomie der Anfragesprache

Die konzipierte Anfragesprache besteht aus vier Kernelementen: einem abstrakten Modell zur Repräsentation von Daten, Operationen zum Erzeugen, Komponieren und Dekomponieren von Daten, elementaren Grundoperationen für Arithmetik, String-Manipulationen, Verzweigungen etc. sowie einer Menge von Operatoren zur Modellierung mengenorientierter Verarbeitungskonzepte.

2.1 Datenmodell

Anfragesprachen betrachten Datenbestände üblicherweise als Sammlung von mehr oder weniger homogenen, flach oder hierarchisch aufgebauten Datenelementen. Für einen portablen Übersetzungsprozess müssen unterschiedliche Datenmodelle aber auf einheitliche Strukturen zurückgeführt werden. Zur Abbildung der Datenarten und -strukturen verschiedenster Frontend-Sprachen auf eine abstrakte, einheitliche Ebene genügt bereits das in Abbildung 2 gezeigte minimalistische Grundmodell. Benötigt werden lediglich einige primitive Datentypen zur Repräsentation von Zahlen, Zeichenketten etc. sowie die zwei Kompositionstypen *Array* und *Map*. Ein Array ist eine geordnete Liste von Werten; eine Map ist eine geordnete Menge von Schlüssel-Wert-Paaren. Optional können zu diesem Grundmodell auch noch Funktoren hinzugenommen werden, was die Realisierung von mächtigeren Sprachen wie das in dieser Arbeit als Beispiel verwendete XQuery 3.0 ermöglicht.

Kompositionstypen können beliebig geschachtelt werden, um konkrete Datenstrukturen nachzubilden. Aus Effizienzgründen besitzen Werte jedoch keine Identität, was impliziert, dass Kompositionen strikt hierarchisch aufgebaut sind und auch keine direkten Verweise zwischen einzelnen Datenelementen möglich sind. Höherwertige, für Anwendungen benötigte Konzepte wie Identität, Beziehungen, Typen, Schemata und sonstige Invarianten werden durch verschiedene Mechanismen der jeweiligen Frontend-Sprache selbst realisiert. Ähnliches gilt auch für die andere Richtung. Wenn für Anfragen oder Datenmodelle bestimmte Aspekte des Grundmodells wie beispielsweise die Ordnung von Map-Werten keine Rolle spielen, kann deren Einhaltung aus Effizienzgründen ignoriert werden.

Wie in Abbildung 2 gezeigt, können relationale Daten recht einfach abgebildet werden. Ein Tupel entspricht einem Map-Wert, der Spaltennamen auf Werte abbildet. Tabellen sind Arrays von homogenen Tupeln. Auch das wesentlich komplexere Datenmodell von XQuery lässt sich auf ähnlich intuitive Weise auf Map- und Array-Werte zurückführen. Die Abbildung solcher Datenmodelle erfolgt jedoch teilweise über mehrere Kompositionsstufen, die zusätzlich bestimmten Invarianten unterliegen.

2.2 Datenzugriffe und Anfragelogik

Den Zugriff und das Erzeugen von Daten übernehmen dedizierte Konstruktoren und Zugriffsoperationen. Durch diese werden die jeweiligen Invarianten eines Datenmodells si-

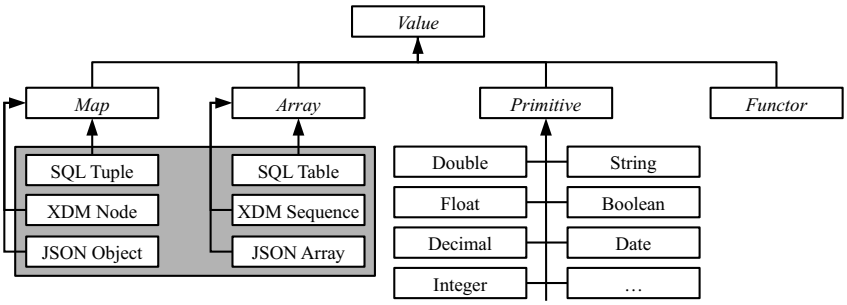


Abbildung 2: Aufbau des elementaren Datenmodells

chergestellt. Die Kapselung von logischen und letztlich auch physischen Datenoperationen in Form eigenständiger Ausdrücke erlaubt es, das Abstraktionsniveau und die Granularität der Frontend-Sprache direkt und sehr effizient auf die Fähigkeiten des Speicherungssystems abzubilden. In XQuery, zum Beispiel, kann eine Zugriffsoperation wie der Pfadschritt `./a//b/c` entweder direkt in Navigationsschritte im XML-Baum oder in eine noch effizientere Scan-Operation übersetzt werden, ohne dabei die konzeptionelle Sicht auf XML-Knoten als Kompositionen aus Map- und Array-Werten einnehmen zu müssen.

Die anderen Sprachbausteine bilden das Komplement zu Konstruktoren und Zugriffsoperationen, um sinnvoll Anfragen formulieren zu können. Sie implementieren Standardkonzepte wie Arithmetik, Boolesche Logik oder Funktionsaufrufe. Sie sind ebenfalls als Ausdrücke gekapselt und können daher bei Bedarf an sprach- oder systemspezifische Eigenschaften angepasst werden, ohne den Übersetzungsprozess an sich zu beeinflussen.

2.3 Operatoren

Mengenwertige Operationen werden als Funktionen über 2-dimensionale Arrays modelliert. Das macht es leichter, sie mit bewährten Verarbeitungskonzepten und Algorithmen relationaler Systeme umzusetzen. Jede dieser Funktionen, die aufgrund ihrer besonderen Rolle *Operatoren* genannt werden, akzeptiert ein 2-dimensionales Array als Eingaberelation und liefert als Ergebnis wieder ein 2-dimensionales Array. Operatoren lassen sich dadurch zu effizienten Verarbeitungspipelines komponieren. Tabelle 1 zeigt eine Auswahl der wichtigsten Operatoren. Beispiele zu einigen davon finden sich in Abbildung 3.

Operatoren werden in drei Gruppen unterschieden. Die Operatoren der ersten Gruppe verarbeiten die Tupel der Eingaberelation einzeln nacheinander. Der wichtigste Operator dieser Kategorie ist `ForEach`. Seine Funktionsweise entspricht einer klassischen *map*-Funktion mit Nested-Loops-Semantik. Die für jedes Eingabetupel ausgewertete Argumentfunktion *bind* liefert als Ergebnis selbst wieder eine Relation, deren Tupel im Verbund mit dem zugehörigen Eingabetupel zur Ausgaberelation hinzugefügt werden. `ForEach` ermöglicht so das Einspeisen von Daten in eine Pipeline und eignet sich unter ande-

Operator	Parameter		Rückgabetyp
`ForEach`	`in`	`[[T]]`	`[[T,S]]`
	`bind`	`[T]→[[S]]`	
`Project`	`in`	`[[T]]`	`[[S]]`
	`proj`	`[T]→[S]`	
`Select`	`in`	`[[T]]`	`[[T]]`
	`pred`	`[T]→bool`	
`OrderBy`	`in`	`[[T]]`	`[[T]]`
	`cmp`	`[T]×[T]→bool`	
`GroupBy`	`in`	`[[T]]`	`[[S]]`
	`grp`	`[T]→int`	
	`agg`	`[[T]]→[S]`	
`Count`	`in`	`[[T]]`	`[[T,int]]`
`Join / LeftJoin`	`in`	`[[T]]`	`[[T,S,R]]`
	`left`	`[T]→[[T,S]]`	
	`right`	`[T]→[[T,R]]`	
	`pred`	`[T,S]×[T,R]→bool`	

Tabelle 1: Auswahl der unterstützten Operatoren.

rem als Abstraktion für Scan-Operationen. Die Operatoren `Project` und `Select` sind äquivalent zu den entsprechenden Operationen im relationalen Fall.

Die zweite Gruppe von Operatoren verarbeitet Eingaberelationen als Ganzes. Zu ihr gehören die bekannten Sortier- und Agreggationsoperatoren `OrderBy` und `GroupBy` sowie der Operator `Count`, der die Tupel der Eingaberelation durchnummeriert.

Die Operatoren der dritten Gruppe kombinieren mehrere Relationen zu einer Ausgaberelation. Als Vertreter dieser Gruppe sind in Tabelle 1 die beiden Verbundoperationen `Join` und `LeftJoin` aufgeführt. Weitere Beispiele sind `Union` und `Intersect`. Wie alle Operatoren akzeptieren auch sie nur eine Eingaberelation. Die eigentliche Kombinationsoperation erfolgt nämlich für die zwei Relationen, die von den zwei Argumentfunktionen `left` und `right` für jedes Eingabetupel ausgegeben werden. Die Ausgabe des Operators selbst besteht aus der Konkatenation aller Teilergebnisse. Diese Funktionsweise stellt eine Verallgemeinerung entsprechender relationaler Operationen dar, wobei deren Algorithmen dennoch für die Realisierung herangezogen werden können. Der Grund für diese andere Struktur ergibt sich im Folgenden aus der Diskussion des Optimierungprozesses.

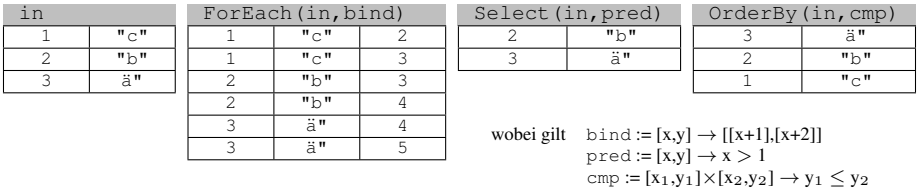


Abbildung 3: Beispiele für die Operatoren `ForEach`, `Select` und `OrderBy`.

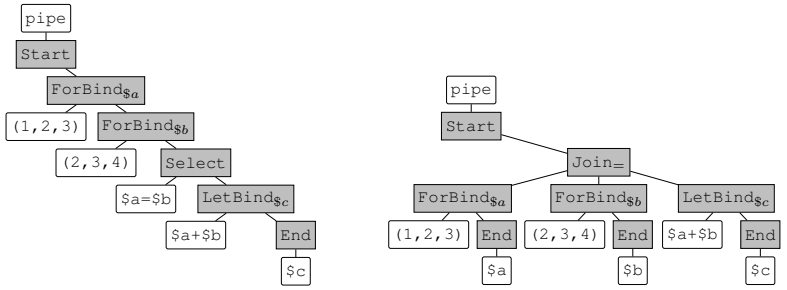
Um das Komponieren von Operatoren zu erleichtern und Hilfsfunktionen mit fixen Referenzen auf Tupel-Positionen wie in Abbildung 3 zu umgehen, werden die Spalten mit Hilfe von λ-Abstraktion wie in relationalen Umgebungen über explizite Spaltennamen

adressierbar gemacht. Abhängigkeiten zwischen Operatoren lassen sich so leichter erkennen, was insbesondere bei der Optimierung von Pipelines von Vorteil ist.

3 Übersetzung und Optimierung

Im Gegensatz zu traditionellen Ansätzen, die Anfragesprachen auf einer Algebra aufbauen, wird die Semantik einer Anfrage und damit auch der Suchraum für den Optimierer alleine über funktionale Konzepte definiert. Jede Anfrage wird durch einen Ausdrucksbaum repräsentiert, dessen Terme rekursiv ausgewertet werden. Da funktionale Werte stets unveränderlich sind und Anfragen im allgemeinen Fall ohnehin frei von Seiteneffekten sind, kann die Auswertung *eager* oder *lazy* erfolgen und beliebig parallelisiert werden. Abbildung 4(a) illustriert den prinzipiellen Aufbau einer Anfrage am Beispiel der einfachen XQuery-Anfrage:

```
for $a in (1,2,3)
return for $b in (2,3,4)
       where $a=$b
       let $c:= $a+$b
       return $c
```



(a) Einfache Pipeline.

(b) Pipeline mit Join-Operator.

Abbildung 4: Repräsentation und Optimierung eines XQuery-FLWOR-Ausdrucks.

Zur Übersetzungszeit wird diese Anfrage als `pipe`-Ausdruck dargestellt, der bei der Auswertung den aktuellen Kontext, in diesem Beispiel das leere Tupel `[]`, über den künstlichen Operator `Start` in die Pipeline einbringt. Die Variablenbindungen der beiden geschachtelten `for`-Schleifen werden in der Pipeline über Varianten des `ForEach`-Operators realisiert. Die beiden `ForBind`-Operatoren erzeugen für jedes Eingabetupel das Kartesische Produkt mit den Elementen ihrer jeweiligen Binding-Sequenz. Der `Select`-Operator filtert den so erzeugten Tupelstrom für das Prädikat `$a=$b`. Der `LetBind`-Operator bindet die Summe `$a+$b` schließlich als zusätzliche Variable `$c`. Der künstliche Operator `End` bildet das Ergebnis der Anfrage, in dem er die Teilergebnisse aller "Iterationen" zur Sequenz `(4,6)` konkateniert, die als Ergebnis des `pipe`-Ausdrucks zurückgeliefert wird. Die Ausgaben der einzelnen Operatoren sind Abbildung 5 nochmals dargestellt.

Die Auswertung eines Ausdrucks kann alleine von eventuell vorhandenen Variablenreferenzen abhängen. Diese bilden die Verknüpfung zwischen mengenorientierten Operatoren und Ausdrücken. Ein Ausdruck wird jeweils für eine bestimmte Variablenbelegung, den bereits erwähnten Kontext, ausgewertet. Dieser wird wiederum durch die von Operatoren produzierten und konsumierten Tupel repräsentiert, womit ein Pipeline-Tupel vergleichbar ist zu einem *stack frame* in einer prozeduralen Sprache.

Im Unterschied zu traditionellen Ansätzen, die Anfragen in *bottom-up*-Darstellung verarbeiten, werden Anfragen, wie gezeigt, in *top-down*-Form verwaltet. Die Operatoren werden dazu im *continuation-passing style* [SJ75] definiert, so dass der Datenfluss innerhalb einer Pipeline von oben nach unten verläuft. Diese Modellierung vereinfacht den Optimierungs- und Übersetzungsprozess erheblich, da sich die Sichtbarkeit von Variablen ganz natürlich mit der hierarchischen Struktur der Anfrage deckt.

ForBind$_{\$a}$
$a
1
2
3

ForBind$_{\$b}$	
$a	$b
1	2
1	3
...	...
3	4

Select	
$a	$b
2	2
3	3

LetBind$_{\$c}$		
$a	$b	$c
2	2	4
3	3	6

End			
$a	$b	$c	
2	2	4	4
3	3	6	6

Abbildung 5: Ausgaberelationen der Operatoren aus Abbildung 4(a).

3.1 Anfrageoptimierung

Die am Beispiel gezeigte Abbildung auf die interne Repräsentation ist einfach auf gängige Anfragekonstrukte verschiedenster Frontend-Sprachen übertragbar: mengenorientierte Passagen werden auf Operatoren abgebildet; die verbleibenden sprach- und modellspezifischen Artefakte werden in Ausdrücken gekapselt. Je besser es gelingt, große Bestandteile einer Anfrage zu einer Pipeline zusammenzufassen, desto effektiver sind Optimierungen.

Die natürliche Trennung von mengenorientierten und physischen Aspekten im Ausdrucksbaum erleichtert die Analyse und Optimierung von Datenflüssen. Hierbei werden die gleichen Ziele verfolgt wie im relationalen Fall. Filter sollten möglichst früh in der Pipeline ausgewertet werden, um die Anzahl der zu verarbeitenden Tupel schnell zu verringern. Für die durch `ForEach` häufig auftretenden Kartesischen Produkte gilt es, diese nach Möglichkeit wie in Abbildung 4(b) durch effizientere Join-Operatoren zu ersetzen.

Die formalen Grundlagen solcher Optimierungen sind in algebraischen Ansätzen direkt ersichtlich. Zur Herleitung entsprechender Transformationsregeln für das funktional aufgebaute Operatorenmodell kann man stattdessen auf Monaden zurückgreifen. Diese bilden ein auf den sogenannten Monadischen Gesetzen aufbauendes, formales Typkonstrukt und werden primär in funktionalen Programmiersprachen verwendet, um "nicht-funktionale" Aspekte wie sequentielle Abläufe, Indeterminismus oder Seiteneffekte zu modellieren. Die Möglichkeit, sie auch zur Spezifikation von Anfragen und Transformationsregeln zu verwenden, wurde bereits vor über 20 Jahren erkannt [JW07].

Da sich Operatoren auf Monadische Konstrukte zurückführen lassen, ist es möglich, über diese formal korrekte Transformationen für Operatorkompositionen herzuleiten [Gru99]. Monaden dienen somit als einer Algebra ebenbürtiges theoretisches Fundament, über das ein Großteil etablierter Optimierungstechniken, etwa für Joins oder Aggregate, als generische Pipeline-Optimierungen im Compiler verankert werden können.

Das Optimieren auf physischer Ebene wird durch die Kapselung von Datenzugriffen in dedizierten Ausdrücken vereinfacht. Im Normalfall erfolgen die Zugriffe über eine Wrapper-Architektur. Im Falle einer naïven Übersetzung von XQuery bedeutet das, dass über eine Schnittstelle auf den einzelnen XML-Knoten navigiert wird, ohne zu wissen, ob es sich dabei um im Hauptspeicher gehaltende Baumstrukturen oder serialisierte Instanzen auf dem Externspeicher handelt. Der Spielraum für Optimierungen ist entsprechend groß. Durch die Vereinfachung von Zugriffssequenzen zu gröberen Operationsgranulaten oder durch die Gruppierung von Zugriffen kann der relative Overhead pro Zugriff deutlich reduziert werden. Durch das Umgehen aufwändiger Speziallogik für Standardfälle können zudem die durchschnittlichen Kosten pro Zugriff reduziert werden. Desweiteren arbeiten alternative Zugriffswege, wie zum Beispiel Indexe, in vielen Situationen wesentlich effizienter. Direkte Zugriffe auf die Speicherungsstrukturen und andere Optimierungen können auf vielfältige Weise realisiert werden. Das Spektrum reicht von spezialisierten Ausdruckstypen, die native Erweiterungen von Wrappern nutzen oder die Wrapper-Schicht vollständig umgehen, bis hin zu umfangreichen Transformationen von korrelierten Zugriffen innerhalb einer Pipeline.

4 Parallele Verarbeitung

Der Datenfluss in einer Pipeline ähnelt stark dem Funktionsprinzip geschachtelter Schleifen. Wie in Abbildung 6 gezeigt, entspricht die Ausgabereihenfolge der tupelweise arbeitenden Operatoren der ersten Gruppe der Abfolge der Variablenbelegungen in geschachtelten Schleifen. Die Operatoren der zweiten Gruppe, die *pipeline blocker*, führen die aus den einzelnen Schleifendurchläufen resultierenden Ergebnisse wieder zusammen.

Die Iterationen jeder Schleife sind unabhängig voneinander. Da also keine Datenabhängigkeiten zwischen ihnen bestehen, können große Teile einer Anfrage durch die horizontale und vertikale Aufteilung der einzelnen Schleifendurchläufe in pipeline- und datenparallele Operationen aufgeteilt werden. Da sich die parallelisierbare Baumstruktur jedoch erst zur Laufzeit entwickelt und die Bestimmung einer effizienten Aufteilung a priori äußerst schwierig ist, kommt ein neuartiges Operatormodell zum Einsatz, welches diese Aufteilung dynamisch zur Laufzeit vornimmt. Das Modell basiert auf dem *fork/join*-Verfahren, einer sehr effektiven, nach dem divide-and-conquer-Prinzip arbeitenden Parallelisierungstechnik [Lea00]. Die Idee besteht darin, eine große Eingabe solange rekursiv in zwei unabhängige Teile aufzuspalten (“fork”), bis diese klein genug sind, um effizient seriell verarbeitet zu werden. Die während der Aufteilungsphase erzeugten Teile, die nicht direkt weiterverarbeitet werden, können zwischenzeitlich von freien Prozessen parallel verarbeitet werden, bis der initiierende Prozess zurückkehrt (“join”). Durch die Verwendung eines leichtgewichtigen Schedulers [SLS06] lässt sich so ein hoher Parallelitätsgrad erzielen.

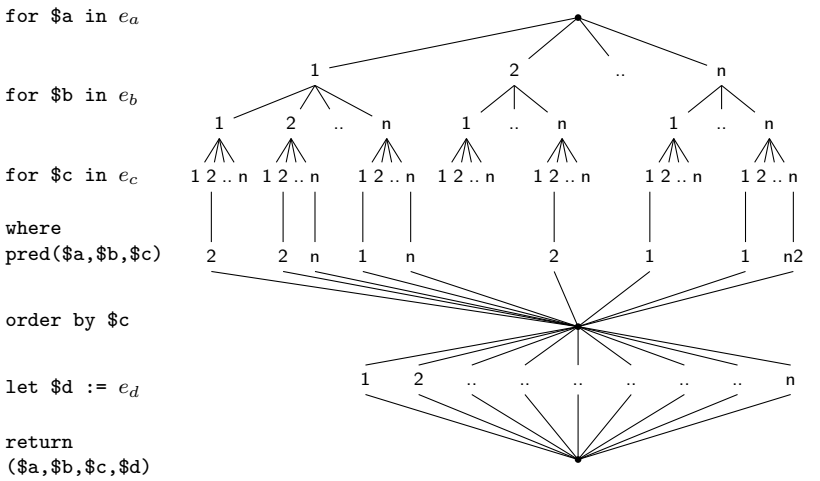
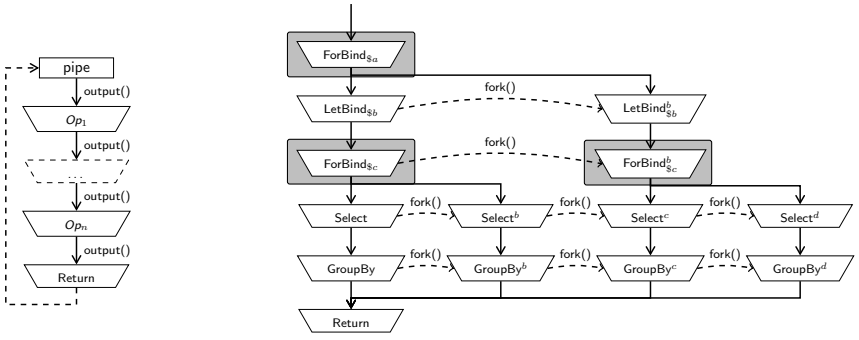


Abbildung 6: Iterationen eines XQuery-FLWOR-Ausdrucks.

Um dieses Prinzip in einer Pipeline anwenden zu können, müssen die Operatoren wie in Abbildung 7(a) *push*-basiert arbeiten. Das bedeutet, dass Operatoren im Gegensatz zum sonst üblichen *pull*-basierten Prinzip [Gra94], ihre Ergebnisse aktiv an den jeweils nachfolgenden Operator weiterreichen. Wenn ein `ForEach`-basierter Operator nun für ein Eingabetupel eine sehr große Binding-Sequenz verarbeiten muss, kann diese nach dem fork/join-Prinzip aufgeteilt und parallel verarbeitet werden. Damit die entstehenden Partitionen aber wirklich unabhängig voneinander verarbeitet werden können, muss der fork-Schritt auch auf Operatorebene erfolgen. So entwickelt sich die initial lineare Pipeline dynamisch zu einem Operatorgraphen wie in Abbildung 7(b). Der nächste blockierende Operator in der Pipeline führt die parallelen Pfade am Ende wieder zusammen.



(a) Lineare Pipeline. (b) Dynamischer Operatorgraph.

Abbildung 7: Push-basiertes Operatormodell mit Fork-Mechanismus.

5 Zusammenfassung

In diesem Rundgang wurden die tragenden Säulen der in [Bä12] entwickelten Konzepte und Techniken vorgestellt. Die abstrakte Anfragesprache setzt sich aus vier Bausteinen zusammen, mit denen man komplexe Datenmodelle auf die einheitlichen Kompositionstypen Map und Array zurückführen kann. Mengenorientierte und physische Aspekte werden getrennt voneinander modelliert, um sie einfacher und effektiver optimieren zu können. Transformationsregeln können dabei auf Monaden als zugrunde liegendes formales Konstrukt zurückgreifen. Für die dynamische Parallelisierung von Anfragen wurde ein push-basiertes Operatordesign entwickelt, das effiziente Partitionierungstechniken und Scheduling-Mechanismen aus dem HPC-Bereich für Datenverarbeitungsalgorithmen zugänglich macht. Eine empirische Evaluation der hier vorgestellten Aspekte findet sich ebenfalls in [Bä12] .

Literatur

[Bä12] Sebastian Bächle. *Separating Key Concerns in Query Processing – Set Orientation, Physical Data Independence, and Parallelism*. Dr. Hut Verlag, München, December 2012.

[Gra94] Goetz Graefe. Volcano: An Extensible and Parallel Query Evaluation System. *IEEE Trans. on Knowl. and Data Eng.*, 6(1):120–135, Februar 1994.

[Gru99] Torsten Grust. Comprehending Queries. Bericht, 1999.

[JW07] Simon Peyton Jones und Philip Wadler. Comprehensive Comprehensions. In *Proc. SIGPLAN Workshop on Haskell*, Seiten 61–72, 2007.

[Lea00] Doug Lea. A Java Fork/Join Framework. In *Proceedings ACM Java Grande*, Seiten 36–43, 2000.

[SJ75] Gerald Jay Sussman und Guy L Steele Jr. Scheme: An Interpreter for Extended Lambda Calculus. In *MEMO 349, MIT AI LAB*, 1975.

[SLS06] William N. Scherer, III, Doug Lea und Michael L. Scott. Scalable Synchronous Queues. In *Proc. PPoPP*, Seiten 147–156, 2006.



Sebastian Bächle wurde am 11. November 1981 in Zweibrücken geboren. Nach dem Abitur 2001 trat er im Oktober 2002 ein Studium der Angewandten Informatik an der TU Kaiserslautern an. Im Anschluss an die abgeschlossene Diplomprüfung im September 2007 begann er seine Forschungsarbeit als wissenschaftlicher Mitarbeiter an der TU in der Arbeitsgruppe *Datenbanken und Informationssysteme* unter der Leitung von Prof. Dr.-Ing. Dr. h. c. Härder. Im Dezember 2012 schloss er dort seine Promotion über Anfrageverarbeitung für strukturierte und semi-strukturierte Daten ab. Seit Oktober 2012 arbeitet er bei der SAP AG in Walldorf.

Benutzbare Sicherheit für wirksame Berechtigungen in Organisationen*

Steffen Bartsch

CASED, TU Darmstadt
steffen.bartsch@cased.de

Abstract: Berechtigungen in Informationssystemen können die tägliche Arbeit behindern. Um ungewollte Behinderungen und daraus resultierende Sicherheitsprobleme zu minimieren, betrachtet diese Dissertation nicht nur die technischen Aspekte dieser Probleme. Stattdessen wurde umfassend aus verschiedenen Perspektiven analysiert, welche Ursachen und Konsequenzen diese Probleme in Organisationen haben. Es wurden dabei verschiedenste Probleme, von der unerlaubten Weitergabe von Passwörtern bis zur Unbenutzbarkeit der Verwaltungswerkzeuge, identifiziert. Um diese Probleme fundamental zu beheben, wurden acht Prinzipien für benutzbare Berechtigungen vorgeschlagen und anhand von fünf konkreten Artefakten, wie etwa flexiblen Berechtigungen, evaluiert. Insbesondere die Einbindung der verschiedenen Betroffenen, die Kombination von technischen mit nicht-technischen Maßnahmen und die präzise Anpassung auf die jeweilige Umgebung erweisen sich als wirksame Ansätze.

1 Ineffizienz und fehlende Sicherheit durch Berechtigungen

Berechtigungen und Restriktionen in Informationssystemen – Autorisierung – sind Eckpfeiler der Informationssicherheit und wurden und werden daher intensiv in Forschung und Praxis entwickelt. Umso mehr überrascht, dass – trotz der anzunehmenden technischen Reife von Berechtigungssystemen – weiterhin regelmäßig Probleme mit Berechtigungen auftreten. Häufig stören Berechtigungen die Arbeitsabläufe in Organisationen; beispielsweise, wenn eine Aufgabe wegen fehlender Berechtigungen nicht *effizient* bearbeitet werden kann. Probleme werden aber nicht nur durch restriktive Berechtigungen verursacht, sondern auch durch zu weitgehende, zum Beispiel, wenn Berechtigungen nach einem Positionswechsel zugewiesen bleiben. In diesem Fall ist die *Effektivität* der Sicherheitsmaßnahme beeinträchtigt, denn die Berechtigungen bietet nicht den erwarteten Schutz. Die Effektivität wird ebenfalls beeinträchtigt, wenn übermäßig restriktive Berechtigungen die Anwender dazu verleiten, die Autorisierung für ihre Aufgaben zu umgehen und beispielsweise ihre Passwörter weiterzugeben.

Diese Probleme betreffen vorrangig die Organisation selbst und die Anwender. Bei genauerer Betrachtung können aber weitere Personen innerhalb von Organisationen iden-

*Vollständiger Titel der Dissertation: "Broadening the Scope of Security Usability from the Individual to the Organizational: Participation and Interaction for Effective, Efficient, and Agile Authorization" [Bar12a]

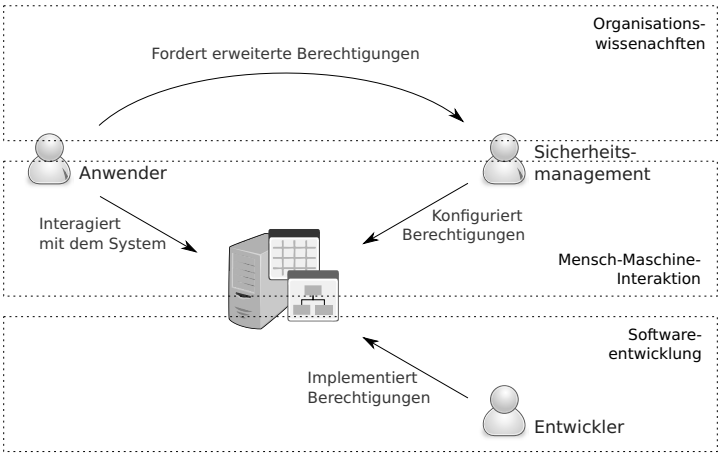


Abbildung 1: Perspektiven auf Berechtigungen und relevante Forschungsdisziplinen

tifiziert werden, die ebenfalls Probleme mit Berechtigungen haben, allerdings aus anderen Perspektiven (siehe Abbildung 1): etwa in der Verwaltung der Berechtigungen („Sicherheitsmanagement“). Beispielsweise müssen sich Anwender in vielen Organisationen an Verantwortliche wenden, wenn sie zusätzliche Berechtigungen benötigen. Als drittes müssen auch Entwickler mit einbezogen werden, denn diese implementieren die möglichen Beschränkungen erst in der Anwendung. Wenn diese Abläufe, Interaktionen und Aktivitäten im sozio-organisatorischen und -technischen Berechtigungssystem nicht harmonieren, werden Berechtigungen ihr Ziel, Sicherheit zu schaffen, wenn überhaupt, nur in Form einer übermäßigen Hürde erreichen. Die Produktivität der Organisation sinkt und Sicherheitsrisiken entstehen. *Rein technisch oder mit selektivem Blick auf eine einzelne Perspektive lassen sich die Probleme nicht bewältigen.* Abbildung 1 benennt einige der Disziplinen, die betrachtet werden müssen: Organisationswissenschaften, die Mensch-Maschine-Interaktion und die Softwareentwicklung.

Bisherige Arbeiten zu Berechtigungen bleiben dabei zumeist auf einer technischen Ebene, wie Siponen und Oinas-Kukkonen schreiben [SOK07]. Erst Zurko et al. [ZSS99] untersuchten die Benutzbarkeit von Berechtigungskonfigurationen und Brostoff et al. [BSC+05] wie verständlich die verwendeten Konzepte wie Rollen sind. Erst spät folgten einige – im Vergleich zur technischen Literatur zu Berechtigungen – wenige Studien zu den Praxisproblemen beim Setzen von Berechtigungen [WSC06, BCR+09, SG09]. Wie im vorhergehenden Absatz gesehen, greift allerdings eine selektive Betrachtung des Setzens von Berechtigungen zu kurz und übersieht etwa Probleme für den Anwender und die Auswirkungen für die Organisation. Damit bleibt dann für Entscheider unklar, warum sie diese Probleme angehen sollen.

Das Ziel der Dissertation [Bar12a] ist es deshalb, umfassende Lösungsansätze für die Probleme mit Berechtigungen in Organisationen zu entwickeln – also sich insbesondere nicht auf einzelne Perspektiven auf Berechtigungen zu beschränken. Dazu werden die Probleme systematisch und umfassend analysiert sowie die Bezüge zwischen den verschiede-

nen Perspektiven und deren Problemen hergestellt. Darauf aufbauend werden Ansätze zur grundsätzlichen Behebung der Probleme als acht Prinzipien entwickelt und anhand von fünf Artefakten evaluiert. Insbesondere die Einbindung der verschiedenen Betroffenen, die Kombination von technischen mit nicht-technischen Maßnahmen und die präzise Anpassung auf die jeweilige Umgebung erweisen sich als wirksame Ansätze.

2 Ganzheitliches Modell der Berechtigungsprobleme

Um die Probleme mit Berechtigungen umfassend zu erheben, wurden sie in einer großen qualitativen Studie – basierend auf Interviews mit 118 Mitarbeitern aus vielfältigen Umgebungen eines Großunternehmens – mittels des Grounded-Theory-Ansatzes [GS67] systematisch untersucht. Außerdem wurden die kausalen Zusammenhänge zwischen den Problemen identifiziert und mit den Organisationszielen in Bezug gesetzt. So zeigt sich etwa, dass Passwörter unter Mitarbeitern weitergegeben werden, weil die Prozesse für die Anforderung von Berechtigungen zum Teil zu lange („Monate“) dauern, aber die Arbeit erledigt werden muss. Aus diesen Ergebnissen in Verbindung mit den Problemen aus der Literatur ließ sich ein umfassendes Modell der Probleme und deren Abhängigkeiten entwickeln, basierend auf den verschiedenen Perspektiven von Benutzern auf Berechtigungen [BS13].

Zuoberst im Modell (dargestellt in Abbildung 2) befindet sich die Perspektive der *Entwickler*, die etwa das Berechtigungsmodell (also auch die möglichen Arten von Berechtigungen) und die Werkzeuge zum Setzen von Berechtigungen entwickeln. Diese Ebene beeinflusst unter anderem die nächsttiefer liegende Ebene der *Entscheidungen* zur Vergabe von Berechtigungen, die etwa, je nach Modell, feingranularer ausfallen können. Wie diese Entscheidungen erfolgen, gibt unter anderem den Rahmen für die *Prozesse* vor, denen Berechtigungsänderungen von der Beantragung bis zur Umsetzung folgen. Probleme sowohl mit Entscheidungen als auch mit den Prozessen können wiederum Auswirkungen auf die nächsttiefere Ebene der *Berechtigungen* selbst haben – beispielsweise, wenn Entscheidungen ohne ausreichendes Wissen gefällt werden oder Berechtigungen sich durch langlaufende Prozesse verzögern (wie im oberen Beispiel aus der Studie). Die Berechtigungen selbst beeinflussen dann die *primären Aufgaben der Anwender*; etwa wenn jeweils notwendige Berechtigungen fehlen. Letztlich haben Probleme in all diesen Ebenen Auswirkungen auf die *Ziele der Organisation*, also auf ihre Produktivität und die Wirksamkeit der Sicherheit.

Darüber hinaus konnte in der Studie anhand der Berechtigungssysteme in verschiedenen eingesetzten Systemen in dem Unternehmen gezeigt werden, dass das Auftreten der verschiedenen Typen von Problemen entscheidend von der Ausgestaltung des Berechtigungssystems abhängt. So traten Probleme mit den Prozessen zur Vergabe von Berechtigungen eher in Berechtigungssystemen mit zentralisierten und formalisierten Prozessen auf. Probleme mit Entscheidungen traten dagegen eher in Berechtigungssystemen mit dezentralen Strukturen auf. Daraus lässt sich schließen, dass die Probleme durch die richtige Gestaltung des Berechtigungssystem mit allen zugehörigen Komponenten (u.a. Werkzeugen, Prozessen und Entscheidungsstrukturen) adressiert werden können.

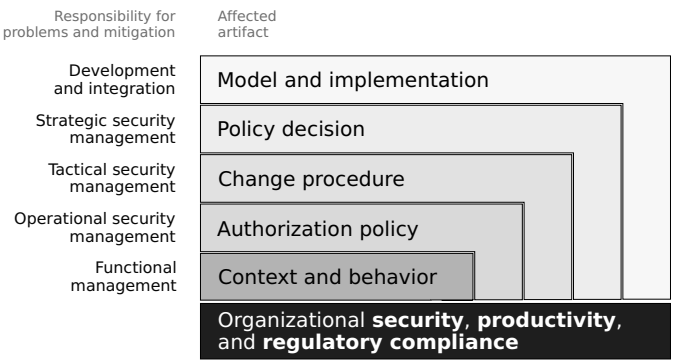


Abbildung 2: Empirisch identifizierte Ebenen der Berechtigungsprobleme

3 Acht Prinzipien für benutzbare Autorisierung

Für das Ziel, Ansätze zur Behebung der Probleme und zur Gestaltung von benutzbaren Berechtigungssystemen zu entwickeln, wurden acht Prinzipien für benutzbare Autorisierung entwickelt. Sie basieren auf etablierten und innovativen Forschungsansätzen aus der benutzbaren Sicherheit sowie praktischen Ansätzen aus der sicheren Agilen Software-Entwicklung:

Partizipation fördern Die Partizipation der verschiedenen Perspektiven und deren Austausch untereinander sollen gefördert, also etwa der betroffene Anwender stärker in die Entscheidungen einbezogen werden. Dadurch sollen dann zum Beispiel fehlende Berechtigungen aufgrund von fehlenden Informationen über deren Notwendigkeit beim Entscheider verhindert werden (vgl. Koordinierungsprozesse [Pal09]).

Belastung für den Einzelnen verringern Insbesondere wird dazu die Belastung für den Einzelnen verringert, also beispielsweise die Belastung, die ein Entscheider beim Ändern von Berechtigungen empfindet (vgl. [ZSS99]). Dadurch müssen unter anderem weniger Änderungen an Spezialisten, wie Administratoren, ausgelagert werden, was Missverständnisse vermeidet.

Interaktion konkretisieren Für eine leichtere Verständlichkeit wird angestrebt, das Abstrakte in den Benutzungsschnittstellen zu konkretisieren, so dass zum Beispiel von konkreten Anwendern und konkreten Berechtigungen und nicht von abstrakten Rollen gesprochen wird (vgl. [BCG08]).

Interdisziplinarität fördern Es sollen explizit Ansätze aus verschiedenen Disziplinen integriert werden, beispielsweise soziologische und organisatorische Herangehensweisen als Ergänzung der momentan vorherrschenden technischen.

Menschliches Verhalten einbeziehen Das menschliche Verhalten entsprechend der sozialen Umgebung soll berücksichtigt werden, also etwa, wann der Missbrauch einer Berechtigung zu erwarten ist (z.B. basierend auf Insider-Angreifer-Modellen

[Sch02]). Daraus kann dann etwa abgeleitet werden, ob Einschränkungen überhaupt notwendig sind.

Sicherheitsbewusstsein und Sicherheitsexpertise fördern Generell soll das Sicherheitsbewusstsein und die Sicherheitsexpertise gefördert werden [Bar11c], damit beispielsweise die Verwaltung von Berechtigungen näher zur eigentlichen Arbeit verlagert und zum Beispiel direkt im Team erledigt werden kann.

Auf Dynamik ausrichten Organisationen verändern sich. Um besser dieser Realität zu entsprechen, wird die Autorisierung als Maßnahme explizit auf Dynamik ausgerichtet. Wenn gar nicht davon ausgegangen wird, dass Berechtigungen statisch sind, sollten diese auch eher mit den realen Aufgaben und Bedürfnissen Schritt halten.

Auf die Umgebung anpassen Die Maßnahme soll generell eine Angemessenheit entsprechend der Umgebung in Bezug auf Prozesse (z.B. Formalität und Zentralisation der Organisation [Min89]) und Werkzeuge (notwendige Flexibilität, vorhandene Expertise) anstreben.

4 Entwicklung und Evaluierung von exemplarischen Lösungen

Die Autorisierungsprinzipien wurden evaluiert, indem fünf konkrete Artefakte entwickelt und jeweils empirisch evaluiert wurden. Die Artefakte zielen auf die Behebung verschiedener identifizierter Autorisierungsprobleme ab und sind so gewählt, dass sie jeweils primär eine der fünf Ebenen des Problemmodells abdecken.

4.1 Flexible Berechtigungen

Eines der entwickelten und evaluierten Artefakte betrifft die Ebene der Störungen im Arbeitsablauf der Anwender, die hier für Ausnahmesituationen adressiert werden. Die dahinterstehende Beobachtung ist, dass Berechtigungen häufig durch Weitergabe des Passwortes umgangen werden, um in Ausnahmesituationen kurzfristig wichtige Aufgaben zu erledigen, für die die Mitarbeiter im Normalfall nicht autorisiert sind. In Abbildung 3 sind diese Bedürfnisse gestrichelt dargestellt. Um Probleme in diesen Situationen zu vermeiden, werden flexible Berechtigungen umgesetzt, die es dem Anwender erlauben, kontrolliert die eigenen Berechtigungen temporär auszuweiten („Policy Override“). In Abbildung 3 sind diese Beschränkungen, die im Ausnahmemodus überschritten werden können, als „Soft Boundary“ eingezeichnet. Im Rahmen einer Fallstudie in einem mittelgroßen Unternehmen konnte die Machbarkeit des Ansatzes gezeigt sowie Faktoren für den Erfolg eines solchen Ansatzes identifiziert werden [Bar12b]. Insbesondere ist es wichtig, dass die flexiblen Berechtigungen in geeignete Prozesse eingebunden werden, damit reagiert werden kann, wenn der Ausnahmefall zur Regel wird.

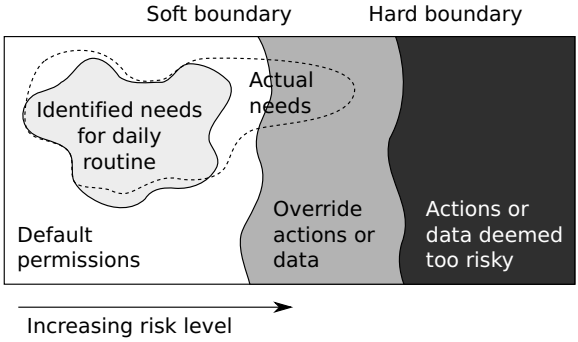


Abbildung 3: Schematische Darstellung normaler und Ausnahmeberechtigungen

4.2 Unterstützung für Berechtigungsänderungen

Ein weiteres Artefakt bietet eine Unterstützung für das Bearbeiten von komplexen Berechtigungen. Insbesondere bei rollenbasierten Berechtigungen kann es für Nicht-Experten schwierig sein, die technischen Änderungen an den Berechtigungen zu formulieren. Eine Änderungsunterstützung schlägt daher auf Basis von konkreten Änderungszielen (z.B. „Person A benötigt Berechtigung X, aber B soll sie nicht erhalten“) mögliche technische Änderungen vor. Dabei wurde ein effizienter KI-Algorithmus sowie eine Benutzerschnittstelle (dargestellt in Abbildung 4) implementiert [BSB09]. Auch hier zeigten sich in einer empirischen Evaluation mit Entscheidern und Administratoren aus verschiedenen organisatorischen Umgebungen die Vorteile des Ansatzes. Unter anderem berichteten Administratoren von einem erhöhten Sicherheitsgefühl beim Ändern von Berechtigungen, keine Fehler zu begehen. Darüber hinaus wurde in dieser Verwaltungsart eine verbesserte Basis für die Diskussion der Änderungsmöglichkeiten gesehen.

4.3 Entscheidungsunterstützung

Die Studie zu Problemen mit Berechtigungen zeigte auch, dass Entscheider mitunter überfordert sind, wenn sie entscheiden müssen, ob eine Person eine bestimmte Berechtigung bekommen sollte. Um diese Entscheidung zu unterstützen, wurde eine Entscheidungsunterstützung entwickelt, die Informationen zur Notwendigkeit von Berechtigungen und zu den potentiellen Risiken durch die Vergabe der Berechtigungen einbezieht [BS12]. Dazu werden verschiedene Betroffene – wie der Anwender und sein Vorgesetzter – in den Entscheidungsprozess einbezogen. Die Evaluation eines Prototypen des Werkzeugs (siehe Abbildung 5) mit Anwendern und Entscheidern aus unterschiedlichen Organisationen zeigte, dass ein solches Werkzeug zwar nicht in allen Umgebungen angemessen ist, aber einige Betroffene stark davon profitieren würden.

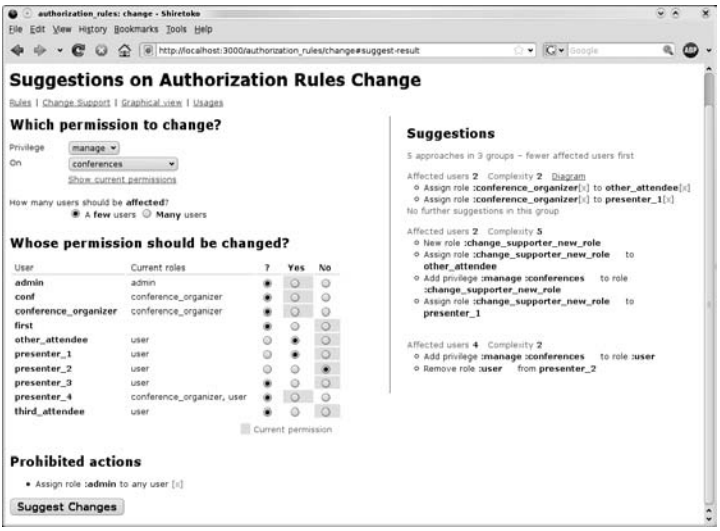


Abbildung 4: Benutzerschnittstelle für die Änderungsunterstützung

4.4 Angemessene Abläufe und Prozesse

Probleme mit Berechtigungen entstehen auch, wenn Anwendungen fortentwickelt werden, ohne bestehende oder durch neue Funktionen notwendige Berechtigungen zu beachten. Dann können Anwendern nach einem Update die benötigten Berechtigungen fehlen. Um diese Probleme anzugehen, wurde auf Basis der Literatur das integrative Prozessmodell INDUSE entwickelt, dass den Austausch zwischen Berechtigungsvergabe- und Entwicklungsprozessen explizit macht [Bar11b]. Dieses Modell wurde anhand von Interviews mit Entscheidern und Entwicklern in verschiedenen Umgebungen evaluiert. Dadurch konnten eine Reihe von informellen Prozessen und daraus resultierenden Probleme identifiziert werden.

4.5 Integration von Beschränkungen in Anwendungen

Die Probleme mit Berechtigungen, die ihren Ursprung in der Anwendungsentwicklung haben, hängen häufig mit fehlerhaftem Quelltext zur Durchsetzung der Berechtigungen zusammen – also etwa, wenn Berechtigungsabfragen fehlen. Je aufwendiger es ist, Durchsetzungen (z.B. Berechtigungsabfragen) in eine Anwendung zu integrieren und zu ändern, je wahrscheinlicher ist es, dass hieraus Probleme entstehen. Im Rahmen der Dissertation wurde daher eine Erweiterung für das Web-Entwicklungs-Frameworks *Ruby on Rails* entwickelt (*declarative_authorization*), deren Ansatz es ist, diese Aufwände zu minimieren [BSB09]. Die Open-Source-Erweiterung war zwischenzeitlich die beliebteste Ruby-on-Rails-Erweiterung für Berechtigungen. Um die Effekte der Erweiterung zu untersuchen,



	A	B	D	G
1	**Berechtigungsprofil**	Eigenschaften der Daten und Systeme		
2				
3	System	Auf welches System bezieht sich die Berechtigung?	[redacted]	
4	Datentyp	Welche Daten betreffen die Berechtigungen?	[redacted]	
5	Aktivität	Welche Aktivität wird erlaubt?	**Lesen**	z.B. Lesen, Ändern, Konfigurieren
6				
10				
11	**Datensensibilität**			
12	Personenbezogene Daten	Sind personenbezogene Daten von den Berechtigungen betroffen?	N	Y: Yes, N: No
13	Mitarbeiterdaten	Mitarbeiterdaten?	N	Y: Yes, N: No
14	Sensible Daten	sensible personenbezogene Daten?	N	Y: Yes, N: No
16	Kommerzielle Sensibilität	Betreffen die Daten z.B. Verträge, das Risiko-Management oder externe Dritte?	Y	Y: Yes, N: No
17				
18	**Schäden**	(z.B. durch ungewollte Veröffentlichung, Änderungen		
19		Stellen Sie sich vor, die Daten würden ungewollt veröffentlicht. Was wären die Konsequenzen für das Unternehmen?		1: vernachlässigbar, 2: gering, 3: merkbar, 4: kritisch, 5: katastrophal
21	Unternehmen	Wie schwer wären die Konsequenzen...		
22	Öffentlichkeitsarbeit	... für die Öffentlichkeitsarbeit des Unternehmens?	3	1 – 5
23	Kommerzielle Schäden	... für die kommerziellen Interessen oder die Produktivität?	4	1 – 5
25	Rechtliche Konsequenzen	... aus vertraglichen oder gesetzlichen Verpflichtungen?	3	1 – 5
27	Persönliche Konsequenzen	Wie schwer wären die persönlichen Konsequenzen für den Verantwortlichen in Form von...		
28	(Straf-)Rechtlich	... rechtlichen oder strafrechtlichen Ansprüchen?	1	1 – 5
29	Karriere, Arbeitsplatzsicherheit	... Effekten auf die Karriere oder den Arbeitsplatz?	2	1 – 5
30				
31	**Bedrohungen**	für die Daten oder das System		
37	Vorsätzliche Bedrohungen	Wie wahrscheinlich ist es, dass einer der folgenden Akteure Interesse an der unerlaubten Veröffentlichung von Daten hat?		1: unwahrscheinlich, 2: entfernt, 3: gelegentlich, 4: möglich, 5: häufig
38	durch Konkurrenten	(z.B. um Kunden abzuwerben)	2	1 – 5
39	durch Lieferanten	(z.B. um höhere Preise zu erzielen oder Konkurrenten auszustechen)	1	1 – 5
40	durch Medien	(z.B. um eine interessante Geschichte zu veröffentlichen)	3	1 – 5
41	von eigenen Mitarbeitern	(z.B. um die Daten zu verkaufen oder weiterzugeben)	4	1 – 5
43	Unbeabsichtigte Bedrohungen			
		Wie wahrscheinlich ist es, dass Daten unbeabsichtigt veröffentlicht		

Anfragender - Verwendung | Vorgesetzter - Zustimmung | Verantwortlicher - Rollenprofil | **Verantwortlicher - Berechtigungsprofil** | Verantwo

Abbildung 5: Prototyp der Entscheidungsunterstützung

wurde es in der Entwicklung einer realen Web-Anwendung für die Geschäftsprozesse eines mittelgroßen Unternehmens eingesetzt. In einer empirischen Auswertung des Entwicklungsverlaufs [Bar11a] ließ sich zeigen, dass die Entwickler tatsächlich Aufwände gespart hatten.

5 Leitlinien für effektive und effiziente Informationssicherheit

Das Anwenden der acht Prinzipien in den praktischen Artefakten und die damit verbundenen empirischen Evaluationen zeigen, dass die Prinzipien helfen, Autorisierung benutzbarer zu gestalten. Insbesondere die Partizipation aller Betroffenen an Entscheidungen zu Berechtigungen und die Kombination aus technischen Mechanismen zur Durchsetzung von Berechtigungen und nicht-technischen Maßnahmen (z.B. flexible Berechtigungen) verringern Produktivitätsverluste und Frustration. Weiterhin muss für alle Entscheidungen der Gestaltung der technischen und nicht-technischen Aspekte der Autorisierung die jeweilige Umgebung einbezogen werden. Genauso wie eine rein technische Lösung für die Berechtigungen nur in Ausnahmefällen zu optimalen Ergebnissen führt, gibt es bei der Vielzahl von sehr unterschiedlichen Kontexten von Autorisierung (vom Unternehmensumfeld über Berechtigungen für Nachrichten auf sozialen Netzwerken bis zu solchen für Anwendungen auf Smartphones) keine Standardlösung. Die Prinzipien bieten eine Leitlinie für die Entwicklung von angemessenen Berechtigungssystemen.

Die Lösungsansätze lassen sich auf weitere Gebiete der Informationssicherheit übertragen. Wie bei der Vergabe von Berechtigungen mangelt es auch hier häufig an dem notwendigen Wissen zu Risiken von bestimmten Entscheidungen (etwa: ob die Sicherheitswarnung des Web-Browsers ignoriert werden kann). Nicht zuletzt liegt es daran, dass die Kommunikation zwischen den sehr verschiedenen Gedankenmodellen von Entwicklern, Anwendern und Sicherheitsexperten fehlschlägt und damit z.B. Warnungen unverständlich und un-

verstanden bleiben. Die integrativen Methodik dieser Dissertation, also der Einbeziehung der verschiedenen Perspektiven von Betroffenen und der Multidisziplinarität, bietet einen vielversprechenden Ansatz für Forschung und Praxis, den genannten Herausforderungen zu begegnen: Durch das *Unterstützen einer „informierten Partizipation"* – also der Einbindung von Betroffenen in Entscheidungen [BDH93] – und durch die *Förderung der Interaktion zwischen den Betroffenen*. Dieser Ansatz bedeutet letztlich die Ausdehnung der Sichtweise vom Blick auf das Individuum in der benutzbaren Sicherheit (Wie kann der Einzelne mit dem Sicherheitsmechanismus umgehen?) auf das gesamte sozio-organisatorische Umfeld (Wie passt der Mechanismus in die realen Interaktionen und Abläufe im Umfeld? Wie können die Betroffenen eingebunden werden?). Der Ansatz erfordert allerdings auch eine noch größere Offenheit der Forschung für die Multidisziplinarität, um die Probleme mit der effektiven Sicherheit in Informationssystemen umfassend zu lösen und gleichzeitig ihre gesellschaftliche Akzeptanz zu fördern.

Literatur

[Bar11a] Steffen Bartsch. An Authorization Enforcement Usability Case Study. In *ESSoS 2011*. Springer, 2011.

[Bar11b] Steffen Bartsch. Exploring Twisted Paths: Analyzing Authorization Processes in Organizations. In *NSS '11: Proceedings of the 5th International Conference on Network and System Security*. IEEE Computer Society, 2011.

[Bar11c] Steffen Bartsch. Practitioners' Perspectives on Security in Agile Development. In *FARES '11: 6th International Workshop on Frontiers in Availability, Reliability and Security*. IEEE Computer Society, 2011.

[Bar12a] Steffen Bartsch. *Broadening the Scope of Security Usability from the Individual to the Organizational: Participation and Interaction for Effective, Efficient, and Agile Authorization*. Dissertation, Universität Bremen, 2012.

[Bar12b] Steffen Bartsch. Policy Override in Practice: Model, Evaluation, and Decision Support. *Security and Communication Networks*, 2012. In print.

[BCG08] Alan F. Blackwell, Luke Church und Thomas Green. The Abstract is 'an Enemy': Alternative Perspectives to Computational Thinking. *PPIG*, 2008.

[BCR+09] Lujo Bauer, Lorrie Faith Cranor, Robert W. Reeder, Michael K. Reiter und Kami Vaniea. Real life challenges in access-control management. In *CHI '09: Proceedings of the 27th international conference on Human factors in computing systems*, Seiten 899–908, New York, NY, USA, 2009. ACM.

[BDH93] John Seely Brown, Paul Duguid und Susan Haviland. Towards informed participation: Six scenarios in search of democracy in the electronic age. In *The Promise and Perils of Emerging Information Technologies*. The Aspen Institute, Queenstown, Maryland, USA, 1993.

[BS12] Steffen Bartsch und M. Angela Sasse. Guiding Decisions on Authorization Policies: A Participatory Approach to Decision Support. In *SAC '12: 27th ACM Symposium On Applied Computing*. ACM, 2012.

[BS13] Steffen Bartsch und M. Angela Sasse. How Users Bypass Access Control – and Why: The Impact of Authorization Problems on Individuals and the Organization. In *Proceedings for the 21st European Conference on Information Systems (ECIS 2013)*. AIS eLibrary, 2013. Accepted.

[BSB09] Steffen Bartsch, Karsten Sohr und Carsten Bormann. Supporting Agile Development of Authorization Rules for SME Applications. In *TrustCol '08: 3rd International Workshop on Trusted Collaboration*, Seiten 461–471, Berlin Heidelberg, 2009. Springer.

[BSC+05] Sacha Brostoff, Martina Angela Sasse, David W. Chadwick, James Cunningham, Uche M. Mbanaso und Sassa Otenko. 'R-What?' Development of a role-based access control policy-writing tool for e-Scientists. *Softw., Pract. Exper.*, 35(9):835–856, 2005.

[GS67] Barney G. Glaser und Anselm L. Strauss. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Transaction, 1967.

[Min89] Henry Mintzberg. *Mintzberg on management: inside our strange world of organizations*. Free Press, New York, NY, USA, 1989.

[Pal09] Frank Pallas. *Information Security Inside Organizations – A Positive Model and Some Normative Arguments Based on New Institutional Economics*. Dissertation, TU Berlin, 2009.

[Sch02] E. Eugene Schultz. A framework for understanding and predicting insider attacks. *Computers & Security*, 21(6):526–531, 2002.

[SG09] Diana K. Smetters und Nathan Good. How users use access control. In *SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security*, Seiten 1–12, New York, NY, USA, 2009. ACM.

[SOK07] Mikko T. Siponen und Harri Oinas-Kukkonen. A review of information security issues and respective research contributions. *SIGMIS Database*, 38:60–80, February 2007.

[WSC06] Tara Whalen, Diana K. Smetters und Elizabeth F. Churchill. User experiences with sharing and access control. In *CHI '06 extended abstracts on Human factors in computing systems*, Seiten 1517–1522, New York, NY, USA, 2006. ACM.

[ZSS99] Mary Ellen Zurko, Rich Simon und Tom Sanfilippo. A User-Centered, Modular Authorization Service Built on an RBAC Foundation. In *S&P '99: Proceedings of the 1999 IEEE Symposium on Security and Privacy*, Los Alamitos, CA, USA, 1999. IEEE Computer Society.



Steffen Bartsch wurde von der Universität Bremen im Juni 2012 mit einer Dissertation zum Thema benutzbare Sicherheit in organisatorischen Umgebungen promoviert. Seit Februar 2012 ist er Mitglied der Arbeitsgruppe SecUSo – Security, Usability and Society im CASED an der TU Darmstadt. Hier beschäftigt er sich mit der Unterstützung von sicherheitsrelevanten Entscheidungen, unter anderem durch die Verbesserung der Kommunikation zwischen den Verantwortlichen und Betroffenen. Zuvor forschte Steffen Bartsch seit Erhalt des Informatik-Diploms von der Universität Bremen 2007 im Technologie-Zentrum Informatik (TZI) der Universität Bremen.

Berechnungskomplexität von Problemen in der Computational Social Choice*

Dorothea Baumeister
Institut für Informatik
Heinrich-Heine Universität Düsseldorf
40225 Düsseldorf, Deutschland
baumeister@cs.uni-duesseldorf.de

Abstract: Diese Arbeit untersucht die Berechnungskomplexität von verschiedenen Problemen aus drei Bereichen der *Computational Social Choice*. Der erste Bereich beschäftigt sich mit Wahlen und speziell dem Problem, zu bestimmen, ob ein ausgewählter Kandidat in einer Wahl mit unvollständiger Information ein Gewinner sein kann. Im zweiten Bereich, der im weiteren Sinne mit dem Problem der Gewinnerbestimmung verwandt ist, wird die Berechnungskomplexität von Problemen bezüglich *minimal upward* und *minimal downward covering sets* untersucht. Der letzte Bereich ist die gemeinsame Urteilsfindung. Hier wird nicht die Komplexität einer Art von „Gewinnerproblem" untersucht, sondern die dreier Formen von Beeinflussung, nämlich Manipulation, Bestechung und Kontrolle.

1 Einleitung

Computational Social Choice ist ein sich rasant entwickelndes Gebiet an der Schnittstelle von Social-Choice-Theorie und Informatik, mit einem bidirektionalen Wissenstransfer zwischen beiden Disziplinen. Die Social-Choice-Theorie liefert die theoretischen Grundlagen zur kollektiven Entscheidungsfindung, mit der wir auch häufig in alltäglichen Situationen konfrontiert werden. Betrachten wir zum Beispiel eine kontroverse Elfmeterentscheidung in einem Fußballspiel. Nach den Regeln ist klar, dass es bei einem Foul im Strafraum einen Elfmeter geben muss. Der erste Schiedsrichter sagt, dass es ein Foul im Strafraum war und es somit einen Elfmeter geben muss, aber die anderen beiden Schiedsrichter verweigern den Elfmeter. Der zweite Schiedsrichter sagt, dass das, was er im Strafraum gesehen hat, eine Schwalbe war, und der Dritte behauptet, dass es ein Foul außerhalb des Strafraums war. Diese individuellen Beurteilungen und die Auswertung anhand der Mehrheitsregel sind in Tabelle 1 dargestellt. Das gemeinsame Urteil, dass es ein Foul im Strafraum war, es jedoch keinen Elfmeter gibt ist allerdings nicht regelkonform.

*Englischer Titel der Dissertation: "Computational Complexity in Three Areas of Computational Social Choice: Possible Winners, Unidirectional Covering Sets, and Judgment Aggregation" [Bau12].

Tabelle 1: Schiedsrichterurteile einer Elfmeterentscheidung

	Strafraum	Foul	Elfmeter
Schiedsrichter 1	Ja	Ja	Ja
Schiedsrichter 2	Ja	Nein	Nein
Schiedsrichter 3	Nein	Ja	Nein
Mehrheitsentscheid	Ja	Ja	Nein

Ein wichtiges Resultat in der Social-Choice-Theorie ist, dass das Ergebnis einer solchen gemeinsamen Urteilsfindung inkonsistent sein kann, auch wenn alle zugrunde liegenden individuellen Urteile konsistent sind. Diese Tatsache wird auch *doctrinal Paradox* oder *diskursives Dilemma* genannt (siehe Kornhauser und Sager [KS86] für die ursprüngliche Formulierung und Pettit [Pet01] für eine Generalisierung).

Im Gebiet der Computational Social Choice werden nun einerseits Methoden aus der Informatik angewendet, um die Mechanismen der Social-Choice-Theorie zu untersuchen, andererseits werden aber auch die in der Social-Choice-Theorie entstandenen Konzepte in Informatiktechnologien eingesetzt. Die Methoden der Social-Choice-Theorie haben ihren Ursprung zumeist in politischen Wahlen, aber wie man an der Elfmeterentscheidung sieht, sind diese Entscheidungsfindungsprozesse sehr vielfältig. Unter anderem werden sie bei der Aggregation von Resultaten unterschiedlicher Suchmaschinen, bei der Interaktion von autonomen Agenten in Multi-Agenten-Systemen oder bei der Aufteilung von Internetbandbreite verwendet. Bei Szenarien von diesem Größenumfang ist eine formale mathematische Spezifikation und Analyse besonders wichtig und stellt uns vor neue Herausforderungen. Zum Beispiel bekommt betrügerisches Verhalten eine ganz andere Bedeutung. Hier kann eine hohe Berechnungskomplexität einen gewissen Schutz vor unerwünschter Einflussnahme auf Entscheidungsfindungsprozesse bieten. Neben Problemen, die im Zusammenhang mit Wahlen und Präferenzaggregation stehen, werden in der Computational Social Choice auch Probleme der gerechten Aufteilung (*fair division*), der gemeinsamen Urteilsfindung (*judgment aggregation*), der Ressourcenaufteilung in Multi-Agenten-Systemen, der algorithmischen Spieltheorie und aus vielen weiteren Bereichen untersucht. Weiterführende Informationen zu diesem Bereich bieten das Buch von Rothe et al. [RBLR11] und das Buchkapitel von Brandt et al. [BCE12]. In dieser Arbeit liegt der Schwerpunkt auf der Untersuchung der Berechnungskomplexität von Wahlproblemen, Lösungskonzepten in Dominanzgraphen und Problemen der gemeinsamen Urteilsfindung.

2 Mögliche Gewinner

Ein großer Bereich in der Computational Social Choice ist der Untersuchung verschiedener Eigenschaften von Wahlsystemen gewidmet. Eine Wahl ist gegeben

durch eine Menge von Kandidaten und eine Liste von Wählern, deren Präferenzen über die Kandidaten durch ihre Stimmen repräsentiert werden. Häufig sind die Stimmen komplette Rangfolgen (also vollständige lineare Ordnungen) der Kandidaten; es gibt aber auch andere Darstellungen. Ein Wahlsystem ist eine Vorschrift, wie aus den gegebenen Stimmen ein oder mehrere Sieger der Wahl bestimmt werden. Eine wichtige Klasse von Wahlsystemen bilden die sogenannten Scoring-Protokolle, die über einen Scoring-Vektor definiert werden. Dessen Einträge geben an, wie viele Punkte ein Kandidat für eine bestimmte Position in einer Wählerstimme bekommt. Die bekannte Pluralitätswahl wird durch den Scoring-Vektor $(1, 0, \ldots, 0)$ dargestellt, also bekommt nur der Kandidat an erster Position einen Punkt, alle anderen gehen leer aus. Entsprechend ist $(1, \ldots, 1, 0)$ der Scoring-Vektor für das Veto-System, bei dem alle Kandidaten einen Punkt bekommen, außer dem Kandidaten auf der letzten Position, der keinen Punkt bekommt. Bei einer k-approval-Wahl hat der Scoring-Vektor an den ersten k Positionen eine Eins und sonst nur Nullen. Neben den Scoring-Protokollen werden auch Copeland$^\alpha$-Wahlen betrachtet. Bei dieser Familie von Wahlsystemen werden zwei Kandidaten paarweise miteinander verglichen, und der Kandidat, der von mehr Wählern bevorzugt wird, bekommt einen Punkt, der Andere geht leer aus. Im Falle eines Gleichstandes bekommen beide α Punkte, wobei α eine rationale Zahl zwischen 0 und 1 ist.

Die ursprüngliche Annahme, dass die Präferenzen aller Wähler vollständige lineare Ordnungen sind, ist in der Praxis aus verschiedenen Gründen manchmal nicht realistisch. Wenn zum Beispiel die Menge der Kandidaten sehr groß ist, ist es für die Wähler unter Umständen nicht möglich, eine Rangfolge über alle Kandidaten zu erstellen. Allgemein modellieren PossibleWinner-Probleme unterschiedliche Situationen, in denen eine Wahl in einer bestimmten Weise unvollständig angegeben ist, und fragen, ob sie so vervollständigt werden kann, dass ein gewünschter Kandidat gewinnt. Das zentrale Problem der Gewinnerbestimmung in Wahlen ist in der Praxis wünschenswerterweise in Polynomialzeit zu lösen. Im Gegensatz dazu ist es meist jedoch nicht erwünscht, dass mögliche Gewinner in Polynomialzeit berechnet werden können, da dies einen Anreiz zur Manipulation des Wahlprozesses geben würde, denn PossibleWinner verallgemeinert das Manipulationsproblem. Im ersten Teil dieser Arbeit werden verschiedene Varianten von PossibleWinner-Problemen für unterschiedliche Wahlsysteme hinsichtlich ihrer algorithmischen Eigenschaften und Komplexität untersucht.

Das ursprüngliche PossibleWinner-Problem wurde von Konczak und Lang [KL05] definiert und fragt, ob die unvollständigen Präferenzen der Wähler so zu linearen Ordnungen über alle Kandidaten erweitert werden können, dass ein gewünschter Kandidat der Sieger der Wahl ist. Für ein konkretes Wahlsystem $\mathcal{E}$ ist dieses Problem folgendermaßen definiert.

$\mathcal{E}$-PossibleWinner	
Gegeben:	Eine Menge C von Kandidaten, eine Liste V von Stimmen, die Halbordnungen über C sind, und ein ausgezeichneter Kandidat $c \in C$.
Gesucht:	Gibt es eine Erweiterung V' der Stimmen in V zu einer linearen Ordnung über C, sodass c ein Gewinner der Wahl (C, V') unter dem Wahlsystem $\mathcal{E}$ ist?

In dieser Arbeit wird gezeigt, dass PossibleWinner für das konkrete Scoring-Protokoll $(2, 1, \ldots, 1, 0)$ NP-vollständig ist. Dieses Resultat ist besonders wichtig, da es zusammen mit den Resultaten von Betzler und Dorn [BD10] ein Dichotomie-Resultat für die Familie der Scoring-Protokolle ergibt. Die Komplexität des PossibleWinner-Problems ist somit für alle Scoring-Protokolle bekannt: Für Pluralitätswahlen und Veto ist das Problem in Polynomialzeit lösbar, und für alle anderen Scoring-Protokolle ist es NP-vollständig.

Neben dem ursprünglichen PossibleWinner-Problem werden auch Varianten dieses Problems untersucht, denen jedoch allen gemeinsam ist, dass sie fragen, ob ein gewünschter Kandidat durch eine geeignete Vervollständigung der Wahl zu einem Sieger werden kann. Eine dieser Problemvarianten ist PossibleWinner *mit Hinzufügen von neuen Kandidaten*. Dieses von Chevaleyre et al. [CLMM10] eingeführte Problem modelliert die Situation, bei der eine Teilmenge der Kandidaten erst zu einem späteren Zeitpunkt zur Wahl hinzugefügt wird, diese Kandidaten also in keiner der bisher abgegebenen Präferenzen auftauchen. Es wird gezeigt, dass dieses Problem für alle Scoring-Vektoren der Form $(\alpha_1, \alpha_2, 1, 0, \ldots, 0)$, mit $\alpha_1 > \alpha_2 > 1$, NP-vollständig ist, wenn ein neuer Kandidat hinzugefügt wird. Außerdem wird dieses Problem für k-approval-Wahlen untersucht, allerdings für den Fall, bei dem die Stimmen der Wähler unterschiedlich gewichtet werden. Hier wird ebenfalls NP-Vollständigkeit gezeigt, wenn ein neuer Kandidat hinzugefügt wird.

Bei der PossibleWinner-Variante *mit verkürzten Stimmen* haben die Präferenzen der Wähler alle eine bestimmte verkürzte Form. Wenn die Menge der Alternativen zu groß ist, als dass man eine lineare Ordnung über alle Kandidaten erwarten könnte, ist es sinnvoll, die Wähler nur nach ihren am meisten und/oder am wenigsten bevorzugten Kandidaten zu fragen. Im Gegensatz zu dem zuvor betrachteten Problem wird hier gezeigt, dass für k-approval-Wahlen das PossibleWinner-Problem für alle drei Formen von verkürzten Stimmen in Polynomialzeit lösbar ist.

Die PossibleWinner-Variante *mit unbekannten Gewichten* betrachtet eine andere Form einer unvollständigen Wahl. Im Gegensatz zu den vorherigen Problemen sind hier die Präferenzen der Wähler vollständig gegeben, allerdings ist nicht bekannt, welche Gewichte die Stimmen der einzelnen Wähler haben. Insgesamt werden vier verschiedene Varianten dieses Problems betrachtet, die für Copeland$^\alpha$-Wahlen alle NP-vollständig sind. Für k-approval-Wahlen werden, für verschiedene Werte von k, sowohl Polynomialzeitalgorithmen als auch NP-Vollständigkeitsbeweise angegeben.

Die letzte untersuchte Variante ist PossibleWinner *bei unbekanntem Wahlsystem*. Die Unsicherheit liegt hier nicht in den Stimmen der Wähler, ihren Gewichten

oder der Menge der Kandidaten, sondern es ist nicht bekannt, welches Wahlsystem zur Aggregation der Stimmen verwendet wird. Falls das Wahlsystem aus der Familie der Copeland$^\alpha$-Wahlsysteme gewählt wird, ist dieses Problem in Polynomialzeit lösbar. Wenn allerdings eine geeignet eingeschränkte Klasse von Scoring-Protokollen betrachtet wird, ist dieses Problem NP-vollständig.

Die NP-Härte für die verschiedenen PossibleWinner-Probleme wird durch Reduktionen von den bekannten NP-vollständigen Problemen HittingSet, 3-DimensionalMatching, Partition, ExactCoverByThreeSets und IntegerKnapsack gezeigt. Für einige der Polynomialzeitalgorithmen werden Flußnetzwerke verwendet. In der Computational Social Choice werden weitere Probleme untersucht, die den verschiedenen Varianten der PossibleWinner-Probleme ähnlich sind. In direktem Zusammenhang stehen hierbei das Manipulationsproblem und die Bestechungsvariante SwapBribery, sodass einige der hier erzielten Resultate direkt übertragen werden können.

3 Unidirektionale Überdeckungsprobleme

Verwandt mit dem Gewinnerproblem für Wahlen sind Lösungskonzepte für Dominanzgraphen, wie sie aus einer paarweisen Mehrheitsrelation resultieren können. Ein Lösungskonzept ist eine Möglichkeit, die „beliebtesten“ Elemente eines solchen Dominanzgraphen zu bestimmen. Die Knoten eines Dominanzgraphen entsprechen den Alternativen, und eine gerichtete Kante von a nach b liegt genau dann vor, wenn b von a dominiert wird. Anwendungen für solche Dominanzgraphen gibt es unter anderem in der Argumentationstheorie, der Spieltheorie und bei Sportturnieren. Im zweiten Teil dieser Arbeit wird die Komplexität von verschiedenen Problemen bezüglich sogenannter *upward* und *downward covering sets* untersucht. Diese Mengen basieren auf den *upward* und *downward covering relations*:

- Eine Alternative a *upward covers* eine Alternative b, wenn b von a dominiert wird und alle Alternativen, die a dominieren, auch b dominieren.
- Eine Alternative a *downward covers* eine Alternative b, wenn b von a dominiert wird und alle Alternativen, die von b dominiert werden, auch von a dominiert werden.

Die Lösungskonzepte, die auf diesen unidirektionalen Überdeckungsrelationen basieren, sind inklusionsminimale Teilmengen der Alternativen, die gewisse Kriterien der internen und externen Stabilität bezüglich der upward bzw. downward covering relations erfüllen. Kürzlich haben Brandt und Fischer [BF08] gezeigt, dass es NP-hart ist, zu entscheiden, ob für einen gegebenen Dominanzgraphen eine gegebene Alternative in einem minimal upward bzw. minimal downward covering set liegt. Dieses Problem wird mit $\mathrm{MC_u}$-Member bzw. $\mathrm{MC_d}$-Member bezeichnet. Die obere Schranke wurde in beiden Fällen offen gelassen. In dieser Arbeit wird die untere Schranke auf die Stufe $\Theta_2^p = \mathrm{P}^{\mathrm{NP[log]}}$ der Polynomialzeithierarchie angehoben und die obere Schranke $\Sigma_2^p = \mathrm{NP}^{\mathrm{NP}}$ angegeben. Neben dem Problem, zu entscheiden, ob

eine gegebene Alternative in einem minimal upward/downward covering set liegt, werden noch weitere Probleme untersucht. Für minimal upward covering sets sind es folgende Probleme:

- MC_u-MemberAll: Liegt für einen gegebenen Dominanzgraphen eine gegebene Alternative in allen minimal upward covering sets?
- MC_u-Size: Gibt es für einen gegebenen Dominanzgraphen und eine gegebene Zahl k ein minimal upward covering set mit höchstens k Alternativen?
- MC_u-Unique: Hat ein gegebener Dominanzgraph ein eindeutiges minimal upward covering set?
- MC_u-Test: Ist für einen gegebenen Dominanzgraphen eine gegebene Teilmenge der Alternativen ein minimal upward covering set?

Außerdem wird das Suchproblem betrachtet, bei dem ein minimal upward covering set für einen gegebenen Dominanzgraphen ausgegeben werden soll. Zusätzlich zu den inklusionsminimalen upward covering sets werden die Probleme auch für upward covering sets von minimaler Größe betrachtet. Diese Probleme werden jeweils mit MSC_u bezeichnet. Ebenso werden alle diese Probleme auch für downward covering sets untersucht, und entsprechend mit MC_d und MSC_d bezeichnet. Die Resultate für alle betrachteten Entscheidungsprobleme sind in Tabelle 2 zusammengefasst.

Tabelle 2: Resultate für upward und downward covering set Probleme. Die beiden mit * gekennzeichneten Resultate gehen auf Brandt und Fischer [BF08] zurück; alle weiteren Ergebnisse werden in dieser Arbeit gezeigt.

Problemtyp	MC_u	MSC_u	MC_d	MSC_d
Size	NP-vollst.	NP-vollst.	NP-vollst.	NP-vollst.
Member	Θ_2^p-hart, $\in \Sigma_2^p$	Θ_2^p-vollst.	Θ_2^p-hart, $\in \Sigma_2^p$	coNP-hart, $\in \Theta_2^p$
MemberAll	coNP-vollst.*	Θ_2^p-vollst.	coNP-vollst.*	coNP-hart, $\in \Theta_2^p$
Unique	coNP-hart, $\in \Sigma_2^p$	coNP-hart, $\in \Theta_2^p$	coNP-hart, $\in \Sigma_2^p$	coNP-hart, $\in \Theta_2^p$
Test	coNP-vollst.	coNP-vollst.	coNP-vollst.	coNP-vollst.

Um die Θ_2^p-Härte Resultate zu erzielen, wird mit Hilfe von raffinierten Konstruktionen Wagners Technik [Wag87] angewendet. Eine zentrale Folgerung aus diesen Resultaten ist, dass alle vier betrachteten Suchprobleme nicht in Polynomialzeit lösbar sind, sofern nicht P = NP gilt. Dies ist ein starker Kontrast zu dem Resultat von Brandt und Fischer [BF08], dass bidirektionale minimal covering sets in Polynomialzeit berechenbar sind.

4 Gemeinsame Urteilsfindung

Der letzte Teil dieser Arbeit beschäftigt sich mit der gemeinsamen Urteilsfindung. Hier werden, wie im Beispiel der Elfmeterentscheidung, individuelle Urteile über

möglicherweise miteinander verbundene logische Propositionen aggregiert. In der Social-Choice-Theorie werden verschiedene Möglichkeiten der Einflussnahme auf Wahlen untersucht, und in der Computational Social Choice wird die Berechnungskomplexität von Problemen in Bezug auf Manipulation, Bestechung und Kontrolle untersucht. Diese Probleme sind allerdings nicht nur für Wahlen interessant, sondern auch allgemein für Entscheidungsfindungsprozesse. Endriss et al. [EGP12] initiierten die algorithmische und komplexitätstheoretische Untersuchung von gemeinsamer Urteilsfindung, unter anderem mit der Analyse des Gewinner- und Manipulationsproblems. In dieser Arbeit werden die Ergebnisse zum Manipulationsproblem auf eine ganze Klasse von Urteilsfindungsprozeduren ausgeweitet, und es wird die Untersuchung von Bestechungs- und Kontrollproblemen in Urteilsfindungsprozessen motiviert und ihre Berechnungskomplexität untersucht. Auch hier kann NP-Härte eine Art Schutz gegen diese unerwünschten Arten von Einflussnahme bieten. Zusätzlich zur klassischen Komplexitätstheorie untersuchen wir hier auch die parametrisierte Komplexität und zeigen W[2]-Härte für verschiedene Probleme.

Die Teilnehmer eines Urteilsfindungsprozesses werden als *Richter* bezeichnet, und die Menge der Aussagen, über die sie ihr Urteil abgeben, ist die *Agenda*. Eine Urteilsfindungsprozedur ermittelt ein gemeinsames Urteil auf Basis der individuellen Urteile der Richter. Die hier betrachtete Klasse von voraussetzungsbasierten Urteilsfindungsprozeduren liefert, unter gewissen Voraussetzungen, immer konsistente gemeinsame Urteile. Dies wird durch eine geschickte Unterteilung der Agenda in Voraussetzungen und Folgerungen erreicht. Bei der Aggregation wird die Urteilsfindungsprozedur jetzt nur noch auf die Voraussetzungen angewendet, und das gemeinsame Urteil für die Folgerungen wird daraus abgeleitet. Die *Premise-based Procedure*, kurz *PBP*, bezeichnet die voraussetzungsbasierte Prozedur, bei der zur Aggregation der Voraussetzungen die Mehrheitsregel angewendet wird. Eine Verallgemeinerung ist die *Uniform Premise-based Quota Rule*, kurz $UPQR_q$, wobei q eine rationale Zahl zwischen 0 und 1 ist. Hier wird bei n Richtern eine Aussage der Agenda in das gemeinsame Urteil aufgenommen, wenn mindestens ein Schwellenwert von $n \cdot q$ Zustimmungen erreicht wird. Des weiteren wird die *Uniform Constant Premise-based Quota Rule*, kurz $UCPQR_q$, betrachtet, bei der der Schwellenwert q eine feste Anzahl von Richtern ist.

Das Manipulationsproblem in der gemeinsamen Urteilsfindung, definiert von Endriss et al. [EGP12], fragt, ob ein Richter einen Anreiz hat, ein unaufrichtiges Urteil abzugeben, da es zu einem für ihn besseren Ergebnis führt. Die Distanz zwischen zwei Urteilen ist hierbei über die Hammingdistanz definiert. Eng verwandt mit dem Manipulationsproblem ist das in dieser Arbeit für gemeinsame Urteilsfindung eingeführte Bestechungsproblem (Bribery). Hier versucht eine externe Person das Ergebnis durch Bestechung der Richter zu seinen Gunsten abzuändern, ohne dabei sein Budget zu überschreiten. Durch die Zahlung eines Bestechungsgeldes wird erreicht, dass der Richter das von der externen Person gewünschte Urteil abgibt. Auch hier wird die Distanz zwischen zwei Urteilen über die Hammingdistanz definiert. Zusätzlich wird jedoch auch eine exakte Variante (ExactBribery) betrachtet, bei der das Ziel der externen Person ist, ein bestimmtes (möglicherweise

unvollständiges) Urteil zu erzielen. Außerdem wird für diese beiden Varianten auch die sogenannte Mikrobestechung (MICROBRIBERY) untersucht, bei der nicht dafür gezahlt wird ein komplettes individuelles Urteil abzuändern, sondern für jeden einzelnen Eintrag der Voraussetzungen, der abgeändert werden soll.

Neben der klassischen Berechnungskomplexität werden einige dieser Probleme auch bezüglich ihrer parametrisierten Komplexität untersucht. Hier wird untersucht, ob NP-harte Probleme vielleicht doch in Polynomialzeit lösbar sind, wenn bestimmte Parameter der Eingabe fest vorgegeben sind. Wenn dies der Fall ist, dann wird ein Problem *fixed-parameter tractable* bezüglich dieses Parameters genannt. In dieser Arbeit wird allerdings Härte für die Klasse W[2] gezeigt, welche Probleme beinhaltet, die als *fixed-parameter intractable* angesehen werden. Im Bezug auf Wahlsysteme können solche Parameter zum Beispiel die Anzahl der teilnehmenden Wähler oder die Anzahl der Kandidaten sein. Die in dieser Arbeit erzielten Ergebnisse zum Manipulationsproblem und den verschiedenen Bestechungsproblemen in gemeinsamer Urteilsfindung sind in Tabelle 3 zusammengefasst.

Tabelle 3: Übersicht über die Ergebnisse zu Manipulation und Bestechung

Parameter	$UPQR_q$-MANIPULATION	PBP-BRIBERY	PBP-EXACTBRIBERY	PBP-MICROBRIBERY	PBP-EXACTMICROBRIBERY
# Richter	NP-vollst.	NP-vollst.		NP-vollst.	NP-vollst.
max # Änderungen	W[2]-hart	✗	✗	✗	✗
# Bestechungen	✗	NP-vollst.	W[2]-hart	✗	✗
# Mikrobestechungen	✗	✗	✗	NP-vollst.	NP-vollst.
Allg. Problem	NP-vollst.	NP-vollst.	NP-vollst.	NP-vollst.	NP-vollst.

Zusätzlich zur NP-Härte für die allgemeinen Probleme wird gezeigt, dass einige der Probleme NP-hart bleiben, selbst wenn bestimmte Parameter der Eingabegröße fest sind. So bezeichnet „# Richter“ eine feste Anzahl von Richtern, und „max # Änderungen“ die maximale Anzahl von Änderungen in den Voraussetzungen, die nötig sind, um das Ziel zu erreichen. „# Bestechungen“ bezeichnet das Problem, bei dem nur eine feste Anzahl von Richtern bestochen werden kann, und „# Mikrobestechungen“ steht für das Problem, bei dem die Anzahl der Mikrobestechungen eine feste Konstante ist. Die NP-Vollständigkeit wird in allen Fällen durch Reduktionen vom NP-vollständigen Problem DOMINATINGSET gezeigt. Für den Parameter „Größe der dominierenden Menge“ ist dieses Problem ebenfalls W[2]-vollständig. Diese Tatsache wird verwendet, um W[2]-Härte für das Manipulationsproblem zu

zeigen. Die W[2]-Härte im Falle der exakten Bestechung folgt jedoch aus der W[2]-Härte des eng verwandten OptimalLobbying-Problems. Der Eintrag ✗ impliziert, dass die gegebene Kombination von Problem und Parameter nicht anwendbar ist. Für die W[2]-harten (und erst recht für die für feste Parameter NP-harten) Probleme sind Manipulation bzw. Bestechung in den hier untersuchten Urteilsfindungsprozeduren nicht ohne weiteres durchführbar.

Neben Manipulation und Bestechung werden in dieser Arbeit drei Arten von Kontrolle untersucht, bei denen die Menge der teilnehmenden Richter verändert wird. Zum einen ist das Kontrolle durch Hinzufügen oder Entfernen von Richtern (Control by Adding/Deleting Judges) und zum anderen Kontrolle durch Ersetzen von Richtern (Control by Replacing Judges). Die ersten beiden Probleme sind abgeleitet von den Kontrollproblemen durch Hinzufügen oder Entfernen von Wählern, und das dritte wird in dieser Arbeit speziell für die gemeinsame Urteilsfindung eingeführt. Da das Eingreifen in eine Wahl durch Kontrolle meist ein unerwünschtes Verhalten ist, übernehmen wir hier die Notation aus dem Bereich Wahlen und sagen, ein Problem ist resistent gegen ein bestimmtes Kontrollproblem, wenn das entsprechende Entscheidungsproblem NP-hart ist. Auch hier werden wieder je zwei Varianten der Probleme untersucht: die auf der Hammingdistanz basierende und die exakte Variante. Im Gegensatz zu Manipulation und Bestechung sind hier die Uniform Premise-based Quota Rule und die Uniform Constant Premise-based Quota Rule echt verschiedene Klassen von Urteilsfindungsprozeduren, da sich die Zahl der teilnehmenden Richter, und somit der Schwellenwert, durch die Kontrollaktion verändern kann. Die Ergebnisse für die in dieser Arbeit untersuchten Kontrollprobleme sind in Tabelle 4 zusammengefasst. Ähnlich zu den Härteresultaten für Manipulation und Bestechung ist die Resistenz der untersuchten Urteilsfindungsprozeduren ein positives Resultat.

Tabelle 4: Übersicht über die Ergebnisse für die verschiedenen Kontrollprobleme

Problem	$UCPQR_q$	$UPQR_{1/2}$	$UPQR_q$
Control by Adding Judges	resistent	resistent	
Exact Control by Adding Judges	resistent	resistent	
Control by Deleting Judges	resistent	resistent	
Exact Control by Deleting Judges	resistent	resistent	
Control by Replacing Judges	resistent	resistent	resistent
Exact Control by Replacing Judges	resistent	resistent	resistent

Fazit: Insgesamt beinhaltet die Social-Choice-Theorie viele interessante Probleme, die uns auch im Alltag immer wieder begegnen. Mit der Verbindung zur Informatik wurde mit der Computational Social Choice ein Gebiet geschaffen, welches uns vor spannende Herausforderungen stellt, vor allem bei der Untersuchung der algorithmischen Eigenschaften und der Komplexität der zugehörigen Probleme.

Literatur

[Bau12] D. Baumeister. *Computational Complexity in Three Areas of Computational Social Choice: Possible Winners, Unidirectional Covering Sets, and Judgment Aggregation.* Dissertation, Heinrich-Heine-Universität Düsseldorf, Germany, 2012.

[BCE12] F. Brandt, V. Conitzer und U. Endriss. Computational Social Choice. In G. Weiß, Hrsg., *Multiagent Systems.* MIT Press, 2012. 2nd edition, to appear.

[BD10] N. Betzler und B. Dorn. Towards a Dichotomy of Finding Possible Winners in Elections Based on Scoring Rules. *Journal of Computer and System Sciences*, 76(8):812–836, 2010.

[BF08] F. Brandt und F. Fischer. Computing the Minimal Covering Set. *Mathematical Social Sciences*, 56(2):254–268, 2008.

[CLMM10] Y. Chevaleyre, J. Lang, N. Maudet und J. Monnot. Possible Winners when New Candidates Are Added: The Case of Scoring Rules. In *In Proceedings of AAAI'10*, Seiten 762–767. AAAI Press, 2010.

[EGP12] U. Endriss, U. Grandi und D. Porello. Complexity of Judgment Aggregation. *Journal of Artificial Intelligence Research*, 45:481–514, 2012.

[KL05] K. Konczak und J. Lang. Voting Procedures with Incomplete Preferences. In *Proceedings of the Multidisciplinary IJCAI-05 Worshop on Advances in Preference Handling*, Seiten 124–129, 2005.

[KS86] L. A. Kornhauser und L. G. Sager. Unpacking the Court. *Yale Law Journal*, 96(1):82–117, 1986.

[Pet01] P. Pettit. Deliberative Democracy and the Discursive Dilemma. *Philosophical Issues*, 11:268–299, 2001.

[RBLR11] J. Rothe, D. Baumeister, C. Lindner und I. Rothe. *Einführung in Computational Social Choice: Individuelle Strategien und kollektive Entscheidungen beim Spielen, Wählen und Teilen.* Spektrum Akademischer Verlag, 2011.

[Wag87] K. Wagner. More Complicated Questions About Maxima and Minima, and some Closures of NP. *Theoretical Computer Science*, 51:53–80, 1987.



Dorothea Baumeister wurde am 01. Juli 1983 in Duisburg geboren. Von Oktober 2002 bis September 2007 studierte sie Informatik mit Nebenfach Mathematik an der Heinrich-Heine-Universität Düsseldorf. In ihrer Masterarbeit beschäftigte sie sich mit der Berechnungskomplexität des Problems Tantrix^{TM}Rotation Puzzle. Seit Oktober 2007 arbeitet sie als wissenschaftliche Mitarbeiterin in der Arbeitsgruppe von Prof. Dr. Jörg Rothe und hat ihre Dissertation in dem interdisziplinären Gebiet Computational Social Choice im September 2012 erfolgreich abgeschlossen. Seit September 2011 ist sie außerdem Mutter einer Tochter. Zur Zeit arbeitet sie als Postdoc in der Arbeitsgruppe von Prof. Dr. Jörg Rothe.

Mengenwertige Lösungskonzepte in Spieltheorie und Social-Choice-Theorie*

Markus Brill

Institut für Informatik
Technische Universität München
brill@in.tum.de

Abstract: Meine Arbeit beschäftigt sich mit mengenwertigen Lösungskonzepten aus der Spieltheorie und der Social-Choice-Theorie. Hauptaugenmerk liegt dabei auf der Berechnungskomplexität von Lösungskonzepten. Insbesondere werden komplexitätstheoretische Fragestellungen im Kontext von Normalform-Spielen, Wahlverfahren und Turnierlösungen betrachtet. Außerdem werden die Manipulierbarkeit mengenwertiger Wahlverfahren sowie axiomatische Aspekte von Lösungskonzepten untersucht.

1 Einleitung

Spieltheorie und Social-Choice-Theorie sind Teilgebiete der theoretischen Wirtschaftswissenschaften und haben in den vergangenen zwei Jahrzehnten innerhalb der Informatik stark an Bedeutung gewonnen. In beiden Bereichen geht es darum, Entscheidungen auf der Grundlage von Präferenzen zu treffen. Die Akteure der Entscheidungssituation werden üblicherweise als *Agenten* bezeichnet. Ein Agent ist eine autonome Entität, der Präferenzen über mögliche Ergebnisse zugeschrieben werden können. Das kann ein Mensch, eine Organisation, oder ein Computerprogramm sein. Kompliziert – und interessant – werden Entscheidungssituationen erst dann, wenn mehrere Agenten beteiligt sind.

Die *Spieltheorie* untersucht Situationen, in denen das Wohlergehen eines Agenten nicht nur von seinen eigenen Aktionen, sondern auch von den Aktionen der anderen Agenten abhängt. Ihre Anfänge hat die Spieltheorie in der Analyse von Gesellschaftsspielen; mittlerweile hat sie sich zu einem wichtigen Gebiet mit zahlreichen Anwendungen in den Sozialwissenschaften entwickelt.

Die *Social-Choice-Theorie* (am ehesten als *Theorie kollektiver Entscheidungen* zu übersetzen) betrachtet die Frage, wie eine Gruppe von Agenten eine gemeinsame Entscheidung treffen kann, die alle Mitglieder der Gruppe betrifft. Im allgemeinsten Fall gibt es eine Menge von möglichen Alternativen und jeder Agent hat Vorlieben über diese, meist ausgedrückt in Form einer Präferenzliste. Social-Choice-Theorie ist ein stark interdiszi-

*Englischer Titel der Dissertation: "Set-Valued Solution Concepts in Social Choice and Game Theory: Axiomatic and Computational Aspects".

plinär geprägtes Forschungsgebiet, zu dem unter anderem Mathematiker, Wirtschaftswissenschaftler, Politikwissenschaftler und Psychologen Beiträge geleistet haben.

Die wichtigsten Untersuchungsgegenstände von Spieltheorie und Social-Choice-Theory sind sogenannte *Lösungskonzepte*. In der (nicht-kooperativen) Spieltheorie modelliert ein Lösungskonzept rationales Verhalten. Für eine gegebene Spezifizierung einer Entscheidungssituation gibt ein Lösungskonzept jedem Agenten eine Handlungsempfehlung, die das Wohlergehen des Agenten maximiert. Dieser präskriptiven Interpretation wird oft eine deskriptive Perspektive gegenüber gestellt, die die Rolle von Lösungskonzepten bei der Vorhersage rationalen Verhaltens betont.

In der Social-Choice-Theorie hingegen versteht man unter Lösungskonzepten Verfahren zur Bündelung von Präferenzen. Wahlverfahren sind ein typischens Beispiel. Ein Lösungskonzept bildet die individuellen Präferenzen der einzelnen Agenten entweder auf eine oder mehrere Alternativen (die „Gewinner“) oder auf eine aggregierte Präferenzliste ab. Zum Vergleich verschiedener Lösungskonzepte werden oft Fairnesskriterien, sogenannte *Axiome*, herangezogen. Ein einfaches Beispiel für ein solches Axiom ist die Forderung, dass alle Agenten gleich behandelt werden sollen. Auch in der Social-Choice-Theorie kommt spieltheoretischen Überlegungen eine wichtige Rolle zu. Eine grundlegende Frage ist beispielsweise, ob Agenten das vom Lösungskonzept ausgewählte Ergebnis zu ihren Gunsten beeinflussen können, indem sie falsche Angaben zu ihren Präferenzen machen. Da dieses Phänomen im Allgemeinen unerwünscht ist, wird neben der Einhaltung einer Reihe von Fairnessaxiomen üblicherweise auch eine gewisse Immunität eines Lösungskonzepts gegenüber solchen „strategischen Manipulationen“ gefordert.

Ein Lösungskonzept heißt *mengenwertig*, wenn die Möglichkeit besteht, dass mehr als eine Handlungsempfehlung bzw. Alternative ausgewählt wird. Aus mathematischer Sicht sind mengenwertige Lösungskonzepte oftmals eleganter, vor allem weil sie nicht auf ein willkürliches Tie-Breaking angewiesen sind. Die Interpretation mengenwertiger Lösungskonzepte ist nicht offensichtlich: Letzten Endes muss aus der Menge eine eindeutige Auswahl getroffen werden; wie diese endgültige Auswahl zu geschehen hat, wird von einem mengenwertigen Lösungskonzept allerdings nicht spezifiziert. Der Fokus eines mengenwertigen Lösungskonzeptes liegt daher eher auf dem Aussortieren unerwünschter Alternativen als auf der endgültigen Auswahl einer einzigen „optimalen“ Alternative.

In den vergangenen Jahren hat die Bedeutung *algorithmischer* Eigenschaften von Lösungskonzepten sowohl in der Spieltheorie als auch in der Social-Choice-Theorie stetig zugenommen. Diese Entwicklung wird häufig mit dem Schlagwort *Algorithmic Economics* zusammengefasst und mit dem Aufkommen des Internets in Zusammenhang gebracht. In der Tat kann man das Internet als einen großen Marktplatz sehen, auf dem viele Agenten mit unterschiedlichen Interessen interagieren. Diese Sichtweise legt den Einsatz von Konzepten und Techniken nahe, die in Spieltheorie und Social-Choice-Theorie entwickelt wurden. In der Folge sind zwei interdisziplinäre Forschungsgebiete an der Schnittstelle zwischen Informatik und Wirtschaftswissenschaften entstanden: *Algorithmische Spieltheorie* und *Computational Social Choice* (Abb. 1).

Der Ideenaustausch zwischen der algorithmischen und der wirtschaftswissenschaftlichen Perspektive erfolgt in beide Richtungen. Einerseits werden strategische Überlegungen und

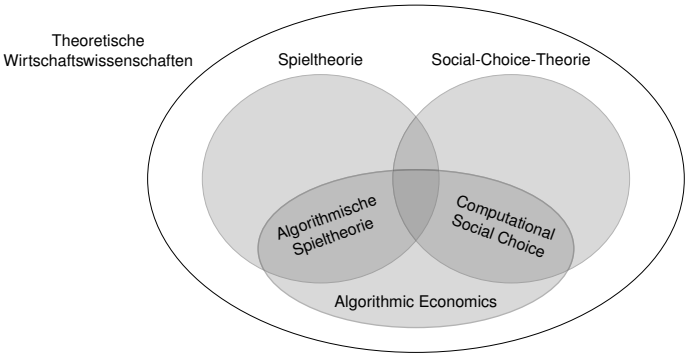


Abbildung 1: Einordnung der Gebiete *Algorithmische Spieltheorie* und *Computational Social Choice*

Fairnessaxiome beispielsweise beim Design von Multiagentensystemen berücksichtigt. Andererseits helfen Ansätze und Techniken aus der Informatik dabei, in der Spieltheorie und Social-Choice-Theorie auftretende Phänomene besser zu verstehen. Ein gutes Beispiel für die letztgenannte Richtung findet sich in der umfangreichen Literatur zum Thema *Berechnungskomplexität von Lösungskonzepten*. Die Motivation solcher Fragestellungen ist naheliegend: Ohne einen effizienten Algorithmus zur Berechnung der Lösung ist selbst das schönste Lösungskonzept mehr oder weniger nutzlos. Bei spieltheoretischen Lösungskonzepten hängt die Berechnungskomplexität sogar direkt mit der Plausibilität des Konzeptes als einem Mittel zur Vorhersage des Ergebnisses zusammen. Wieso sollten sich rationale Agenten entsprechend eines Lösungskonzeptes verhalten, wenn Lösungen nicht in vernünftiger Zeit berechnet werden können?

2 Spieltheorie

Algorithmische Spieltheorie hat sich mittlerweile als wichtiges Forschungsgebiet innerhalb der Informatik etabliert (siehe z. B. den Übersichtsartikel [Rou10]). Das wohl prominenteste Resultat betrifft die Berechnungskomplexität von Nash-Gleichgewichten, dem zweifelsohne wichtigsten spieltheoretischen Lösungskonzept. Während Nash-Gleichgewichte in Matrixspielen (2-Personen-Nullsummenspiele) noch effizient berechnet werden können, haben Daskalakis et al. gezeigt, dass das Problem bereits in allgemeinen 2-Personen-Spielen PPAD-vollständig ist. Dieses und ähnliche Resultate haben nicht zuletzt die Suche nach alternativen spieltheoretischen Lösungskonzepten mit angenehmeren algorithmischen Eigenschaften inspiriert. Die mengenwertigen Lösungskonzepte, die ich im Rahmen meiner Arbeit untersuche, stellen solche Alternativen zum Nash-Gleischgewicht dar. Diese Konzepte beruhen auf verschiedenen Varianten von Dominanz. Eine *Dominanzart* formalisiert, wann eine Aktion besser als eine andere Aktion desselben Spielers ist. Beispielsweise dominiert eine Aktion x eine Aktion y bzgl. *strikter Dominanz*, falls das Ergebnis für den Spieler bei der Wahl von x immer strikt besser ist als das Ergebnis bei der Wahl von y, unabhängig von den Aktionen der anderen Spieler.

	b_1	b_2	b_3	b_4
a_1	5	3	4	6
a_2	2	4	5	3
a_3	4	2	6	1
a_4	1	3	0	7

Abbildung 2: Ein Matrixspiel mit Aktionen a_1, a_2, a_3, a_4 für den Zeilenspieler und Aktionen b_1, b_2, b_3, b_4 für den Spaltenspieler. Das Paar $(\{a_1, a_2\}, \{b_1, b_2\})$ ist ein Sattel des Spiels, da jede der vier Nicht-Sattel-Aktionen a_3, a_4, b_3, b_4 jeweils von einer Sattel-Aktion strikt dominiert wird, falls der andere Spieler nur Sattelaktionen spielt. Interne Stabilität und Minimalität lassen sich ebenfalls leicht überprüfen.

2.1 Algorithmen für dominanzbasierte Lösungskonzepte

Der Wirtschafts-Nobelpreisträger Lloyd Shapley hat bereits in den frühen 1950er Jahren eine Alternative zum Nash-Gleichgewicht in Matrixspielen vorgeschlagen, das *minimale Mengen* von Aktionen anstatt Randomisierungen als Lösungen zulässt. Shapley definiert einen *verallgemeinerten Sattelpunkt* (VSP) als ein Tupel von Teilmengen von Aktionen eines jeden Spielers, das *extern stabil* ist: falls die anderen Spieler lediglich Aktionen aus ihren jeweiligen Teilmengen wählen, so ist jede Aktion außerhalb der Teilmenge von einer Aktion innerhalb der Teilmenge strikt dominiert. Ein VSP ist minimal, falls er keinen anderen VSP enthält. Minimale VSPs, von Shapley *Sattel* genannt, sind auch *intern stabil* in dem Sinne, dass keine Aktion in der Teilmenge eines Spielers von einer anderen Aktion in der Teilmenge strikt dominiert wird – wiederum unter der Voraussetzung, dass alle anderen Spieler nur Aktionen aus ihren Teilmengen wählen. Abb. 2 zeigt ein Beispiel.

Duggan und Le Breton haben den Ansatz von Shapley auf Normalform-Spiele und auf verschiedene Arten von Dominanz erweitert, indem sie ein D-*set* als ein minimales Tupel von Teilmengen von Aktionen definieren, das intern und extern stabil bzgl. einer Dominanzart D ist. Auf diese Weise erhält man eine Vielzahl von interessanten mengenwertigen Lösungskonzepten. Neben den von Shapley eingeführten Satteln lassen sich etwa auch die *primitive formations* von Harsanyi und Selten sowie die *CURB sets* von Basu und Weibull als D-sets für ein geeignetes D darstellen.

In meiner Arbeit beschäftige ich mich zunächst mit der Frage, wie viele D-sets ein Spiel haben kann und unter welchen Bedingungen verschiedene Dominanzarten zu dem gleichen Lösungskonzept führen. Für strikte Dominanz (S) hat Shapley die Eindeutigkeit von S-sets in Matrixspielen gezeigt. Duggan und Le Breton bewiesen das analoge Resultat für schwache Dominanz (W) und sehr schwache Dominanz (V) in Konfrontationsspielen, einer Teilklasse von Matrixspielen. Ich identifiziere viele weitere Klassen von Spielen, in denen D-sets für bestimmte D eindeutig sind. Andererseits zeige ich, dass für manche Dominanzarten selbst sehr eingeschränkte Spielklassen eine in der Größe des Spiels exponentielle Anzahl von Lösungen haben können.

	S	B	S^*	C_d	C	V	V^*
Normalform-Spiele	poly	poly	poly				
Matrixspiele	eind.	eind.	eind.				
symmetrische Matrixspiele				eind.	eind.	exp	
Konfrontationsspiele				eindeutig			exp
Turnierspiele		eindeutig		eindeutig			

Tabelle 1: Resultate zur Anzahl und Berechnungskomplexität von D-sets. Für eine gegebene Dominanzart D und eine Klasse von Spielen (per Mengeninklusion geordnet) enthält die Tabelle Angaben über die Anzahl der D-sets (eindeutig, polynomiell oder exponentiell). Für alle dunkelgrau hinterlegten Zellen findet der Greedy-Algorithmus alle D-sets in polynomieller Zeit. Für die hellgrau hinterlegten Zellen findet der fortgeschrittene Algorithmus das eindeutige D-set. Zellen, die sich über mehrere Spalten erstrecken, zeigen an, dass die entsprechenden D-sets in der jeweiligen Spielklasse übereinstimmen. Die Dominanzarten C_d und C sind nur in symmetrischen Matrixspielen definiert. Die Dominanzart W wurde nicht betrachtet, da es Spiele ohne W-sets gibt.

Anschließend betrachte ich die Berechnungskomplexität von D-sets. Neben den bereits erwähnten Dominanzarten S und V betrachte ich deren gemischte Varianten S^* und V^*, *Börgers-Dominanz* (B), *covering* (C) und *deep covering* (C_d). Ich schlage zwei generische Algorithmen zur Berechnung von D-sets vor: einen Greedy-Algorithmus und einen „fortgeschrittenen“ Algorithmus. Anschließend werden für beide Algorithmen abstrakte Eigenschaften definiert, die – falls sie für eine gegebene Dominanzart in einer gegebenen Spielklasse erfüllt sind – die Korrektheit und Effizienz des jeweiligen Algorithmus garantieren. Mit diesem Ansatz erhalte ich dann für jede betrachtete Kombination aus Dominanzart und Spielklasse einen effizienten Algorithmus zur Berechnung *aller* D-sets eines Spiels – mit Ausnahme derer Kombinationen, für die die Anzahl von D-sets exponentiell sein kann. Interessanterweise basieren die fortgeschrittenen Algorithmen auf der wiederholten Berechnung von Nash-Gleichgewichten mittels linearer Optimierung. Dies ist bemerkenswert, da die resultierenden mengenwertigen Lösungen wenig mit Nash-Gleichgewichten gemein haben. Die Ergebnisse sind in Tabelle 1 zusammengefasst.

2.2 Härteresultate für dominanzbasierte Lösungskonzepte

Die Algorithmen aus Abschnitt 2.1 funktionieren für viele, aber nicht für alle betrachteten Dominanzarten. Zum Beispiel zeigt Tabelle 1, dass selbst ein symmetrisches Matrixspiel exponentiell viele V-sets und V^*-sets haben kann. Gleiches gilt für W-sets und W^*-sets. Es kann also keinen effizienten Algorithmus geben, der für eines dieser Konzepte alle Lösungen (explizit) berechnet. Nichtsdestotrotz bleiben einige natürliche Komplexitätsfragen offen. Man kann beispielsweise fragen, ob man *eine* Lösung schnell finden kann oder ob eine Lösung mit bestimmten Eigenschaften existiert. Fragen dieser Art un-

tersuche ich in meiner Arbeit für schwache (W) und für sehr schwache (V) Dominanz. Da W-sets nicht immer existieren, betrachte ich *schwache Sattel*, eine Variante von W-sets, deren Existenz dadurch garantiert ist, dass lediglich externe Stabilität gefordert wird. Sowohl für V-sets als auch für schwache Sattel beweise ich eine Reihe von Härteresultaten. Beispielsweise ist das Suchproblem „Finde eine Lösung“ für beide Konzepte NP-schwer. Darüberhinaus ist es sogar Θ_2^p-schwer zu entscheiden, ob ein schwacher Sattel existiert, der eine gegebene Aktion enthält. Das bedeutet, dass dieses Entscheidungsproblem vermutlich nicht einmal in NP enthalten ist. Für V-sets ist das analoge Problem sowohl NP-schwer als auch coNP-schwer.

2.3 Iteriertes Löschen von dominierten Aktionen

Neben D-sets und schwachen Satteln untersuche ich eine weitere Klasse von dominanzbasierten Lösungskonzepten. Diese Klasse hat in der Spieltheorie eine lange Tradition und ist durch das iterierte Löschen von dominierten Aktionen definiert. Für eine gegebene Dominanzart D sucht man in jedem Schritt Aktionen, die von einer anderen Aktion D-dominiert werden. Diese werden dann gelöscht und die Suche geht in dem verkleinerten Spiel weiter, so lange bis es keine D-dominierten Aktionen mehr gibt. Die verbleibenden Aktionen definieren die Lösung des Spiels. Für manche Dominanzarten wie z. B. S, S^* und B ist die so definierte Lösung eines Spiels *unabhängig* von der Reihenfolge der Löschungen. Für andere, wie beispielsweise W, ist das nicht der Fall.

In meiner Arbeit analysiere ich das iterierte Löschen von W-dominierten Aktionen komplexitätstheoretisch. Für das Problem der Eliminierbarkeit gegebener Aktionen in Matrixspielen gebe ich einen nicht-trivialen effizienten Algorithmus an. Andererseits zeige ich, dass eine Reihe natürlicher Probleme bereits in sehr eingeschränkten Spielklassen NP-vollständig ist. Beispielsweise ist es bereits in Matrixspielen schwer zu entscheiden, ob ein gegebenes Teilspiel durch eine Löschungssequenz erreicht werden kann. Dieses Resultat ist besonders bemerkenswert, da Härteresultate für Matrixspiele sehr selten sind.

3 Wahlverfahren

Computational Social Choice ist auf dem Weg, sich ähnlich wie algorithmische Spieltheorie an der Schnittstelle zwischen Wirtschaftswissenschaften und Informatik zu etablieren. Diverse Übersichtsartikel dokumentieren das gestiegene Interesse, das diesem jungen Forschungsgebiet zuteil wird [Con10, FHH10].

Man kann sich ein Lösungskonzept aus der Social-Choice-Theorie als ein *Wahlverfahren* vorstellen, das für eine gegebene Menge von Präferenzlisten („Stimmzetteln“) eine Menge von Alternativen als *Gewinner* auswählt. Agenten werden in diesem Kontext *Wähler* gennant. Abb. 3 (links) zeigt eine typische Instanz eines Social-Choice-Problems, ein sogenanntes *Präferenzprofil*. Die Zahlen über der horizontalen Linie geben an, wie viele Wähler die der Spalte entsprechenden Präferenzen haben. In dem Beispiel haben drei

3	4	3	4	1
a	d	a	c	d
b	c	b	b	a
c	a	d	d	b
d	b	c	a	c

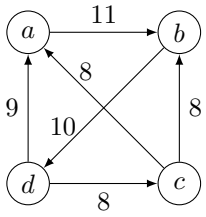


Abbildung 3: Präferenzprofil mit 15 Wählern und 4 Alternativen a, b, c, d (links) und zugehöriger gewichteter Mehrheitsgraph (rechts)

Wähler die Präferenzen $a \succ b \succ c \succ d$, vier Wähler die Präferenzen $d \succ c \succ a \succ b$ usw. Für jedes Präferenzprofil kann man den *gewichteten Mehrheitsgraphen* aufstellen (Abb. 3, rechts). Die Knoten dieses Graphen sind durch die Alternativen gegeben und die Kanten zeigen die Ergebnisse der paarweisen Mehrheitsvergleiche an. Außerdem ist jede Kante mit der Anzahl der Wähler, die die entsprechende Präferenz teilen, gewichtet.

3.1 Komplexität der Gewinnerbestimmung

Das grundlegendste algorithmische Problem für ein Wahlverfahren ist die Bestimmung der Gewinner. In meiner Arbeit untersuche ich dieses Problem für drei Wahlverfahren: das von Tideman entwickelte Verfahren *Ranked Pairs* [Tid87] und die Verfahren von Young und Dodgson.

Ranked Pairs ist eines der am weitesten verbreiteten Condorcet-Verfahren und ist in seinem Ansatz sehr ähnlich zu dem Verfahren von Schulze, das unter anderem bei der Wikimedia Foundation und der Piratenpartei zur Entscheidungsfindung genutzt wird. Grundidee von Ranked Pairs ist die Konstruktion eines kollektiven Rankings, das so viel wie möglich mit den Präferenzen der einzelnen Wähler übereinstimmt. Dazu wird zunächst für jedes geordnete Paar (x, y) von Alternativen gezählt, wie viele Wähler x gegenüber y bevorzugen. Diese Zahlen entsprechen also genau den Kantengewichten in Abb. 3. Für das Paar, das diese Anzahl maximiert, wird im kollektiven Ranking die Reihenfolge fixiert. In dem Beispiel in Abb. 3 wird im ersten Schritt festgelegt, dass im kollektiven Ranking a gegenüber b bevorzugt ist. Anschließend schaut man sich die Kante mit dem nächstkleineren Gewicht an und fixiert die Relation, falls man dadurch keinen Kreis mit den bisher fixierten Paaren erzeugt. Im Beispiel wird die Kante von b nach d fixiert, die von d nach a allerdings nicht, weil sie einen Kreis mit (a, b) und (b, d) erzeugen würde. Das nächtkleinere Kantengewicht ist nicht eindeutig, weil die Kanten (c, a), (c, b) und (d, c) alle Gewicht 8 haben. In solchen Fällen schreibt Ranked Pairs vor, alle möglichen Reihenfolgen zu betrachten. Im Beispiel führt diese Vorgensweise zu zwei verschiedenen Rankings: $a \succ b \succ d \succ c$ und $c \succ a \succ b \succ d$. Ranked Pairs Gewinner sind nun alle Alternativen, die an der Spitze eines so konstruierten Rankings stehen, in unserem Fall a und c.

Obwohl Ranked Pairs ein wohlbekanntes Wahlverfahren ist, das viele wünschenswerte Eigenschaften erfüllt, war die Komplexität der Gewinnerbestimmung unbekannt. In eini-

gen Arbeiten wurde implizit und ohne Begründung angenommen, dass das Problem in P ist. In meiner Arbeit zeige ich allerdings, dass das Problem NP-vollständig ist. Aus diesem Resultat folgen eine ganze Reihe anderer Härteresultate als Korollare, beispielsweise die NP-Schwere der Berechnung von notwendigen und möglichen Gewinnern bei unvollständig spezifizierten Präferenzen.

Für die Verfahren von Young und Dodgson zeige ich, dass das Problem der Gewinnerbestimmung Θ_2^p-vollständig ist. Für beide Resultate gibt es bereits frühere Beweise, die nicht vollständig korrekt sind und von mir adaptiert bzw. korrigiert werden.

3.2 Manipulation mengenwertiger Wahlverfahren

Die Manipulation von Wahlverfahren durch die falsche Angabe von Präferenzen ist ein gut untersuchtes Phänomen. Eines der bekanntesten Resultate der Social-Choice-Theorie, das Gibbard-Satterthwaite-Theorem, besagt im Wesentlichen, dass jedes nicht-triviale Wahlverfahren anfällig für derartige Manipulationen ist. Allerdings gilt dieses Theorem nicht für mengenwertige Wahlverfahren. Es ist daher naheliegend, sich mit der Manipulation mengenwertiger Wahlverfahren zu beschäftigen, wobei man bald feststellt, dass bereits die Definition einer Manipulation im mengenwertigen Kontext nicht unmittelbar klar ist. Wie will man schließlich entscheiden, ob ein Wähler ein Ergebnis gegenüber einem anderen Ergebnis bevorzugt, wenn beide Ergebnisse Mengen sind? Zur Beantwortung dieser Frage wurden verschiedene sogenannte *Mengenerweiterungen* definiert. Eine Mengenerweiterung erweitert eine Präferenzrelation über Alternativen auf eine Präferenzrelation über Mengen von Alternativen. Einfachstes Beispiel ist die Mengenerweiterung von Kelly, die besagt, dass ein Wähler eine Menge X gegenüber einer Menge Y genau dann bevorzugt, wenn er jedes Element von X gegenüber jedem Element von Y bevorzugt. Natürlich ist diese Mengenerweiterung sehr konservativ und erklärt viele Paare von Mengen für unvergleichbar. Deshalb wurden im Laufe der Zeit einige Verfeinerungen der Kelly-Erweiterung vorgeschlagen. Für jede gegebene Mengenerweiterung kann man nun einen entsprechenden Manipulationsbegriff definieren. Demnach ist ein Wahlverfahren manipulierbar, falls ein Wähler durch falsche Angabe seiner Präferenzen eine Gewinnermenge erreichen kann, die er bzgl. der Mengenerweiterung gegenüber der ursprünglichen Gewinnermenge bevorzugt.

In meiner Arbeit untersuche ich die Manipulierbarkeit von mengenwertigen Wahlverfahren bzgl. der Fishburn-Erweiterung und bzgl. der Gärdenfors-Erweiterung. Da beides Verfeinerungen der Kelly-Erweiterung sind, kommen nur solche Wahlverfahren als nicht-manipulierbar in Betracht, die auch bzgl. der Kelly-Erweiterung nicht manipulierbar sind. Für jedes dieser Wahlverfahren beweise ich entweder die Nicht-Manipulierbarkeit oder gebe ein konkretes Manipulationsbeispiel an. Das Besondere an meiner Vorgehensweise ist dabei, dass ich nicht jedes Wahlverfahren einzeln untersuche. Vielmehr definiere ich eine Reihe von abstrakten Eigenschaften, die – falls erfüllt – die Nicht-Manipulierbarkeit garantieren. Neben diesen hinreichenden Bedingungen identifiziere ich auch notwendige Bedingungen für die Nicht-Manipulierbarkeit. Die Bedingungen erlauben es mir, für sämtliche interessanten Verfahren die Manipulierbarkeit zu entscheiden.

4 Turnierlösungen

Ein Turnier ist ein gerichteter Graph, in dem es zwischen je zwei Knoten genau eine gerichtete Kante gibt. Eine *Turnierlösung* ist eine Funktion, die jedem Turnier eine Teilmenge seiner Knoten zuordnet. Turniere und Turnierlösungen können sowohl gewichtet als auch ungewichtet sein. Turnierlösungen spielen eine wichtige Rolle in der Social-Choice-Theorie, da viele Wahlverfahren als (gewichtete oder ungewichtete) Turnierlösung interpretiert werden können. Das liegt daran, das viele Wahlverfahren, wie beispielsweise Ranked Pairs (Abschnitt 3.1), über paarweise Vergleiche von Alternativen definiert sind. Für die Gewinnerbestimmung solcher Verfahren genügt es daher, den gewichteten Mehrheitsgraphen (Abb. 3) zu kennen. Manche Wahlverfahren benötigen nicht einmal die Kantengewichte und operieren lediglich auf der (ungewichteten) Mehrheitsrelation. Letztere Verfahren sind damit im Wesentlichen äquivalent zu ungewichteten Turnierlösungen. Turnierlösungen haben auch Anwendungen, die über Wahlverfahren hinausgehen. Sie können immer dann eingesetzt werden, wenn aufgrund von paarweisen Vergleichen die beste Alternative ausgewählt werden soll. Paradebeispiele sind Sportligen, in denen jede Mannschaft gegen jede andere antritt und die Resultate dieser paarweisen Vergleiche am Ende in Form eines Rankings aggregiert werden müssen.

4.1 Gewinnerbestimmung bei unvollständigen Informationen

Oft kommt es vor, dass nur lückenhafte Informationen über die paarweisen Vergleiche innerhalb eines Turniers vorliegen, etwa weil einige Wähler noch nicht abgestimmt haben oder weil bestimmte Spiele einer Sportliga noch nicht ausgetragen wurden. In solchen Fällen ist es naheliegend, sich darüber Gedanken zu machen, welche Alternativen am Ende gewinnen werden. Zu diesem Zweck betrachtet man alle möglichen Vervollständigungen eines unvollständig spezifizierten Turniers und definiert *mögliche Gewinner* als diejenigen Alternativen, die in mindestens einer Vervollständigung ausgewählt werden. Eine Alternative ist darüberhinaus ein *notwendiger Gewinner*, falls sie in *allen* Vervollständigungen ausgewählt wird.

In meiner Arbeit untersuche ich die Berechnungskomplexität von möglichen und notwendigen Gewinnern für eine Reihe von gängigen gewichteten und ungewichteten Turnierlösungen. Die Ergebnisse reichen von einfachen Greedy Algorithmen (z. B. für die Turnierlösungen *Copeland* und *Top Cycle*) über nicht-triviale kombinatorische Algorithmen (*Maximin* und *Borda*) bis hin zu interessanten Härteresultaten (*Ranked Pairs* und *Uncovered Set*).

4.2 Minimale retentive Mengen

Thomas Schwartz hat einen Operator auf Turnierlösungen eingeführt, der kooperative Mehrheitsentscheidungen innerhalb eines Komitees modelliert. Für eine gegebene Tur-

nierlösung S wählt die Turnierlösung $\mathring{S}$ die Vereinigung aller inklusions-minimalen S-*retentiven* Mengen. S-Retentivität ist eine natürliche Stabilitätseigenschaft für Teilmengen von Alternativen. Schwartz hat den $\circ$-Operator benutzt, um die Turnierlösung *Tournament Equilibrium Set (*TEQ*)* rekursiv zu definieren: $TEQ = \mathring{TE}Q$.

In meiner Arbeit betrachte ich die Auswirkungen des $\circ$-Operators auf beliebige ungewichtete Turnierlösungen. Insbesondere zeige ich, unter welchen Umständen attraktive axiomatische Eigenschaften von S auf $\mathring{S}$ „vererbt“ werden. Durch die wiederholte Anwendung des $\circ$-Operators erhält man Sequenzen von attraktiven und effizient berechenbaren Turnierlösungen, die gegen TEQ konvergieren. Da die Berechnung von TEQ NP-schwer ist, sind diese Sequenzen besonders interessant, um TEQ mit einem Anytime-Algorithmus zu „approximieren“. Schließlich stelle ich mit $\mathring{TC}$ eine neue Turnierlösung vor, die alle gängigen wünschenswerten Eigenschaften erfüllt und effizient berechnet werden kann.

Danksagung Ich danke meinen Koautoren Haris Aziz, Felix Brandt, Felix Fischer, Paul Harrenstein, Edith Hemaspaandra, Lane Hemaspaandra, Jan Hoffmann, Jérôme Lang und Hans Georg Seedig. Meine Arbeit wurde von der Deutschen Forschungsgemeinschaft (Projekte BR-2312/6-1 und BR 2312/10-1) unterstützt.

Literatur

[Bri12] M. Brill. *Set-Valued Solution Concepts in Social Choice and Game Theory: Axiomatic and Computational Aspects*. Dissertation, Technische Universität München, 2012.

[Con10] V. Conitzer. Making Decisions Based on the Preferences of Multiple Agents. *Communications of the ACM*, 53(3):84–94, 2010.

[FHH10] P. Faliszewski, E. Hemaspaandra und L. Hemaspaandra. Using Complexity to Protect Elections. *Communications of the ACM*, 53(11):74–82, 2010.

[Rou10] T. Roughgarden. Algorithmic Game Theory. *Communications of the ACM*, 53(7):78–86, 2010.

[Tid87] T. N. Tideman. Independence of Clones as a Criterion for Voting Rules. *Social Choice and Welfare*, 4(3):185–206, 1987.



Markus Brill wurde am 10. März 1984 in Neustadt an der Weinstraße geboren. Er studierte Mathematik mit Nebenfach Informatik an der TU Kaiserlautern, der ETH Zürich und der TU München, wo er Mitglied im Elitestudiengang *TopMath* war. Seine Promotion erfolgte an der LMU München und der TU München im Rahmen des durch die European Science Foundation koordinierten Projekts *Computational Foundations of Social Choice*. Während dieser Zeit verbrachte er zwei Monate als Gastwissenschaftler an der École Polytechnique in Paris. Seine Arbeiten wurden in zahlreichen internationalen Journalen und Tagungsbänden veröffentlicht. Im September 2013 tritt er ein Feodor-Lynen-Forschungsstipendium an der Duke University an.

Branchenspezifische IT-Innovationssysteme: Von der Analyse zur Intervention - Am Beispiel des IT-Innovationssystems für Krankenhäuser in Deutschland

Paul Drews

Fachbereich Informatik
Universität Hamburg
drews@informatik.uni-hamburg.de

Abstract: Bisher hat sich die Analyse der Entstehung und Aneignung von IT-Innovationen vor allem auf die Ebene der Organisationen und auf den Vergleich von nationalen Innovationssystemen konzentriert. Das Ergebnis dieser Arbeit ist ein integrierter Analyse- und Interventionsansatz für branchenspezifische IT-Innovationssysteme. Der Ansatz besteht aus einem theoretisch-konzeptuellen Rahmen und einem methodischen Rahmen, die jeweils sowohl die aus der Literatur als auch die aus dem empirischen Teil der Arbeit abgeleiteten Erkenntnisse berücksichtigen. Gegenstand der empirischen Untersuchung ist das IT-Innovationssystem für Krankenhäuser in Deutschland. Die bei der Analyse dieses Systems identifizierten Interventionspotenziale und Handlungsempfehlungen dienten als Ausgangspunkt für ein aktionsforschungsorientiertes Beratungsprojekt. In diesem Projekt konnten neue Strukturen für den Austausch von IT-Innovationen, die lokal in Krankenhäusern entwickelt werden, geschaffen werden.

1 Einleitung

Innovationen gelten als Königsweg, um aktuelle und zukünftige Probleme in der Gesellschaft zu lösen. Der Informationstechnik (IT) kommt dabei als einem zentralen Innovationsfeld große Bedeutung zu. Die Einführung und Nutzung von IT-Innovationen in Organisationen hat viele Branchen erheblich verändert. Bisher hat sich die Analyse der Entstehung und Aneignung von IT-Innovationen vor allem auf die Ebene der Organisationen und auf den Vergleich von nationalen Innovationssystemen konzentriert. In dieser Arbeit wird der Frage nachgegangen, wie branchenspezifische IT-Innovationssysteme, die zwischen den beiden zuvor genannten Ebenen zu verorten sind, analysiert werden können. Eine systematische Analyse von branchenspezifischen IT-Innovationssystemen soll dazu beitragen, dieses bedeutende gesellschaftliche Innovationsfeld besser zu verstehen. Zusätzlich sollen Wege aufgezeigt werden, wie die Ergebnisse einer Analyse für die Intervention in ein branchenspezifisches IT-Innovationssystem genutzt werden können.

In der Informatik und Wirtschaftsinformatik wurden Innovationen bisher primär aus einer technischen und intra-organisationalen Sicht betrachtet, ihr Kontext wurde hingegen zu wenig berücksichtigt [u. a. AM04]. In anderen Disziplinen wird dieser

Kontext als nationales, branchenspezifisches oder regionales Innovationssystem explizit als Untersuchungsgegenstand behandelt [u. a. BM97, Ed05]. Branchenspezifische Innovationssysteme für IT wurden bisher lediglich aus Sicht der IT-Hersteller untersucht [u. a. St04]. Die bisherigen Arbeiten zu branchenspezifischen Innovationssystemen beschränken sich weitgehend auf die Analyse, einige Arbeiten liefern darüber hinaus Empfehlungen für die Politik. Die Umsetzung dieser Empfehlungen und der Eingriff in die Innovationssysteme werden nicht betrachtet. Ausgehend von diesem Forschungsdefizit kann folgende Hauptfragestellung (FS1) abgeleitet werden:

Wie können die Analyse von branchenspezifischen IT-Innovationssystemen, die Ableitung von Handlungsempfehlungen und die Intervention in diese Systeme theoretisch-konzeptuell und methodisch geleitet werden?

In dieser Arbeit wird ein konkretes branchenspezifisches IT-Innovationssystem empirisch untersucht, um den theoretisch-konzeptuellen Rahmen mithilfe der Ergebnisse dieser Untersuchung weiterzuentwickeln. Aufgrund seiner gesellschaftlichen Relevanz und der oft beschriebenen Rückständigkeit im Vergleich zu anderen Branchen [EC07] wurde das IT-Innovationssystem für Krankenhäuser in Deutschland ausgewählt. Eine umfangreiche Beschreibung dieses IT-Innovationssystems existiert bisher nicht. Für den empirischen Fall ergeben sich die folgenden Fragestellungen:

FS2: Wie werden IT-Innovationen im IT-Innovationssystem für Krankenhäuser in Deutschland entwickelt und zur Anwendung gebracht?

FS3: Wie können aus den Analyseergebnissen zum IT-Innovationssystem für Krankenhäuser in Deutschland Handlungsempfehlungen abgeleitet und im Rahmen einer Intervention umgesetzt werden?

Die Fragestellungen dieser Arbeit können innerhalb der Informatik in den Bereich der angewandten Informatik eingeordnet werden. Dort sind insbesondere die Wirtschaftsinformatik (bzw. Information Systems) und – für das exemplarisch betrachtete IT-Innovationssystem – die Medizininformatik relevante Teildisziplinen. Die Innovationsforschung ist keine etablierte Disziplin, sie ist ein interdisziplinäres Forschungsgebiet [Ro03], zu der es neben originär interdisziplinären Arbeiten [Ro03, Va99] Beiträge aus zahlreichen Disziplinen gibt. Zusätzlich sind die Bezüge zur Innovationsforschung in der Wirtschaftswissenschaft, den Sozialwissenschaften und der Psychologie zu berücksichtigen. Um zu den für die angewandte Informatik relevanten Ergebnissen zu gelangen, können die Konzepte des Mikropolis-Modells (siehe unten) sowie Ergebnisse der interdisziplinären Innovationsforschung und der Techniksoziologie als theoretische Grundlage verwendet werden. Diese Form der disziplinübergreifenden und an einer auch für die Praxis relevanten Fragestellung ausgerichteten Forschung wird als transdisziplinär bezeichnet [Gi94, Mi03]. Für die transdisziplinäre Forschung ist die Problemstellung und nicht die disziplinäre oder theoretische Reinheit der Forschung konstituierend, da diese nicht mehr oder nur unvollständig gewährleistet werden können. Für die transdisziplinäre Forschung bietet das Mikropolis-Modell (MM) einen Orientierungsrahmen aus der Sicht der Informatik an [La08, Ro08]. Das MM stellt für die Forschung über die Zusammenhänge von Informationstechnik in Organisationen und

Gesellschaft eine Reihe analytischer Konzepte bereit, beschreibt ihre Zusammenhänge und zeigt Wege zur Gestaltung auf [Kr06]. Da das MM eine zentrale theoretische Grundlage darstellt, ist ergänzend die Fragestellung FS4 zu stellen: Welche Konsequenzen ergeben sich aus den zuvor gewonnenen Erkenntnissen für das Mikropolis-Modell?

2 Eingrenzung und theoretisch-konzeptueller Rahmen

Die Eingrenzung des Untersuchungsgegenstandes dieser Arbeit erfolgt über Edquists Definition des Innovationssystems [Ed05], einer anwendungsorientierten Branchendefinition sowie einer zuvor entwickelten Definition für IT-Innovationen: Ein branchenspezifisches IT-Innovationssystem umfasst die (sozialen, ökonomischen, technischen und institutionellen) Rahmenbedingungen für die IT-Innovationsprozesse in einer Branche. Eine Branche wird dabei als eine Gruppe von Unternehmen und Organisationen verstanden, die nah verwandte Produkte oder Dienstleistungen anbieten und im IT-Innovationssystem als Anwendungskontext für IT in Erscheinung treten.

Für den Entwurf eines theoretisch-konzeptuellen Rahmens werden die grundlegende Struktur und die Kernkonzepte des Mikropolis-Modells mit den Kernkonzepten des allgemeinen Systems of Innovation-Ansatzes und weiteren Konzepten aus der Innovationsforschung zusammengeführt. Das Ergebnis ist eine Grundstruktur des Analyserahmens für branchenspezifische IT-Innovationssysteme. Dieser Rahmen konkretisiert IT-Innovationssysteme mithilfe der Konzepte Akteur, Innovationsaktivitäten und Innovationsprozesse. Zusätzlich stellt er eine Beziehung zur Umgebung, dem Makrokontext, her und bietet drei Perspektiven, mit deren Hilfe ein tieferes Verständnis über IT-Innovationssysteme erlangt werden kann: die soziotechnische Perspektive, die normativ-kritische Perspektive und die historische Perspektive der Innovationspfade. Diese Konzepte werden durch Teilkonzepte konkretisiert und ihre Zusammenhänge werden aufgezeigt. Der entwickelte Rahmen fließt als wesentliche Quelle zur Erhöhung der theoretischen Sensibilität [SC96] in die empirischen Untersuchungen ein und soll den Blick möglichst zielsicher auf die wesentlichen Strukturen und Aktivitäten lenken, ohne eine zu starre Struktur für die empirische Untersuchung vorzugeben.

3 Methodenrahmen für Analyse und Intervention

Der Methodenrahmen für den empirischen Teil der Arbeit besteht aus einer Kombination der Grounded Theory (für den analytischen Teil) und der Aktionsforschung (für die Intervention). Als Forschungsmethode für den empirisch-analytischen Teil der Arbeit wurde Grounded Theory (GT) nach Strauss und Corbin [CS08, SC96] ausgewählt, da sich der entwickelte Analyserahmen in einem frühen Stadium befindet. Die GT nach Strauss und Corbin ermöglicht es, diesen Rahmen für die Erhöhung der theoretischen Sensibilität zu nutzen, gleichzeitig aber primär induktiv eine Theorie über das jeweilige IT-Innovationssystem zu entwickeln. Auf diese Weise ist gewährleistet, dass auch neue

Konzepte und Kategorien entwickelt werden können, die im Anschluss zur Erweiterung oder Ergänzung des Analyserahmens verwendet werden können. Gegenüber der GT nach Glaser zeichnet sich die GT nach Strauss und Corbin auch dadurch aus, dass sie zahlreiche analytische Werkzeuge für die Datenauswertung bereitstellt.

Im Rahmen dieser Arbeit soll das fokale branchenspezifische IT-Innovationssystem nicht nur beschrieben und analysiert werden. Es sollen auch Handlungsempfehlungen abgeleitet und eine gezielte Intervention auf der Grundlage der Analyseergebnisse durchgeführt werden. An dieser Stelle sei kurz auf die Verwendung des Interventionsbegriffs eingegangen: In der Informatik und Wirtschaftsinformatik ist man daran gewöhnt, gestalten zu können, beispielsweise in der Softwareentwicklung. Bei der Einführung von IT-Innovationen in Organisationen wird der Gestaltungsspielraum kleiner, wie u. a. Organisationstheorie und -entwicklung verdeutlichen. Diese bereits bei intra-organisationalen Veränderungen bestehende Limitation wird auf der Ebene branchenspezifischer IT-Innovationssysteme weiter reduziert. Betrachtet man unter Berücksichtigung der Erkenntnisse aus der Systemtheorie diese Systeme als komplexe Systeme, so wird deutlich, dass Eigenschaften wie nicht-lineare Vernetzung, unerwartet träge bzw. starke Reaktion auf Eingriffe und eine kontra-intuitive Zeitdynamik [Fo71, Wi99] die Gestaltungsmöglichkeiten stark begrenzen. Es ist eher von der "Unwahrscheinlichkeit gelingender Interventionen" [Wi99, S. 4] und dem "Scheitern trivialisierender Strategien der Veränderung" [ebd.] auszugehen. Die Arbeit verwendet daher anstatt des in der Informatik und Wirtschaftsinformatik üblichen Gestaltungsbegriffs den Terminus Intervention, der als gezielter Versuch eines verändernden Eingriffs in ein komplexes System (hier: branchenspezifisches IT-Innovationssystem) mit unsicherem Ergebnis verstanden wird.

Für die im empirischen Teil der Arbeit vorgenommene Intervention wird die Aktionsforschung als methodische Grundlage genutzt, da der Autor diesen Eingriff selbst initiierte und begleitete. Die Aktionsforschung ist in der IS-Forschung eine etablierte Methode für die Untersuchung der Einführung neuer Technologien in Organisationen [Ba99, De05]. Die Verwendung der Methode weicht in dieser Arbeit von diesem klassischen Anwendungsgebiet der IS-Forschung dahingehend ab, dass nicht eine einzelne IT-Innovation und ihre Einführung in einer Organisation betrachtet werden, sondern ein Eingriff, der darauf abzielt, die Strukturen von Innovationsprozessen auf einer Meta-Ebene zu verändern.

4 Vorgehen bei der Datenerhebung und -auswertung

Die Erhebung und die Analyse von Daten wurden entsprechend der Vorgaben der Grounded Theory (GT) durchgeführt [CS08, SC96]. Die aus Experteninterviews und anderen Quellen stammenden Daten wurden aufbereitet und kodiert. Im Anschluss an die Kodierung wurden die Kodes überarbeitet und kategorisiert. Zu den erarbeiteten Konzepten und Kategorien wurden Memos verfasst. Kodes und Kategorien flossen in die Planung der weiteren Datenerhebung ein. Der Prozess der Datenerhebung und -auswertung ist in Abbildung 1 überblicksartig dargestellt.

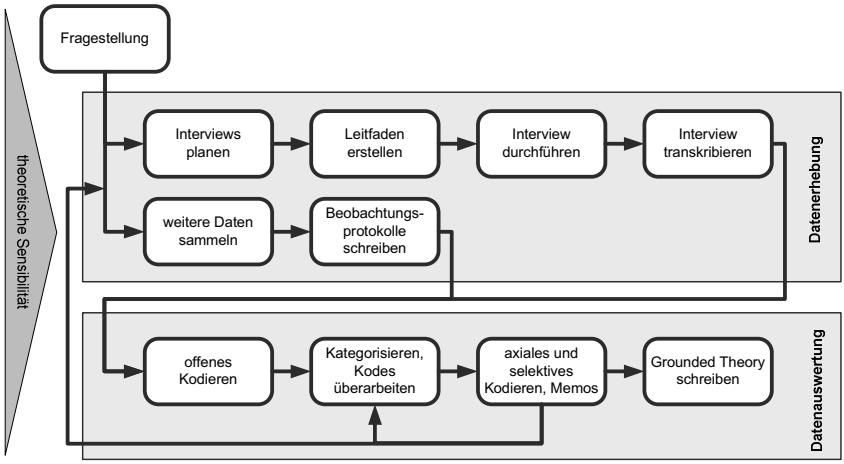


Abbildung 1 - Überblick über den empirisch-analytischen Forschungsprozess

Die Erhebung des empirischen Materials fand in der Zeit von Juli 2006 bis Juni 2011 statt. Den Kern des erhobenen Datenmaterials bilden die Abschriften von 16 Interviews (insgesamt 369 Seiten) sowie 18 Beobachtungsprotokolle (u. a. zu Tagungen, Messen und Workshops). Neben den Interviews wurden über 1700 elektronische Dokumente sowie weitere Materialien in Papierform ausgewertet. Die Interviews dienten als Hauptdatenquelle in dieser Arbeit. Sie wurden als halbstrukturierte, qualitative Experteninterviews [FL03] jeweils auf der Grundlage eines Leitfadens durchgeführt. Die Auswahl von Datenquellen orientierte sich an dem Konzept des theoretischen Samplings der GT [CS08, SC96]. Die Datenauswertung stützte sich auf die Verfahren der GT nach Strauss und Corbin (u. a. ständiges Vergleichen, dreistufiges Kodierverfahren, Nutzung paradigmatisches Modell). Die Auswertung der Daten wurde durch die Software Atlas.ti unterstützt. Dabei wurden 4902 Kodierungen auf der Basis von 438 Kodes vorgenommen.

5 Das IT-Innovationssystem für Krankenhäuser in Deutschland

Die Ergebnisse der empirischen Untersuchung des IT-Innovationssystems für Krankenhäuser in Deutschland werden entlang von drei miteinander verbundenen Kernkonzepten beschrieben. Ausgangspunkt ist das Konzept des IT-Innovationssystems. Es bietet eine umfassende, aber statische Sicht auf die Strukturen des betrachteten branchenspezifischen IT-Innovationssystems. Die Dynamik in diesem System wird durch das Konzept des IT-Innovationsprojektes beschrieben. IT-Innovationen werden in IT-Innovationsprojekten entwickelt und zur Anwendung gebracht. Das neu entwickelte Konzept der IT-Innovationsmuster verbindet die Dynamik von IT-Innovationsprojekten mit den Strukturen des IT-Innovationssystems und abstrahiert von einzelnen Projekten und IT-Innovationen durch die Bildung von Invarianten und Varianten. Ergänzend zu diesen drei Konzepten werden im Sinne einer Schwachstellenanalyse 19 Interventionspotenziale identifiziert und 9 Handlungsempfehlungen entwickelt.

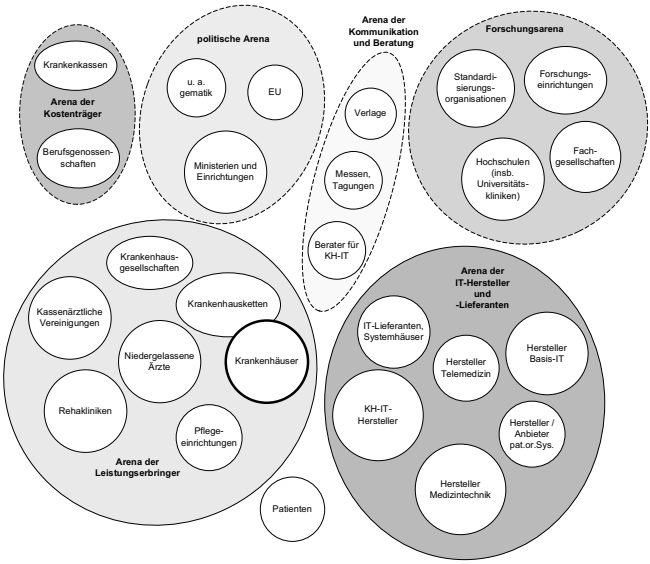


Abbildung 2 - Akteure und Arenen im IT-Innovationssystem für Krankenhäuser in Deutschland

Als Auszug aus der mehr als 120 Seiten umfassenden Beschreibung des IT-Innovationssystems sind im Folgenden exemplarisch drei Teilergebnisse angeführt. Bei der Beschreibung des IT-Innovationssystems wurde unter anderem eine Karte wesentlicher Akteure und Arenen erstellt (vgl. Abbildung 2). Die vielfältigen in diesem IT-Innovationssystem ablaufenden IT-Innovationsprojekte wurden zu neun IT-Innovationsmustern zusammengefasst (vgl. Abbildung 3, dort gemeinsam mit den Innovationstreibern dargestellt). Als Beispiel sei hier das für die im Folgenden beschriebene Intervention relevante IT-Innovationsmuster der lokalen IT-Innovation genannt. Dieses beschreibt Innovationsaktivitäten in den Krankenhäusern, bei denen diese selbst IT-Innovationen entwickeln. Oft geschieht dies aus einer Notsituation heraus, da die IT-Hersteller keine geeigneten Lösungen für ein Problem anbieten. Bezüglich dieses IT-Innovationsmusters konnte ein Innovationspotenzial identifiziert werden: Diese lokalen IT-Innovationen sind nur selten bzw. nur wenigen Personen außerhalb ihres Entstehungskontextes bekannt. Eine der entwickelten Handlungsempfehlungen sieht daher vor, den Austausch von Informationen über diese lokalen IT-Innovationen zu fördern, damit sie in Entwicklungsprozessen bei den Herstellern berücksichtigt werden und in anderen Krankenhäusern eingesetzt werden können.

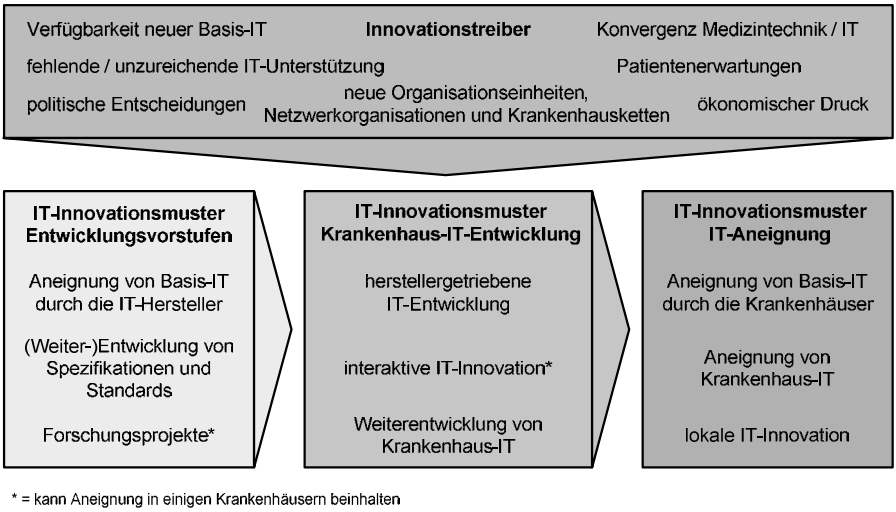


Abbildung 3 - Innovationstreiber und Innovationsmuster für branchenspezifische IT-Innovationsmuster

6 Intervention in einem Beratungsprojekt zu lokalen IT-Innovationen

Ausgehend von der oben beschriebenen Handlungsempfehlung und auf der Grundlage von Konzepten des theoretisch-konzeptuellen Rahmens (insb. Lead Users, Not-Invented-Here-Syndrom und Free Revealing) wurde ein aktionsforschungsorientiertes Beratungsprojekt zu lokalen IT-Innovationen durchgeführt. In der ersten Phase des Projektes wurde ein Innovationsworkshop auf dem Referenzkundentreffen eines führenden Krankenhaus-IT-Herstellers durchgeführt. Das Beratungsprojekt zeichnete sich durch eine aktive Beteiligung des IT-Herstellers und der führenden Anwender seiner Produkte aus. Es wurde deutlich, dass zahlreiche lokale IT-Innovationen in den Krankenhäusern existieren, der Austausch über diese bisher jedoch nicht organisiert war. Die Krankenhäuser forderten den IT-Hersteller auf, diesen Austausch zu organisieren. In der zweiten Phase des Projektes konnten die strukturellen Voraussetzungen für eine Institutionalisierung des Informationsaustausches über lokale IT-Innovationen beim IT-Hersteller geschaffen werden. Der IT-Hersteller schuf eine Stelle für das Management lokaler IT-Innovationen und damit die Voraussetzung für einen organisierten Informationsaustausch. Die vom IT-Hersteller eingestellte Person erhob und dokumentierte insgesamt 50 lokale IT-Innovationen. Auf dem zweiten Workshop wurde das neue Organisationskonzept vorgestellt und mit den Vertretern der Krankenhäuser und des IT-Herstellers diskutiert. Die beiden durchgeführten Workshops erhielten ein Evaluationsergebnis von 1,5 bzw. 1,25 (1= sehr gut, 5 = schlecht).

7 Ein Analyse- und Interventionsansatz für branchenspezifische IT-Innovationssysteme

Als Antwort auf die Hauptfragestellung der Arbeit wurde ein integrierter Analyse- und Interventionsansatz für branchenspezifische IT-Innovationssysteme entwickelt. Dieser besteht aus einem theoretisch-konzeptuellen Rahmen, der auf der Grundlage des aus der Literatur abgeleiteten Entwurfs und einer Reflexion der bei der Auswertung der empirischen Daten entwickelten Konzepte entwickelt wurde. Der methodische Rahmen des Analyse- und Interventionsansatzes für branchenspezifische IT-Innovationssysteme (vgl. Abbildung 4) basiert auf einer Reflexion der Gesamtkonzeption der vorliegenden Arbeit einerseits und der Anwendung der ausgewählten Methoden andererseits. Bisher existierte kein integrierter Ansatz für die Analyse von branchenspezifischen IT-Innovationssystemen, der gleichzeitig auch Wege zur Intervention aufzeigt. Während die Literatur zur Erforschung von Innovationssystemen zwar Grundbegriffe und Konzepte für eine Analyse liefert, fehlen diesen Ansätzen sowohl IT-spezifische Konzepte als auch methodische Ausführungen, die über eine Nutzung der grundlegenden Konzepte zur Strukturierung der Analyse hinausgehen [BM97, Ed05].

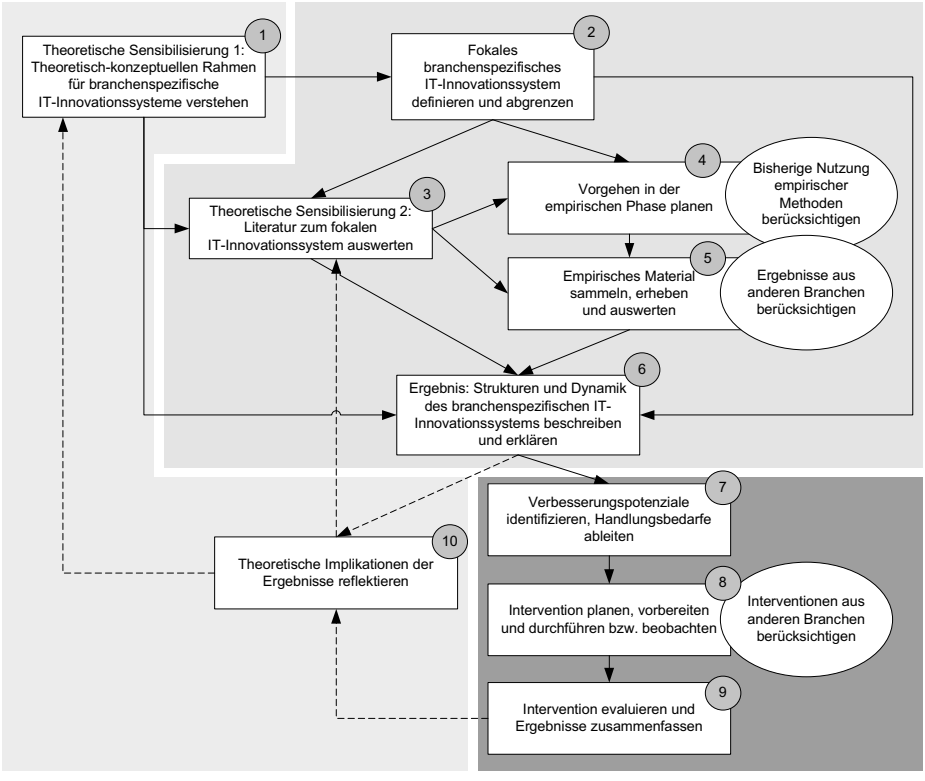


Abbildung 4 - Methodischer Ansatz für die Analyse von und Intervention in branchenspezifische IT-Innovationssysteme

Das Mikropolis-Modell wiederum bietet Konzepte für die Analyse von IT-Innovationen im gesellschaftlichen und organisatorischen Kontext, berücksichtigt bisher aber die Erkenntnisse der Innovationsforschung zu wenig und bleibt bei der Ausgestaltung des Übergangs von der Analyse zur Intervention vage [La08, Ro08]. Der hier vorgestellte Ansatz berücksichtigt bei diesem Übergang, dass Akteure nur begrenzten Einfluss auf die Strukturen in branchenspezifischen IT-Innovationssystemen nehmen können.

8 Zusammenfassung

Um der Bedeutung, die IT-Innovationen von Gesellschaft und Wirtschaft zugeschrieben werden, aus Sicht der Informatik angemessen begegnen zu können, ist nicht nur die Entwicklung von IT-Innovationen erforderlich. Es ist auch Forschung notwendig, die sich der Analyse, dem Verstehen und der Verbesserung des Kontextes widmet. In dieser Arbeit wurde ein integrierter Analyse- und Interventionsansatz für branchenspezifische IT-Innovationssysteme entwickelt, der sich auf etablierte Konzepte der Innovationsforschung stützt, diese jedoch zu einem neuen Rahmen zusammenführt (Ergebnis zu FS1). Durch die Verbindung von Grounded Theory und Aktionsforschung sowie auf der Grundlage des Interventionsbegriffs wurde ein methodischer Rahmen entwickelt, der eine umfangreiche Analyse branchenspezifischer IT-Innovationssysteme und eine gut informierte Intervention leiten kann. Der theoretisch-konzeptuelle Rahmen und der methodische Rahmen konnten mithilfe der bei ihrer Anwendung gewonnenen Erkenntnisse weiterentwickelt werden. Neben diesem Hauptergebnis konnte eine umfangreiche Beschreibung des IT-Innovationssystems für Krankenhäuser in Deutschland erstellt werden (Ergebnis zu FS2). Auf dem Weg zu dieser Beschreibung wurden neue Konzepte wie die IT-Innovationsmuster entwickelt. Aus den identifizierten Innovationspotenzialen und Handlungsempfehlungen wurde der fehlende Informationsaustausch über lokale IT-Innovationen als Ausgangspunkt für ein Interventionsprojekt gewählt. In diesem Projekt konnte gemeinsam mit den beteiligten Krankenhäusern und einem IT-Hersteller erfolgreich eine neue Institution etabliert werden (Ergebnis zu FS3). Dies zeigt, dass die bei der Analyse gewonnenen Erkenntnisse für eine Umsetzung in der Praxis geeignet sind. Ferner konnten aus den Ergebnissen Vorschläge zur Weiterentwicklung des Mikropolis-Modells abgeleitet werden (Ergebnis zu FS4).

Literaturverzeichnis

[AM04] Avgerou, C.; Madon, S.: Framing IS Studies - Understanding the Social Context of IS Innovation. In (Avgerou, C. et al., Hrsg.): The Social Study of Information and Communication Technology - Innovation, Actors and Contexts, Oxford University Press, New York; S. 162-182.

[Ba99] Baskerville, R.L.: Investigating Information Systems with Action Research. Communications of the Association for Information Systems, 2 (Article 19), 1999.

[BM97] Breschi, S.; Malerba, F.: Sectoral Systems of Innovation - Technological Regimes, Schumpeterian Dynamics and Spatial Boundaries. In (Edquist, C., Hrsg.): Systems of Innovation. Frances Pinter, London, 1997; S. 130-150.

[CS08] Corbin, J.M.; Strauss, A.L.: Basics of qualitative research – techniques and procedures for developing grounded theory, Sage Publications, Los Angeles, 2008.

[De05] de Villiers, M.R.: Three Approaches as Pillars for Interpretive Information Systems Research. Proceedings of the Annual Research Conference of the South African Institute of Computer Scientists (SAICSIT 2005), White River, 2005.

[Dr12] Drews, P.: Branchenspezifische IT-Innovationssysteme: Von der Analyse zur Intervention - Am Beispiel des IT-Innovationssystems für Krankenhäuser in Deutschland. Dissertation, Fachbereich Informatik, Universität Hamburg. http://ediss.sub.uni-hamburg.de/volltexte/2012/5539/, zuletzt abgerufen am 03.06.2013.

[EC07] European Commission: eHealth Priorities and Strategies in European Countries, Office for Official Publications of the European Communities, Luxembourg, 2007.

[Ed05] Edquist, C.: Systems of innovation – perspectives and challenges. In (Fagerberg, J. et al., Hrsg.): The Oxford Handbook of Innovation. Oxford University Press, New York, 2005; S. 181-208.

[FL03] Froschauer, U.; Lueger, M.: Das qualitative Interview, WUV-Universitätsverlag, Wien, 2003.

[Fo71] Forrester, J.: Planung unter dem Einfluß komplexer sozialer Systeme. In (Ronge, V.; Schmieg, G., Hrsg.): Politische Planung in Theorie und Praxis. Piper, München, 1971; S. 81-91.

[Gi94] Gibbons, M. et al.: The New Production of Knowledge - The Dynamics of Science and Research in Contemporary Societies, Sage Publications, London, 1994.

[Kr06] Krause, D. et al.: Wissen, wie alles zusammenhängt. Das Mikropolis-Modell als Orientierungswerkzeug für die Gestaltung von Informationstechnik in Organisationen und Gesellschaft. Informatik Spektrum 29 (4), S. 263-273.

[La08] Langer, R. et al.: Soziotechnische Systeme und ihre transdisziplinäre Erforschung - Eine Skizze. In (D. Gumm et al., Hrsg.): Mensch - Technik - Ärger?, Lit-Verlag, Berlin; S. 177-205.

[Mi03] Mittelstraß, J.: Transdisziplinarität - wissenschaftliche Zukunft und institutionelle Wirklichkeit, UVK Universitätsverlag Konstanz, Konstanz, 2003.

[Ro03] Rogers, E.M.: Diffusion of Innovations (Fifth Edition), Free Press, New York, 2003.

[Ro08] Rolf, A.: Mikropolis 2010 - Menschen, Computer, Internet in der globalen Gesellschaft, Metropolis, Marburg, 2008.

[SC96] Strauss, A.L.; Corbin, J.M.: Grounded Theory: Grundlagen qualitativer Sozialforschung, Psychologie Verlags Union, Weinheim, 1996.

[St04] Steinmueller, W.E.: The European Software Sectoral System of Innovation. In (Malerba, F., Hrsg.): Sectoral Systems of Innovation - Concepts, Issues and Analyses of Six Major Sectors in Europe. Cambridge University Press, Cambridge, 2004; S. 193-242.

[Va99] van de Ven, A.H. et al.: The Innovation Journey, Oxford University Press, New York, 1999.

[Wi99] Willke, H.: Systemtheorie II - Interventionstheorie (3. Auflage), Lucius & Lucius, Stuttgart, 1999.



Paul Drews ist derzeit als PostDoc am Arbeitsbereich ITG des Fachbereichs Informatik der Universität Hamburg tätig. Von 2008 bis 2012 arbeitete er dort am Arbeitsbereich ASI bei Prof. Dr. Arno Rolf als wissenschaftlicher Mitarbeiter. Sein 2006 begonnenes Promotionsvorhaben schloss er 2012 mit Auszeichnung ab. Zuvor studierte er von 1998 bis 2004 Wirtschaftsinformatik an der Universität Hamburg. Von 1998 bis 2011 arbeitete er als selbständiger Berater für IT im Gesundheitswesen. Zu seinen Forschungsinteressen gehören die Themen IT-Innovationsmanagement, IT-Consulting, Enterprise Architecture Management sowie IT-Governance und IT im Gesundheitswesen.

Computationale Aspekte der Abstrakten Argumentation*

Wolfgang Dvořák

Universtät Wien, Fakultät für Informatik
wolfgang.dvorak@univie.ac.at

Abstract: Diese Arbeit studiert *Abstract Argumentation Frameworks*, einen der erfolgreichsten Formalismen in der Formalen Argumentation, einem Teilgebiet der Künstlichen Intelligenz. Diese Frameworks abstrahieren von den konkreten Argumenten und ihren Inhalten zu abstrakten Entitäten und einer Konfliktrelation zwischen diesen. Auf Basis der Konfliktrelation werden nun kohärente Mengen von Argumenten identifiziert. Die Literatur kennt eine Vielzahl an unterschiedlichen Kriterien, sogenannte Semantiken, um kohärente Mengen zu definieren. Die Berechnung dieser kohärenten Mengen ist eine Kernaufgabe von Argumentations-Systemen weshalb sich diese Arbeit der computationalen Analyse dieses Schrittes widmet. Konkret präsentieren wir eine klassische *Komplexitätsanalyse* der verschieden Semantiken und studieren mögliche *tractable fragments*, d.h. wir betrachten Abstract Argumentation Frameworks mit einer bestimmte Struktur und untersuchen, ob diese mit geringerem Berechnungsaufwand ausgewertet werden können. Die erzielten Resultate nutzen wir abschließend auch um effiziente *Übersetzbarkeit* zwischen den verschiedenen Semantiken für Abstract Argumentation Frameworks zu studieren. Solche Übersetzungen erlauben die Nutzung eines effizienten Argumentations-Systems für eine Semantik A auch für andere Semantiken, die in Semantik A übersetzt werden können. Diese Untersuchungen bilden gemeinsam die Grundlage für das Design effizienter Argumentations-Systeme, welche eine breite Auswahl an Semantiken bereitstellen sollen.

1 Motivation

Ausgehend von Phan Minh Dungs wegweisender Arbeit [Dun95] hat sich das Forschungsgebiet der Argumentation zu einem der aktivsten in der Künstlichen Intelligenz (KI) entwickelt. Alle großen KI Konferenzen listen heutzutage Argumentation als Thema und unzählige Artikel im Bereich der Argumentation wurden in angesehenen Zeitschriften publiziert. Informell beschrieben beschäftigt sich Argumentation mit der Konstruktion von Argumenten, dem Finden von Konflikten zwischen Argumenten, und der Auswahl von kohärenten Mengen von Argumenten. Das Ziel eines solchen Prozesses ist es üblicher Weise eine Form von Wissen abzuleiten und eine Entscheidung für eine gegebene Problemstellung zu treffen. Solche Argumentations-Szenarien können aus ganz unterschiedlichen Kontexten stammen. Um zwei Kontrastbeispiele zu geben: es kann sich einerseits um einen einzelnen Agenten handeln, der sein Wissen auswertet um eine Entscheidung

*Englischer Titel der Dissertation: Computational Aspects of Abstract Argumentation.

über die nächste Aktion zu treffen, aber andererseits auch um eine Gruppe von Agenten, die Argumente austauschen um über die Nutzung einer Ressource zu verhandeln.

Das Wesen von Argumenten ist, dass sie prinzipiell durch neue Argumente anfechtbar sind. Argumentation ist also eine Form des nicht-monotonen Schließens, d.h. eine Folgerung aus dem aktuellen Wissen kann durch neues Wissen (und damit neuen Argumenten) widerlegt werden. Formale Argumentation wurde zu anderen populären nicht-monotonen Formalismen in Beziehung gesetzt. Dabei kann man beobachten, dass sich nicht-monotone Formalismen als Argumentations-Prozess realisieren lassen, indem zuerst Argumente, die anfechtbaren Beweisen im ursprünglichen Formalismus entsprechen, gebildet werden, dann Konflikte zwischen diesen Beweisen eruiert und abschließend kohärente Mengen von Argumenten ermittelt werden. Konkrete Beispiele für solche Formalismen sind "Default Logic" [Dun95], "Defeasible Logic" [GMAB04] und "Answer Set Programming" [Dun95]. Neben der KI beschäftigen sich auch andere Wissenschaften mit verschiedenen Formen von Argumentation und dementsprechend gibt es zahlreiche interdisziplinäre Schnittstellen zur Philosophie, Linguistik und der Rechtswissenschaft [BCD07].

Der Kern jedes (computerunterstützten) Argumentations-Systems ist eine Komponente, die kohärente Mengen von Argumenten findet. Für eine praktische Realisierung ist es essentiell die computationalen Eigenschaften der damit verbunden Problemstellungen zu verstehen. Ein Aspekt hier ist die klassische *Komplexitätsanalyse*, die einerseits Schranken für das Verhalten von bestmöglichen Algorithmen gibt und anderseits ein Maß für die Ausdrucksstärke verschiedener Semantiken für Argumentation darstellt. Unter einer Semantik versteht man dabei einen Regelsatz, der festlegt welche Mengen von Argumenten kohärent sind. Diese Analyse zeigt, dass viele Problemstellungen NP-schwer sind und daher Algorithmen nicht für alle Instanzen effizient sein können (unter der Annahme P $\neq$ NP).

Trotz dieser NP-Schwere gibt es zahlreiche Instanzen, die in Polynomialzeit gelöst werden können. Für das Design von Systemen, die jede Instanz so effizient wie möglich verarbeiten, ist es also unabdingbar Klassen solcher Instanzen, sogenannte "*tractable fragments*" zu identifizieren. Eine weitere Möglichkeit für eine differenzierte Komplexitätsanalyse kommt aus der *Parametrisierten Komplexitätstheorie* (siehe u.a. [Nie06]). Während klassische Komplexitätstheorie die Komplexität im Verhältnis zur Größe der Instanz misst, erlaubt es die parametrisierte Komplexitätstheorie die Komplexität in Bezug auf Problem-Parameter anzugeben. Für viele NP-schwere Probleme gibt es Algorithmen, deren Laufzeit zwar exponentiell mit dem Parameter wächst, aber nur polynomiell mit der Größe der Instanz. Betrachtet man nur Instanzen bei denen der Parameter beschränkt ist, kann man diese in Polynomialzeit lösen, man nennt das Problem dann "*fixed-parameter tractable*".

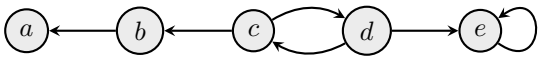
Ein weiterer Aspekt ist die Vielzahl an unterschiedlichen Semantiken, die es unrealistisch erscheinen lässt für jede ein effizientes System zu kreieren. Um dieses Problem zu handhaben kann man Semantiken ineinander übersetzten, d.h. Probleminstanzen so modifizieren, dass eine andere Semantik B das gleiche Resultat liefert wie die ursprüngliche Semantik A auf der ursprünglichen Instanz. So eine *Übersetzung von Semantiken* erlaubt es dann ein ausgefeiltes System für Semantik B auch für Semantik A zu verwenden.

In dieser Arbeit geben wir eine umfassende Analyse dieser Aspekte für Abstrakte Argumentation [Dun95], die den meisten Argumentations-Systemen zu Grunde liegt [BCD07].

2 Argumentation in der Künstlichen Intelligenz

In diesem Abschnitt stellen wir Argumentation in der KI in der hier geboten Kürze vor. Für eine ausführliche Einführung sei der interessierte Leser an den Überblicksartikel von Bench-Capon und Dunne [BCD07] verwiesen.

Abstrakte Argumentation Diese Arbeit konzentriert sich auf Abstrakte Argumentation, den zentralen Formalismus im Gebiet der Formalen Argumentation. Der Kern der Argumentation ist das "Auflösen" von Konflikten zwischen Argumenten durch das Identifizieren von in sich schlüssigen Mengen von Argumenten. Dieser Schritt kann durch sogenannte *Abstract Argumentation Frameworks (AFs)* [Dun95] formalisiert werden. So ein AF besteht einerseits aus abstrakten Objekten, die Argumente repräsentieren, und andererseits aus einer Menge von Attacken zwischen diesen Argumenten die Konflikte modellieren. Dabei geht eine Attacke immer von genau einem Argument aus und attackiert genau ein Argument. AFs kümmern sich aber weder um die Aussage oder innere Struktur eines Arguments noch um die Ursache der Konflikte zwischen Argumenten. Dieses Modell kann als gerichteter Graph interpretiert werden, wobei die Knoten des Graphen den Argumenten entsprechen und die gerichteten Kanten des Graphen den Attacken. Zum Beispiel kann das AF das aus den fünf Argumenten a, b, c, d, e besteht und die Attacken (b, a), (c, b), (c, d), (d, c), (d, e), (e, e) enthält wie folgt als Graph visualisiert werden:



Abstrakte Argumentation basiert auf dieser Graph Struktur und identifiziert mittels dieser kohärente Mengen von Argumenten. Die Literatur kennt eine Vielzahl unterschiedlicher Kriterien, die kohärente Mengen erfüllen sollen, einen Satz solcher Kriterien nennen wir *Semantik* (einen guten Überblick liefert [BCG11]). Zwei grundlegende Konzepte für diese Semantiken sind die Konfliktfreiheit und die Verteidigung von Argumenten. Wir nennen eine Menge von Argumenten konfliktfrei, wenn es keine Attacke zwischen den Argumenten in der Menge gibt. Eine Menge M verteidigt ein Argument a, wenn jedes Argument b das a attackiert von einem Argument $c \in M$ attackiert wird. Konfliktfreie Mengen die alle ihre Argumente auch verteidigt werden "admissible" genannt und bilden die Grundlage für den Großteil der betrachteten Semantiken. Die verschiedenen Semantiken sind durch unterschiedliche Szenarien und Intuitionen begründet und haben daher auch unterschiedlichste Eigenschaften. Dementsprechend beschäftigt sich eine Vielzahl von Arbeiten mit den Eigenschaften, die "gute" Argumentations-Semantiken erfüllen sollen, Implikationen solcher Eigenschaften, und den Beziehungen zwischen unterschiedlichen Semantiken (siehe z.B. [CA07, BCG11]). Diese Arbeit ergänzt diese Bemühungen durch eine Analyse der computationalen Eigenschaften der Semantiken.

Der Argumentations-Prozess Wir betrachten Abstrakte Argumentation als den zentralen Formalismus von Argumentation, nichtsdestotrotz ist Abstrakte Argumentation immer in eine Form von Argumentations-Prozess eingebettet. Schon in Dung's Arbeit werden Abstract Argumentation Frameworks gemeinsam mit mehreren Methoden AFs aus Wissensbasen zu konstruieren, sogennanten Instanzierungen von AFs, vorgestellt.

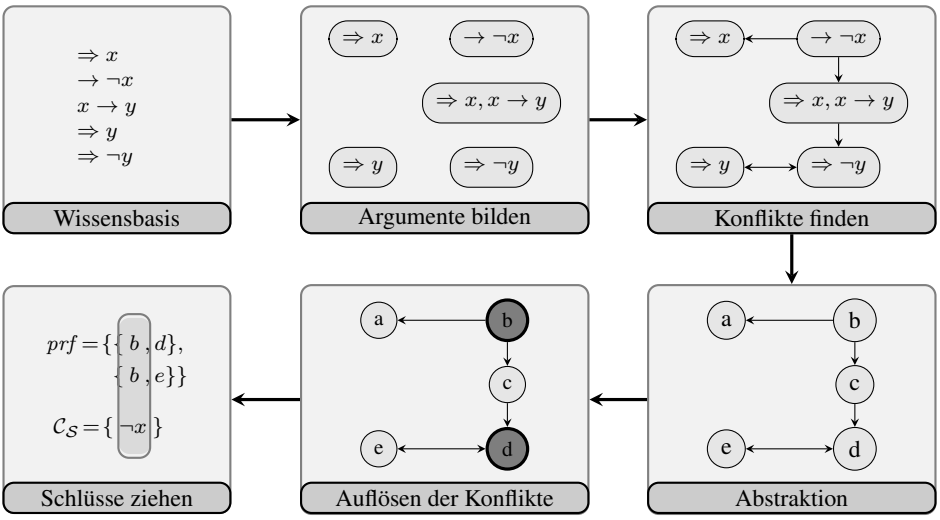


Abbildung 1: Eine Illustration des Argumentations-Prozesses für Defeasible Logic.

Im folgenden beschreiben wir das Konzept dieses Argumentations-Prozess (angelehnt an [CA07]). Dabei unterteilen wir diesen Prozess in sechs Schritte (siehe Abbildung 1): *Generieren einer Wissensbasis:* Eine Argumentation benötigt eine Form von Wissensbasis über die Problemstellung. Das kann eine Theorie in einer formalen Sprache sein oder einfach das Wissen eines Experten, der die Argumente konstruiert. *Konstruktion von Argumenten:* In einem ersten Schritt verwendet man die Wissensbasis um Argumente zu bilden. *Identifizieren von Konflikten:* Hier nutzt man die innere Struktur der Argumente um Konflikte zwischen den verschieden Argumenten zu identifizieren. *Abstraktion von der inneren Struktur der Argumente:* Das Argumentationsproblem wird auf ein Abstract Argumentation Framework reduzier und die innere Struktur der Argumente "vergessen". *Finden der akzeptablen Mengen von Argumenten:* Auf dieser abstrakten Ebene berechnen wir kohärente Mengen von Argumenten. *Schlüsse ziehen:* Als abschließender Schritt wird auf Basis der kohärenten Mengen eine Entscheidung über einen Sachverhalt getroffen, indem man wieder die innere Struktur der akzeptierten Argumente betrachtet.

Computationale Problemstellungen Die zentrale Aufgabe eines Argumentations-Systems ist das Auffinden von kohärenten Mengen von Argumenten. Da Semantiken für solche kohärenten Mengen auf dem abstrakten Level arbeiten, sind eben Abstract Argumentation Frameworks das passende Modell um diese Aufgabe zu studieren. Will man Schlüsse über einen bestimmten Sachverhalt ziehen, ist man aber nicht immer direkt am Berechnen aller kohärenten Mengen interessiert, sondern viel mehr an einem konkreten Argument. Typische computationale Aufgaben sind (neben dem Berechnen von kohärenten Mengen) gutgläubiges ($Cred$) / skeptisches ($Skept$) Schließen, d.h. zu entscheiden ob ein spezielles Argument in mindestens einer / in allen kohärenten Mengen enthalten ist, das Verifizieren einer kohärenten Menge (Ver), d.h. zu entscheiden ob eine konkrete Menge kohärent ist, und zu Entscheiden ob eine (nicht-leere) kohärente Menge existiert

Tabelle 1: Komplexitätsklassifizierungen von Abstrakter Argumentation ($\mathcal{C}$-c bedeutet vollständig für die Klasse $\mathcal{C}$). Neue Resultate sind in Fettschrift hervorgehoben.

σ	$Cred_\sigma$	$Skept_\sigma$	$Ideal_\sigma$	Ver_σ	$Exists_\sigma^{\neg\emptyset}$
cf	**in L**	trivial	trivial	**in L**	**in L**
$naive$	**in L**	**in L**	**P-c**	**in L**	**in L**
grd	**P-c**	**P-c**	**P-c**	**P-c**	**in L**
stb	NP-c	coNP-c	$\mathbf{D^P}$**-c**	**in L**	NP-c
adm	NP-c	trivial	trivial	**in L**	NP-c
com	NP-c	**P-c**	**P-c**	**in L**	NP-c
$resGr$	NP-c	coNP-c	**coNP-c**	**P-c**	in P
prf	NP-c	Π_2^P-c	in Θ_2^P	coNP-c	NP-c
sem	$\mathbf{\Sigma_2^P}$**-c**	$\mathbf{\Pi_2^P}$**-c**	$\mathbf{\Pi_2^P}$**-c**	coNP-c	NP-c
stg	$\mathbf{\Sigma_2^P}$**-c**	$\mathbf{\Pi_2^P}$**-c**	$\mathbf{\Pi_2^P}$**-c**	**coNP-c**	**in L**

($Exists_\sigma^{\neg\emptyset}$). Des Weiteren betrachten wir noch den "ideal" Modus des Schließens, eine Verschärfung des skeptisches Schließen bei dem wir uns für Argumente interessieren die sich durch eine "admissible" Menge aus skeptisch akzeptablen Argumenten fundieren lassen.

Diese Arbeit gibt eine umfassende computationale Analyse der obigen Problemstellungen für die zehn populärsten Argumentations-Semantiken, diese sind "conflict-free" (cf), "naive" ($naive$), "grounded" (grd), "stable" (stb), "admissible" (adm), "complete" (com), "resolution-based grounded" ($resGr$), "preferred" (prf), "semi-stable" (sem) und "stage" (stg). Wir gliedern diese Analyse in drei Kapitel, (klassische) Komplexitätsanalyse, Effiziente Lösbarkeit, und Übersetzbarkeit von Argumentations-Semantiken.

3 Komplexitätsanalyse

Die Komplexität dieser Problemstellungen für die verschiedenen Semantiken wurde in der Literatur teilweise schon studiert [CMDM05, DBC02, Dun09, DC08, BDG11], dennoch gibt es viele offene Fragen. Hier komplementieren wir existierende Resultate wie folgt:

- Wir geben exakte Komplexitätsklassifizierungen für die "semi-stable" und die "stage" Semantik, die zeigen, dass Schlussfolgern mit diesen Semantiken in der 2.Ebene der polynomiellen Hierarchie liegt. Die Komplexitätsklassifizierung der "semi-stable" Semantik war ein offenes Problem, das von [DC08] aufgeworfen wurde.
- Wir geben eine umfassende Klassifizierung für das Schlussfolgern im "ideal" Modus. Einerseits durch generische Resultate und andererseits durch eine konkrete Analyse des "ideal" Modus für die hier betrachteten Semantiken.
- Klassifizierung der in Polynomialzeit lösbaren Problemstellungen in solche, die Polynomialzeit-vollständig (P-c) sind und solche, die mit logarithmischen Speicheraufwand (in L) berechnet werden können.

Die Resultate sind zusammen mit den Komplexitätsresultaten aus der Literatur in Tabelle 1 zusammengefasst.

4 Effiziente Lösbarkeit

Unsere Komplexitätsanalyse zeigt, dass die meisten Problemstellungen NP-schwer sind und daher ein schlecht skalierendes worst-case Laufzeitverhalten haben. Ein Zugang zu "*tractable fragments*" ist es, AFs mit spezieller Graphstruktur zu betrachten. Hierzu gibt es erste Arbeiten für AFs bei denen alle Attacken symmetrisch sind [CMDM05], für AFs ohne Zyklen gerader Länge [DBC02] und eine Analyse verschiedener Ansätze für die "preferred" Semantik [Dun07]. Alle diese Arbeiten beschränken sich aber auf einige wenige Semantiken. Ein Ansatz für *fixed-parameter tractability* ist es, AFs als gerichtete Graphen aufzufassen und die Vielzahl an Graph-Parametern zu nutzen. Erste Untersuchungen für parametrisierte Komplexität von Argumentationsproblemen gibt es in [Dun07], wo die Baumweite als Parameter und in [OS11], wo die Distanz zu speziellen Graphklassen als Parameter genutzt wird. Wir komplementieren diese Resultate wie folgt:

- Wir studieren vier Graphklassen, nämlich azyklische AFs, AFs ohne gerade Zyklen, bipartite AFs und symmetrische AFs, und untersuchen ob sie "tractable fragments" für die betrachteten Semantiken sind. Dazu geben wir für die verschiedenen Semantiken und Graphklassen exakte Komplexitätsklassifikationen, zeigen also insbesondere das gewisse Graphklassen keine "tractable fragments" für gewisse Semantiken sein können. Dabei lösen wir ein offenes Problem aus [BDG11] bezüglich der Komplexität des gutgläubigen Schließens mit der "resolution-based grounded" Semantik in bipartiten AFs. Des weiteren sei erwähnt, dass die breite Komplexitätsanalyse der obigen Graphklassen das Fundament für die erwähnten Distanz-Parametrierungen stärkt und auch zu einer gemeinsamen Publikation geführt [DOS12] hat.
- Für die Problemstellungen, deren Komplexität auf dem zweiten Level der polynomiellen Hierarchie liegt (also schwerer als NP sind), betrachten wir neben den oben genannten "tractable fragments" auch Kriterien die diese Probleme NP-einfach machen. Diese Kriterien reduzieren die Komplexität, aber nicht ausreichend um die Probleme in Polynomialzeit zu lösen. Solche Kriterien erlauben es dann aber SAT-Solver für Probleme die im Allgemeinen zu hohe Komplexität haben zu verwenden. Diese Analyse bildet die Grundlage für das CEGARTIX[1] System [DJWW12], das auf iterativen Aufrufen von SAT-Solvern basiert und gegenwärtig das schnellste System für "preferred", "semi-stable", und "stage" Semantiken ist.
- Im Bereich "Fixed-Parameter Tractability" komplementieren wir einerseits bestehende Resultate, indem wir zeigen, dass alle betrachteten Semantiken "fixed-parameter tractable" bezüglich Baumweite sind. Andererseits erweitern wir diese Resultate auf den Parameter Cliquenweite, eine Generalisierung der Baumweite.
- Im Bereich "Fixed-Parameter Intractability" studieren wir Parameter die speziell für gerichtete Graphen entworfen wurden. Wir zeigen, dass alle unsere Problemstellung NP/coNP-schwer bleiben, selbst wenn wir einen der Parameter cycle-rank, gerichtete Pfadweite, Kelly-Weite, DAG-Weite oder gerichtete Baumweite beschränken.

Die Resultate dieses Kapitels sind in Tabelle 2 zusammengefasst.

[1] `http://www.dbai.tuwien.ac.at/proj/argumentation/cegartix/`

Tabelle 2: "Tractability" für Abstrakte Argumentation. ✓: die betrachtete Problemstellungen auf der gegeben Graphklassen sind "tractable"; ✗: mind. eine Problemstellung bleibt NP/coNP-schwer.

	stb	adm	com	$resGr$	prf	sem	stg
Azyklisch	✓	✓	✓	✓	✓	✓	✓
Ohne gerade Zyklen	✓	✓	✓	✓	✓	✓	✗
Bipartit	✓	✓	✓	✗	✓	✓	✓
Symmetrisch	✗	✓	✓	✓	✓	✗	✗
Beschränkte Baumweite	✓	✓	✓	✓	✓	✓	✓
Beschränkte Cliquenweite	✓	✓	✓	✓	✓	✓	✓
Beschränkter cycle-rank	✗	✗	✗	✗	✗	✗	✗
Beschr. gerichtete Pfadweite	✗	✗	✗	✗	✗	✗	✗
Beschränkte Kelly-Weite	✗	✗	✗	✗	✗	✗	✗
Beschränkte DAG-Weite	✗	✗	✗	✗	✗	✗	✗
Beschr. gerichtete Baumweite	✗	✗	✗	✗	✗	✗	✗

5 Übersetzbarkeit von Argumentations-Semantiken

Eine der populärsten Arten abstrakte Argumentation zu implementieren ist die Übersetzung in einen anderen Formalismus. Anstatt von Grund auf neue Algorithmen zu designen, entwirft man eine Codierung des Argumentationsproblems in einem bekannten Formalismus, für den es bereits ausgereifte Systeme gibt. Beispiele für solche Codierungen sind Übersetzungen in Aussagenlogik [BD04] und Answerset-Programming (ASP) [EGW10]. In dieser Arbeit beschäftigen wir uns mit der Möglichkeit diesen Ansatz innerhalb der abstrakten Argumentation zu verwenden. Wir interessieren also dafür eine Semantik in andere zu übersetzen, indem wir Modifikationen am Argumentation Framework vornehmen. Eine Semantik A kann in eine Semantik B übersetzt, wenn es eine Funktion gibt die ein beliebiges AF so modifiziert, dass die A-kohärenten Mengen des ursprünglichen AFs mit den B-kohärenten Mengen des modifizierten AFs übereinstimmen. Sind die kohärenten Mengen exakt die gleichen sprechen wir von einer exakten Übersetzung, unterscheiden sie sich nur auf neuen Argumenten die durch die Modifikation eingeführt worden sind, stimmen aber auf den ursprünglichen Argumenten überein, von einer sinngetreuen Übersetzung. Wenn die Übersetzung effizient berechnet werden kann genügen beide Arten von Übersetzungen unseren Zwecken. Bei exakten Übersetzungen erhält man die kohärenten Mengen des ursprünglichen Problems unmittelbar, bei sinngetreuen Übersetzungen kann man diese durch eine einfache Projektion erhalten. Das Ziel ist also, wann immer möglich, exakte Übersetzungen zu nutzen (die ja auch sinngetreue Übersetzungen sind) und wenn das nicht möglich ist auf sinngetreue Übersetzungen auszuweichen. Wir betrachten sieben Semantiken[2] und präsentieren die folgenden Resultate:

- Wir betrachten alle Paare von Semantiken A,B und präsentieren (wenn möglich) effiziente exakte oder sinngetreue Übersetzungen von A nach B.
- Wir zeigen, dass es zwischen bestimmten Semantiken keine effiziente exakte / sinnge-

[2]Die Semantiken "conlict-free" und "naive" sind an sich schon effizient berechenbar. Die "Resolution-based grounded" Semantik ist auf Grund ihrer andersartigen Natur nicht (direkt) für diesen Ansatz zugänglich.

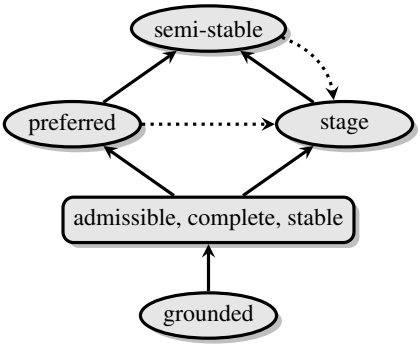


Abbildung 2: Übersetzbarkeit von Argumentations-Semantiken.

treue Übersetzungen geben kann. Manche dieser Resultate basieren auf den präsentierten Komplexitätsresultaten und damit auch auf typischen komplexitätstheoretischen Annahmen, z.B. P $\neq$ NP, andere wiederum folgen unmittelbar aus den unterschiedlichen Eigenschaften der Semantiken.

Die konkreten Resultate bezüglich (sinngetreuen) Übersetzungen sind in Abbildung 2 zusammengefasst. Ein durchgezogener Pfeil von Semantik A zu einer Semantik B drückt aus, dass es eine effiziente sinngetreue Übersetzung von A nach B gibt. Aufgrund der Transitivität von Übersetzungen gilt selbiges für Pfade von solchen Pfeilen. Die zwei gepunkteten Pfeile repräsentieren offenen Fragen, d.h. die Fälle für die wir weder eine effiziente sinngetreue Übersetzung angeben noch einen Beweis für die Nichtexistenz finden konnten. Wenn es keinen Pfad von A nach B gibt, haben wir bewiesen (möglicherweise unter komplexitätstheoretischen Annahmen), dass es keine effiziente Übersetzung gibt.

6 Conclusio

In dieser Arbeit geben wie eine umfassende Komplexitätsanalyse von Abstrakter Argumentation, sowohl im Sinne der klassischen als auch der parametrisierten Komplexitätstheorie. Diese Resultate zeigen einerseits Möglichkeiten und andererseits Schranken für effiziente Systeme auf. Um der Vielzahl an unterschiedlichen Semantiken Herr zu werden studieren wir das Konzept von Übersetzungen zwischen verschiedenen Semantiken.

Die Relevanz dieser Untersuchungen für das Forschungsgebiet wird durch mehrere wissenschaftliche Publikationen untermauert: Resultate der klassischen Komplexitätsanalyse wurden in [DW10, DDW11] publiziert; ”fixed-parameter tractability” Resultate wurden in [DPW12, DSW10] veröffentlicht; und die Übersetzbarkeit von Argumentations-Semantiken wurde in [DW11] publiziert.

Die praktische Bedeutung dieser theoretischen Untersuchungen wird durch zwei auf dieser Arbeit basierenden Systeme belegt. Algorithmen basierend auf dem Parameter Baumweite

werden in [DPW12] präsentiert und sind im dynpartix[3] System implementiert. Das schon erwähnte CEGARTIX System nutzt Parametrisierungen der NP-Fragmente von Semantiken höherer Komplexität um diese mit Hilfe von SAT-Solvern zu implementieren.

Weiterführende Forschungsthemen Aufbauend auf den präsentierten Komplexitätsresultaten kann man verallgemeinerte Problemstellungen betrachten. Ein Beispiel hierzu ist das Berechnen des 8-wertigen "justification status" eines Arguments [Dvo12b]. Ein zentraler Punkt um das erwähnte CEGARTIX System weiter zu verbesserten ist das Identifizieren von weiteren NP-Fragmenten und darauf aufbauenden Parametrisierungen. Das Konzept von Übersetzungen zwischen Semantiken ist nicht nur aus computationaler Sicht interessant, sondern erlaubt es auch die Ausdrucksstärke von Semantiken zu vergleichen. Aus dieser Sicht sind dann auch Übersetzungen interessant, die nicht effizient sind. Erste Resultate hierzu wurden in [DS12] veröffentlicht.

Literatur

[BCD07] Trevor J. M. Bench-Capon and Paul E. Dunne. Argumentation in Artificial Intelligence. *Artif. Intell.*, 171(10-15):619–641, 2007.

[BCG11] Pietro Baroni, Martin Caminada, and Massimiliano Giacomin. An Introduction to Argumentation Semantics. *Knowledge Eng. Review*, 26(4):365–410, 2011.

[BD04] Philippe Besnard and Sylvie Doutre. Checking the Acceptability of a Set of Arguments. In *Proc. NMR 2004*, 59–64, 2004.

[BDG11] Pietro Baroni, Paul E. Dunne, and Massimiliano Giacomin. On the Resolution-Based Family of Abstract Argumentation Semantics and its Grounded Instance. *Artif. Intell.*, 175(3-4):791–813, 2011.

[CA07] Martin Caminada and Leila Amgoud. On the Evaluation of Argumentation Formalisms. *Artif. Intell.*, 171(5-6):286–310, 2007.

[CMDM05] Sylvie Coste-Marquis, Caroline Devred, and Pierre Marquis. Symmetric Argumentation Frameworks. In *Proc. ECSQARU 2005*, LNCS 3571, pages 317–328. Springer, 2005.

[DBC02] Paul E. Dunne and Trevor J. M. Bench-Capon. Coherence in Finite Argument Systems. *Artif. Intell.*, 141(1/2):187–203, 2002.

[DC08] Paul E. Dunne and Martin Caminada. Computational Complexity of Semi-Stable Semantics in Abstract Argumentation Frameworks. In *Proc. JELIA 2008*, LNCS 5293, pages 153–165. Springer, 2008.

[DDW11] Wolfgang Dvořák, Paul E. Dunne, and Stefan Woltran. Parametric Properties of Ideal Semantics. In *Proc. IJCAI 2011*, pages 851–856. IJCAI/AAAI, 2011.

[DJWW12] Wolfgang Dvorák, Matti Järvisalo, Johannes Peter Wallner, and Stefan Woltran. Complexity-Sensitive Decision Procedures for Abstract Argumentation. In *Proc. KR 2012*, pages 54–64. AAAI Press, 2012.

[3] `http://www.dbai.tuwien.ac.at/research/project/argumentation/dynpartix/`

[DOS12] Wolfgang Dvořák, Sebastian Ordyniak, and Stefan Szeider. Augmenting Tractable Fragments of Abstract Argumentation. *Artif. Intell.*, 186(0):157–173, 2012.

[DPW12] Wolfgang Dvořák, Reinhard Pichler, and Stefan Woltran. Towards Fixed-Parameter Tractable Algorithms for Abstract Argumentation. *Artif. Intell.*, 186(0):1 – 37, 2012.

[DS12] Wolfgang Dvořák and Christof Spanring. Comparing the Expressiveness of Argumentation Semantics. In *Proc. COMMA 2012*, FAIA 245, pages 261–272. IOS Press, 2012.

[DSW10] Wolfgang Dvořák, Stefan Szeider, and Stefan Woltran. Reasoning in Argumentation Frameworks of Bounded Clique-Width. In *Proc. COMMA 2010*, FAIA, pages 219–230. IOS Press, 2010.

[Dun95] Phan Minh Dung. On the Acceptability of Arguments and its Fundamental Role in Nonmonotonic Reasoning, Logic Programming and n-Person Games. *Artif. Intell.*, 77(2):321–358, 1995.

[Dun07] Paul E. Dunne Computational Properties of Argument Systems Satisfying Graph-Theoretic Constraints. *Artif. Intell.* 171(10-15):701–729, 2007.

[Dun09] Paul E. Dunne. The Computational Complexity of Ideal Semantics. *Artif. Intell.*, 173(18):1559–1591, 2009.

[Dvo12] Wolfgang Dvořák. Computational Aspects of Abstract Argumentation. Dissertation, Technische Universität Wien, Institut für Informationssysteme, 2012.

[Dvo12b] Wolfgang Dvořák. On the Complexity of Computing the Justification Status of an Argument. In *Proc. TAFA 2011*, LNCS 7132, pages 32–49. Springer, 2012.

[DW10] Wolfgang Dvořák and Stefan Woltran. Complexity of Semi-Stable and Stage Semantics in Argumentation frameworks. *Inf. Process. Lett.*, 110(11):425–430, 2010.

[DW11] Wolfgang Dvořák and Stefan Woltran. On the Intertranslatability of Argumentation Semantics. *J. Artif. Intell. Res. (JAIR)*, 41:445–475, 2011.

[EGW10] Uwe Egly, Sarah Gaggl, and Stefan Woltran. Answer-Set Programming Encodings for Argumentation Frameworks. *Argument and Computation*, 1(2):147–177, 2010.

[GMAB04] Guido Governatori, Michael J. Maher, Grigoris Antoniou, and David Billington. Argumentation Semantics for Defeasible Logic. *J. Log. Comput.*, 14(5):675–702, 2004.

[Nie06] Rolf Niedermeier. *Invitation to Fixed-Parameter Algorithms*, volume 31. Oxford University Press, USA, 2006.

[OS11] Sebastian Ordyniak and Stefan Szeider. Augmenting Tractable Fragments of Abstract Argumentation. In *Proc. IJCAI 2011*, pages 1033–1038. IJCAI/AAAI, 2011.



Wolfgang Dvořák wurde am 24. Juni 1984 in Wien geboren. Er maturierte 2002 am Bundesrealgymnasium Franklinstr. 26 in Wien. Nach dem Grundwehrdienst studierte er an der Technischen Universität Wien das Diplomstudium Technische Mathematik und das Masterstudium Computational Intelligence. Von 2006 – 2012 war er Mitglied der Forschungsgruppe für Datenbanken und Artificial Intelligence an der TU Wien an der er von 2009 bis 2012 in Informatik promovierte. Seit 2012 ist er an der Fakultät für in Informatik der Universität Wien in der Forschungsgruppe “Theorie und Anwendungen von Algorithmen” tätig.

Platz- und Schaltkreiskomplexität von MSO-beschreibbaren Problemen auf baumartig zerlegbaren Strukturen*

Michael Elberfeld

International Computer Science Institute
1947 Center Street, Suite 600
Berkeley, California 94704, USA

elberfeld@icsi.berkeley.edu

Abstract: Dieser Beitrag ist eine deutschsprachige Kurzfassung der Dissertation von Michael Elberfeld [Elb12]. Die Dissertation entwickelt und bearbeitet Fragestellungen aus den Bereichen der Theoretischen Informatik und Mathematischen Logik. Sie untersucht die Platz-, Schaltkreis- und Beschreibungskomplexität von Problemen, die sich durch Formeln in monadischer Logik zweiter Stufe beschreiben lassen und deren Eingaben eine beschränkte Baumweite oder -tiefe besitzen. Die gewonnenen Resultate werden angewendet, um die Komplexität konkreter Entscheidungs-, Zähl- und Optimierungsprobleme aus verschiedenen Anwendungsgebieten zu klassifizieren.

1 Einleitung

Informatik und Mathematische Logik sind verknüpfte Forschungsfelder. Während die Informatik sich mit der *Lösung* von *Berechnungsproblemen* wie dem Finden eines kürzesten Weges in einer Landkarte beschäftigt, untersucht die Mathematische Logik *Eigenschaften* von Strukturen wie Graphen und deren *Beschreibbarkeit* durch logische Formeln. Obwohl diese Fragestellungen auf den ersten Blick recht unterschiedlich erscheinen mögen, gibt es doch Gemeinsamkeiten: Zum einen lassen sich Berechnungsprobleme oft eindeutig und kompakt durch logische Formeln beschreiben. Zum anderen kann man die Frage, ob eine logische Struktur eine Formel erfüllt, selbst als Berechnungsproblem auffassen und nach Algorithmen hierzu suchen. Verbindet man beide Ideen, kann man individuelle Berechnungsprobleme lösen ohne neue spezialisierte Programme schreiben zu müssen. Es reicht aus eine Beschreibung des Problems in Form einer logischen Formel zu entwickeln. Zusammen mit dem Löser, der die Formel auswertet, ergibt sich ein Programm für das Problem. Viele wissenschaftliche Arbeiten haben bisher die *Zeitkomplexität* dieser Art von Logik-basierten Berechnungsproblemen untersucht; also die Frage, wie schnell man

*Englischer Titel der Dissertation: „Space and Circuit Complexity of Monadic Second-Order Definable Problems on Tree-Decomposable Structures."

ein Problem lösen kann. In der Dissertation, von der diese Kurzfassung handelt, liegt der Fokus auf der *Platz-*, und *Schaltkreiskomplexität* von durch logischen Formeln beschreibbaren Problemen; also die Frage, mit wie viel Arbeitsspeicher oder mit welcher Art von integrierten Schaltkreisen ein Problem gelöst werden kann. Ebenfalls wird die eng verwandte *Beschreibungskomplexität* von Problemen eine Rolle spielen; die Frage, in wie weit man logische Problembeschreibungen vereinfachen kann. Hieraus können sich indirekt effizientere Algorithmen ergeben. Seien sie nun schnell, verbrauchen wenig Platz oder haben kleine Schaltkreise.

Allgemeine algorithmische Resultate ergeben sich, wenn man ausdrucksstarke Logiken betrachtet, deren Formeln viele Probleme beschreiben können. Durch die NP-schwere vieler Logik-basierter Probleme ist die Suche nach effizienten Algorithmen aber oft eine waghalsige Gradwanderung. Eines der raffiniertesten Resultate in diesem Gebiet, das eine perfekte Balance zwischen großer Ausdrucksstärke und algorithmischer Effizienz erreicht, ist ein Satz von Courcelle. Dieser sagt, dass sich jedes durch eine Formel in monadischer Logik zweiter Stufe beschreibbare Problem in linearer Zeit lösen lässt, wenn man Eingabestrukturen betrachtet, die eine beschränkte Baumweite haben [Cou90]. Um aufbauend auf dem Satz von Courcelle das Ziel und die Beträge der vorgestellten Dissertation zu diskutieren, werden nun zunächst die Begriffe der monadischen Logik zweiter Stufe und der Baumweite besprochen.

Die *monadische Logik zweiter Stufe* (MSO-*Logik*) verallgemeinert die Prädikatenlogik erster Stufe dahingehend, dass man nicht nur einzelne Elemente einer logischen Struktur durch Quantoren adressieren kann, sondern dies auch für Teilmengen von Elementen und Relationen möglich ist (diese Variante der MSO-Logik nennt man oft auch GSO- oder MSO_2-Logik). Zum Beispiel beschreibt die MSO-Formel $\varphi :=$

$$\exists R\, \exists G\, \exists B\, \forall v \Big(R(v) \vee G(v) \vee B(v) \wedge \\ \forall w \left(E(v,w) \rightarrow \neg(R(v) \wedge R(w)) \wedge \neg(G(v) \wedge G(w)) \wedge \neg(B(v) \wedge B(w)) \right) \Big)$$

genau die Graphen (Kanten werden durch das Relationssymbol E adressiert), deren Knoten sich so in drei Mengen (adressiert durch die Symbole R, G und B) aufteilen lassen, dass benachbarte Knoten in verschiedenen Mengen liegen. Durch Auswertung dieser Formel wird entschieden, ob ein gegebener Graph 3-färbbar ist; also das formale *Entscheidungsproblem* 3-FÄRBBARKEIT gelöst. Zum Beispiel erfüllt der Graph  die obige Formel, der Graph  aber nicht. Neben Berechnungsproblemen, bei denen es hauptsächlich auf eine Entscheidung zwischen „ja“ und „nein“ ankommt, geht es bei *Zähl-* und *Optimierungsproblemen* jeweils um die Frage, wie viele Lösungen einer bestimmten Art es gibt oder wie gut man etwas lösen kann. Diese Probleme kann man häufig auch durch logische Formeln beschreiben. Die MSO-Formel $\psi(X) := \forall v \left(X(v) \vee \exists w \left(X(w) \wedge E(v,w) \right) \right)$ beschreibt zum Beispiel genau die (durch X adressierten) Mengen von Knoten eines Graphen, die alle Knoten abdecken (jeder Knoten des Graphen ist Teil der Menge oder benachbart zu einem Knoten der Menge). Die zugehörigen Zähl- und Optimierungsprobleme fragen für einen gegebenen Graphen nach der Anzahl solcher Lösungen beziehungsweise der Größe einer kleinsten Lösung. Beispielsweise kann der Graph  durch 17 verschiedene Knotenmengen abgedeckt werden, wobei die kleinste Menge aus 3 Knoten besteht. Um

die Gemeinsamkeiten der drei Problemarten (Entscheidungs-, Zähl- und Optimierungsprobleme) bei deren Lösung auszunutzen wird in der Arbeit das Konzept des *Lösungshistogramms* eingeführt: Für das gerade betrachtete Paar von Formel und Graph ist dies das Feld $0 \mid 0 \mid 3 \mid 8 \mid 5 \mid 1$ mit 6 Einträgen, die von links nach rechts durch 0 bis 5 indiziert werden. Entsprechend des Indexes steht an jeder Position die Anzahl der verschiedenen abdeckenden Mengen – *Lösungen* – dieser Größe. Ausgehen von einem Lösungshistogramm für eine MSO-Formel und einer logischen Struktur kann man entscheiden, ob es eine Lösung gibt, die Anzahl der Lösungen durch Aufaddieren bestimmen und die Größe der kleinsten oder größten Lösung ablesen.

Ein großer Vorteil der MSO-Logik ist ihre große Ausdrucksstärke und die einfache Art, mit der man Berechnungsprobleme beschreiben kann. Ein großer Nachteil ist, dass MSO-*beschreibbare Probleme* im algorithmischen Sinn schwer lösbar sein können: Es gibt NP-schwere MSO-beschreibbare Entscheidungsprobleme (äquivalent zum Entscheidungsproblem der Aussagenlogik) und #P-schwere MSO-beschreibbare Zählprobleme (äquivalent zum Zählproblem der Aussagenlogik). Wenn man Problembeschreibungen selbst als Eingabe verarbeiten möchte, dann ist dies sogar schwer für PSPACE (die Klasse aller auf polynomiellem Platz lösbaren Probleme). Um der algorithmischen Schwere zu entgehen, aber trotzdem die große Ausdrucksstärke der MSO-Logik zu haben, werden beim Satz von Courcelle nur Eingabestrukturen betrachtet, die eine beschränkte Baumweite haben.

Die *Baumweite* ist ein Maß für die Ähnlichkeit eines Graphen (allgemein einer logischen Struktur) zu Bäumen. Um die Baumweite zu messen, wird ein Graph als eine *Baumzerlegung* kodiert. Dies ist ein Baum, dessen Knoten so mit Teilgraphen markiert sind, dass Abdeckungs- und Zusammenhangsbedingungen erfüllt sind: Die *Abdeckungsbedingung* sagt, dass jede Kante des Graphen in einem Teilgraphen vorkommen muss. Die *Zusammenhangsbedingung* sagt, dass die Teilgraphen, in denen ein Knoten des Graphen vorkommt, nicht beliebig verstreut sein dürfen, sondern im Baum zusammenhängend sind. Mithilfe von Baumzerlegungen kann man die Methode der dynamischen Programmierung anwenden, um zum Beispiel 3-FÄRBBARKEIT zu lösen: Ausgehend von den Blättern einer Baumzerlegungen berechnet man für jeden Teilgraphen eine Menge von Färbungen, die sich zu Färbungen für den schon betrachteten darunterliegenden Graph erweitern lassen. Wenn die Knoten der zur Verfügung stehenden Baumzerlegung nur durch Teilgraphen konstanter Größe markiert sind, ergibt sich ein effizienter Lösungsansatz. Formal spricht man von einer Menge von Graphen mit *beschränkter Baumweite*, falls es eine natürliche Zahl w gibt, so dass man für jeden Graph aus der Menge eine Baumzerlegung finden kann, die nur Teilgraphen mit maximal w vielen Knoten enthält. Der Satz von Courcelle verallgemeinert den obigen Lösungsansatz für 3-FÄRBBARKEIT so, dass er auf jedes MSO-beschreibbare Probleme anwendbar ist. Im zugehörigen Beweis wird zuerst eine Baumzerlegung konstruiert und dann die MSO-Formel entlang der Zerlegung ausgewertet.

Wenn man dem Satz von Courcelle und seinem Beweis zum ersten Mal begegnet, dann scheint er nur eingeschränkt einsetzbar zu sein: Klassen von Graphen mit beschränkter Baumweite enthalten zum Beispiel nicht alle planaren Graphen oder alle vollständigen Graphen. Des weiteren führt der Beweis von Courcelle zwar auf Algorithmen mit linearer Laufzeit, in deren „O-Notationen“ verstecken sich aber große Konstanten und sie sind somit nicht direkt praktisch anwendbar. Nichtsdestotrotz spielt Courcelles Satz eine entschei-

dende Rolle bei der Entwicklung neuer effizienter Algorithmen. Bevor man viel Arbeit in einen wirklich praktikablen Algorithmus für ein Problem investiert, kann man Courcelles Satz verwenden, um erst einmal zu wissen, ob effiziente Algorithmen möglich sind. Des weiteren hat sich herausgestellt, dass es viele Berechnungsprobleme gibt, deren Eingaben zwar keine beschränkte Baumweite haben oder die nicht MSO-beschreibbar sind, bei denen Courcelles Satz aber als Teil einer größeren Lösungsstrategie verwendet werden kann.

In der Dissertation wird untersucht, in wie weit man die Vorteile von MSO-beschreibbaren Problemen auf Eingaben mit beschränkter Baumweite für die Untersuchung der Platz- und Schaltkreiskomplexität verwenden kann. Durch Beschränkung von Speicherplatz oder der Größe und Tiefe von Schaltkreisen werden die verwendeten algorithmischen Ansätze oft unverhältnismäßig komplex. Die Dissertation untersucht, in wie weit man MSO-basierte Problembeschreibungen und Baumzerlegungen verwenden kann, um algorithmische Ansätze in der Platz- und Schaltkreiskomplexität gleichzeitig zu verallgemeinern und einfacher zugänglich zu machen. Hierbei spielt auch die Beschreibungskomplexität von Problemen eine Rolle, denn durch einfachere Problembeschreibungen erhält man in der Regel auch effizientere Algorithmen. Konkret schlagen sich die Resultate nieder als eine Reihe mathematischer *Sätze* mit Beispielen für deren *Anwendungen* sowie der Erweiterung bestehender und Entwicklung neuer *Beweismethoden*.

Die Beiträge der Arbeit werden in den folgenden Abschnitten 2 bis 5 nach Art der verwendeten Berechnungsmodelle sortiert dargestellt. Im Abschnitt 6 werden die Beiträge nebeneinandergestellt und darauf aufbauend zukünftige Forschungsrichtungen diskutiert.

2 Beschränkte Baumtiefe und Logik erster Stufe

Der erste Teil der Dissertation beschäftigt sich mit der Beschreibungskomplexität von MSO-beschreibbaren Problemen und untersucht die folgende Frage: „Wann ist es möglich, die algorithmisch einfacher zu handhabende Prädikatenlogik erster Stufe (FO-Logik) anstatt der monadischen Logik zweiter Stufe zur Beschreibung von Problemen zu verwenden?“ Das heißt, unter welchen Umständen kann man MSO-Formeln in äquivalente FO-Formeln umwandeln? Es ist bekannt, dass dies nicht möglich ist, wenn man beliebige Graphen oder auch nur Pfad-Graphen betrachtet. Man kann zum Beispiel mit einer MSO-Formel beschreiben, dass ein Pfad eine gerade Anzahl von Knoten enthält. Dies ist mit einer FO-Formel, die nur einzelne Elemente mit ihren Quantoren binden kann, nicht möglich. Der allgemeine Grund hierfür ist, dass FO-Formeln nur Eigenschaften ausdrücken können, die sich auf lokale Umgebungen von Knoten in einem Graph beziehen; wie zum Beispiel die Eigenschaft, dass ein Graph einen Pfad einer konstanten Länge als Teilgraph enthält oder jeder Knoten einen Nachbar besitzt. Dies wirft die Frage auf, was bei Graphen passiert, in denen es keine langen Pfade gibt. Interessanterweise sind dies genau die Graphen, für die es Baumzerlegungen gibt, die gleichzeitig eine beschränkte Weite haben und deren zugrundeliegender Baum eine beschränkte Tiefe besitzt; jede Klasse solcher Graphen hat eine *beschränkte Baumtiefe*. Auf diesen Graphen haben MSO- und FO-Logik dieselbe Ausdrucksstärke:

Satz 2.1. *Sei $\mathcal{C}$ eine Klasse von Graphen mit beschränkter Baumtiefe. Für jede* MSO*-Formel φ gibt es eine* FO*-Formel ψ, so dass jeder Graph $G \in \mathcal{C}$ die Formel φ genau dann erfüllt, wenn dies auch für die Formel ψ gilt.*

Anwendung fand dieser Satz in einer Arbeit [EGT12], die auch untersucht, wann sich die Ausdrucksstärken von MSO- und FO-Logik unterscheiden. Unter bestimmten Abschlussbedingungen an die Klasse $\mathcal{C}$ ist dies der Fall, wenn $\mathcal{C}$ keine beschränkte Baumweite hat.

Für den Beweis des obigen Satzes könnte man versuchen dem typischen Beweisschema von Courcelles Satz zu folgen. Das heißt, erst eine Baumzerlegung beschränkter Weite und Tiefe mit FO-Formeln zu definieren und dann zu verwenden, um die MSO-Formel entlang der Baumzerlegung auszuwerten. Leider schlägt dieser Ansatz fehl. Zwar kann man in FO-Logik verifizieren, ob eine gegebene Baumzerlegung zum Graphen passt, man kann aber nicht immer eindeutig eine solche Zerlegung definieren; die FO-Formel kann nicht unbedingt zwischen verschiedenen Zerlegungen unterscheiden und einfach die (lexikographisch) kleinste herauspicken. In der Arbeit wird daher folgender neuer Ansatz entwickelt: Zuerst wird eine Formel ρ verwendet, die der rekursiven Definition von Graphen mit beschränkter Baumtiefe entspricht [NO12]. Diese wird dann zu einer Formel ψ erweitert, die die ursprüngliche MSO-Formel auswertet, in dem sie induktiv Mengen von MSO-Formeln (MSO-*Typen*) beschreibt, die von Teilstrukturen der gesamten Struktur erfüllt sind. Am Ende stellt sie fest, ob die gesuchte MSO-Formel φ im MSO-Typ des gesamten Graphen enthalten ist. Den Induktionsschritt (wie man die MSO-Typen von Teilgraphen zusammenfügt um den MSO-Typ des gesamten Graphen zu bekommen) kann man auf verschiedene Arten beweisen: In [EGT12] wurde hierzu ein nicht-konstruktiver auf Ehrenfeucht–Fraïssé-Spielen basierender Ansatz verwendet. In der Dissertation wurde ein konstruktiver Ansatz aufbauend auf einem neu entwickelten Automaten-Modell, dem *Multimengen-Baumautomaten*, verwendet. Multimengen-Baumautomaten finden auch im folgenden Abschnitt Verwendung.

3 Beschränkte Baumtiefe und Schaltkreise konstanter Tiefe

Durch die geringe Beschreibungskomplexität von MSO-beschreibbaren Entscheidungsproblemen auf Graphen mit beschränkter Baumtiefe ergibt sich aus bekannten Resultaten der Komplexitätstheorie, dass diese auch durch Boolesche Schaltkreise konstanter Tiefe gelöst werden können (einen Überblick hierzu findet sich im Buch von Immerman [Imm99]). Die betrachteten Probleme liegen daher in der Komplexitätsklasse AC^0, wobei man den Aufbau der verwendeten Schaltkreise in DLOGTIME verifizieren kann – sie sind DLOGTIME-*uniform*. Dies gilt für jede in der Dissertation betrachtete Familie von Schaltkreisen. (Uniforme Schaltkreise werden im Buch von Vollmer [Vol99] behandelt.)

Korollar 3.1. *Sei $\mathcal{C}$ eine Klasse von Graphen mit beschränkter Baumtiefe. Für jede* MSO*-Formel φ gibt es* DLOGTIME*-uniforme* AC^0*-Schaltkreise, die für Graphen aus $\mathcal{C}$ das durch φ beschriebene Entscheidungsproblem lösen.*

Analog zum Korollar, mit dem man Entscheidungsprobleme durch Booleschen Schaltkreise lösen kann, wird in der Arbeit ein Satz entwickelt, mit dem man Zählprobleme durch arithmetische Schaltkreise lösen kann. Die zugehörigen Berechnungsprobleme liegen daher in der Komplexitätsklasse GapAC^0 (einen Überblick über GapAC^0 und verwandte Klassen gibt Allender [All04]). Der folgende Satz löst hierbei nicht nur Zählprobleme, sondern berechnet Lösungshistogramme:

Satz 3.2. *Sei $\mathcal{C}$ eine Klasse von Graphen mit beschränkter Baumtiefe. Für jede* MSO*-Formel $\varphi(X)$ gibt es* DLOGTIME*-uniforme* GapAC^0*-Schaltkreise, die für Graphen aus $\mathcal{C}$ das durch $\varphi(X)$ beschriebene Histogramm (als Zahl kodiert) berechnen.*

Korollar und Satz finden Anwendung bei der Bestimmung oberer komplexitätstheoretischer Schranken für Berechnungsprobleme, die (1) MSO-beschreibbar sind und deren Eingaben man auf Graphen mit beschränkter Baumtiefe einschränkt oder (2) sich (vollständig) in MSO-beschreibbare Probleme über Graphen mit einer konstanten Baumtiefe umwandeln lassen. Ein prominentes Beispiel des ersten Typs ist die Berechnung der Anzahl von Paarungen eines Graphen. Dieses Problem ist im allgemeinen schwer für $\#\mathrm{P}$, aber man kann es bei beschränkter Baumtiefe in $\#\mathrm{AC}^0$ lösen. Ein Beispiel des zweiten Typs ist SUBSET-SUM mit unär kodierten Gewichten. Dieses Problem ist in pseudopolynomieller Zeit lösbar und mit einer Graph-basierten Darstellung des zugehörigen dynamischen Programmierungsansatzes kann man zeigen, dass es in NL (nichtdeterministischem logarithmischem Platz) liegt. Da es sich auf die Berechnung von MSO-beschreibbaren Lösungshistogrammen über Graphen mit beschränkter Baumweite reduzieren lässt, kann man durch Anwendung von Resultaten aus der Dissertation zeigen, dass es in TC^0 liegt.

Zum Beweis von Satz 3.2 wird die initiale Idee aus dem vorherigen Abschnitt zur Konstruktion von Baumzerlegungen wieder aufgegriffen: Es wird zuerst eine Baumzerlegung beschränkter Weite und Tiefe konstruiert. Interessanterweise geschieht dies unter Zuhilfenahme der im vorherigen Abschnitt entwickelten Beschreibung von Strukturen mit beschränkter Baumtiefe durch FO-Formeln. Danach wird die MSO-Formel in einen äquivalenten Multimengen-Baumautomaten umgewandelt. Zuletzt wird gezeigt, wie man den Automaten durch arithmetische Schaltkreise simulieren kann. Hierzu werden bestehende Ansätze aus dem Bereich der Linearzeitalgorithmen aufgegriffen und stark erweitert, um auch mit Bäumen konstanter Tiefe und unbeschränktem Grad arbeiten zu können.

Nachdem uns die Frage nach dem Unterschied in der Ausdrucksstärke von MSO- und FO-Logik auf das Konzept der beschränkten Baumtiefe und Schaltkreise konstanter Tiefe geführt hat, kommen wir in den nächsten beiden Abschnitten wieder auf das am Anfang erwähnte Konzept der beschränkten Baumweite zurück.

4 Baumzerlegungen in Klammerdarstellung und Schaltkreise logarithmischer Tiefe

Im Beweis von Courcelles Satz wird zuerst eine Baumzerlegung für die in der Eingabe kodierte Struktur konstruiert und dann ein zur MSO-Formel äquivalenter Baumautomat ent-

lang der Zerlegung simuliert. In diesem Abschnitt werden zuerst die Ergebnisse der Arbeit besprochen, die sich auf den zweiten Schritt beziehen. Hierbei zeigt sich, dass schon die Auswertung der MSO-Formel entlang einer gegebenen (und möglichst zugänglich kodierten) Zerlegung eine breite Anwendung bei der Untersuchung von Schaltkreiskomplexitätsklassen besitzt. Die entwickelten Methoden helfen Resultate aus der Komplexitätstheorie zu verallgemeinern und gleichzeitig einfacher zu beweisen.



Es ist bekannt, dass die Komplexität von Berechnungsproblemen auf Bäumen stark von der Kodierung des Eingabebaums abhängt. Zum Beispiel ist es vollständig für L (deterministischer logarithmischer Platz), die transitive Hülle eines Baumes zu berechnen. Es wird aber einfacher (vollständig für TC^0), wenn man einen Baum wie auf der rechten Seite gezeigt als *Klammerausdruck* [[ ] [[ ] [ ]]] kodiert. Damit bei der Untersuchung der Komplexität von Problemen wie der Auswertung von Booleschen oder arithmetischen Ausdrücken die Kodierung der Eingabe nicht die Komplexität des eigentlichen Problems überdeckt, verwendet man meist den algorithmisch einfacheren Klammerausdruck. Mit dieser Kodierung sind die obigen Probleme in logarithmischer Tiefe lösbar, wobei die verwendeten Gatter im Fall von Booleschen Ausdrücken ebenfalls Boolesch und im Fall von arithmetischen Ausdrücken ebenfalls arithmetisch sind [BCGR92]. In beiden Fällen haben die Gatter nur beschränkt viele Eingaben; dies entspricht jeweils den Komplexitätsklassen NC^1 und $\#\mathrm{NC}^1$. Die folgenden Sätze verallgemeinern die obigen Resultate:

Satz 4.1. *Sei $\mathcal{C}$ eine Klasse von Graphen mit beschränkter Baumweite. Für jede* MSO*-Formel φ gibt es* DLOGTIME*-uniforme* NC^1*-Schaltkreise, die für Graphen aus $\mathcal{C}$, die zusammen mit einer Baumzerlegung in Klammerdarstellung gegeben sind, das durch φ beschriebene Entscheidungsproblem lösen.*

Satz 4.2. *Sei $\mathcal{C}$ eine Klasse von Graphen mit beschränkter Baumweite. Für jede* MSO*-Formel $\varphi(X)$ gibt es* DLOGTIME*-uniforme* $\#\mathrm{NC}^1$ *Schaltkreise, die für Graphen aus $\mathcal{C}$, die zusammen mit einer Baumzerlegung in Klammerdarstellung gegeben sind, das durch $\varphi(X)$ beschriebene Histogramm (als Zahl kodiert) berechnen.*

Neben der Anwendung der obigen Sätze auf das Lösen von Booleschen oder arithmetischen Ausdrücken, ist ein weiteres Beispiel das Lösen von durch Automaten definierter Probleme, deren Eingaben XML-Dateien sind. Die Anwendung der obigen Sätze ist möglich, da XML-Dateien baumartige Strukturen durch (angereicherte) Klammerdarstellungen kodieren.

Zum Beweis des Satzes zu Entscheidungsproblemen kann zum Beispiel die MSO-Formel in einen äquivalenten Baumautomaten umwandeln und dann bestehende Ergebnisse zur Simulation von Baumautomaten verwenden. Diese Ergebnisse basieren auf der Beweistechnik von Buss et al. [BCGR92] mit der Boolesche Ausdrücke beliebiger Tiefe durch Schaltkreise logarithmischer Tiefe ausgewertet werden können. Kern dieser Technik ist es, rekursiv Teile aus einem bestehenden Ausdruck auszukoppeln, diese auszuwerten und die Ergebnisse so zu kombinieren, dass sich ein Ergebnis für den gesamten Ausdruck ergibt. Wenn man die ausgekoppelten Teile groß genug wählt, ergibt sich eine logarithmisch tiefe Rekursion, die sich mit DLOGTIME-uniformen NC^1-Schaltkreisen implementieren lässt. Um auch den Satz zur Konstruktion von Histogrammen zu beweisen, wird in der Disserta-

tion eine alternative Beweistechnik entwickelt: Anstatt einen Problem-basierten Ansatz zu verwenden, der *gleichzeitig* balanciert und auswertet, werden diese Schritte *getrennt*. Zuerst wird die gegebene Baumzerlegung balanciert. Dies geschieht durch Anwendung von Methoden zur Baumkontraktion. Danach wird ein zur MSO-Formel äquivalenter Baumautomat auf der balancierten (und damit logarithmisch tiefen) Baumzerlegung simuliert.

Was passiert, wenn man sich nicht in der komfortablen Situation befindet, dass schon eine Baumzerlegung in der Eingabe enthalten ist, wird im nächsten Abschnitt besprochen.

5 Beschränkte Baumweite und logarithmischer Platz

In diesem Abschnitt betrachten wir MSO-beschreibbare Probleme auf Graphen mit beschränkter Baumweite. Da die folgenden zwei Sätze L-vollständige Probleme wie das Erreichbarkeitsproblem in Bäumen abdecken, beantworten sie die Frage nach der Komplexität dieser MSO-beschreibbaren Probleme:

Satz 5.1. *Sei $\mathcal{C}$ eine Klasse von Graphen mit beschränkter Baumweite. Für jede* MSO*-Formel φ ist das Entscheidungsproblem für Graphen aus $\mathcal{C}$ in* L *berechenbar.*

Satz 5.2. *Sei $\mathcal{C}$ eine Klasse von Graphen mit beschränkter Baumweite. Für jede* MSO*-Formel $\varphi(X)$ ist das Histogramm für Graphen aus $\mathcal{C}$ in* L *berechenbar.*

Die obigen Sätze werden in der Dissertation auf zwei Arten *angewendet*. Zum einen kann man mit ihnen zeigen, dass MSO-beschreibbare Probleme auf Graphen mit beschränkter Baumweite L-berechenbar sind. Dies umfasst zum Beispiel das Erreichbarkeitsproblem oder die Frage, ob ein gegebener Graph eine Paarung seiner Knoten besitzt. Verwendet man die Sätze als Teil einer größeren Lösungsstrategie, kann man auch Probleme auf Graphen (potentiell) unbeschränkter Baumweite lösen. Dies ist zum Beispiel die Frage, ob ein gegebener Graph einen Kreis gerader Länge enthält: Bei hoher Baumweite ist ein solcher Kreis immer vorhanden. Falls die Baumweite beschränkt ist, verwendet man die Sätze um herauszufinden, ob es einen (MSO-beschreibbaren) Pfad gerader Länge gibt.

Um die Sätze zu beweisen, folgt die Dissertation dem gängigen Beweisschema, bei dem man zuerst eine Zerlegung berechnet und dann, ausgehend von dieser Zerlegung, das betrachtete MSO-beschreibbare Problem löst. Die Resultate aus dem vorherigen Abschnitt zur Lösung des zweiten Schrittes kann man in diesem Abschnitt wiederverwenden, da jede $\#\mathrm{NC}^1$-berechenbare Funktion auch L-berechenbar ist (einen Überblick und Details hierzu gibt Allender [All04]). Der noch verbleibende Schritt zum Beweis der obigen Sätze ist durch den folgenden Satz gegeben:

Satz 5.3. *Sei $\mathcal{C}$ eine Klasse von Graphen mit beschränkter Baumweite. Man kann in* L *für jeden Graphen aus $\mathcal{C}$ eine Baumzerlegung mit beschränkter Weite (in Klammerdarstellung) berechnen.*

Um Baumzerlegungen zu konstruieren wird in der Arbeit das Konzept der Deskriptorzerlegung entwickelt. Mithilfe des Satzes von Reingold [Rei08] werden zuerst Deskriptorzer-

legungen konstruiert. Danach werden Teilmengenbedingungen der Deskriptorzerlegung genutzt, um eine Baumzerlegung aus der Deskriptorzerlegung zu gewinnen.

6 Fazit

Das Ziel der Dissertation war es, die Verwendung von MSO-Logik für die Untersuchung der Platz- und Schaltkreiskomplexität von Entscheidungs-, Optimierungs-, und Zählproblemen zu ermöglichen. Dies wurde durch eine Reihe mathematischer Sätze erreicht, die jeweils eine Aussage über die Komplexität MSO-beschreibbarer Probleme treffen, deren Eingaben baumartige Graphen sind. Abbildung 1 zeigt dies zusammenfassend. Die Ergebnisse verallgemeinern bestehende Resultate, wie zum Beispiel das Auswerten von arithmetischen Ausdrücken in $\#\mathrm{NC}^1$, und ermöglichen es auch neue Aussagen über die Komplexität von Problemen zu treffen, wie zum Beispiel das Finden von gerichteten Pfaden in Graphen mit beschränkter Baumweite in L.

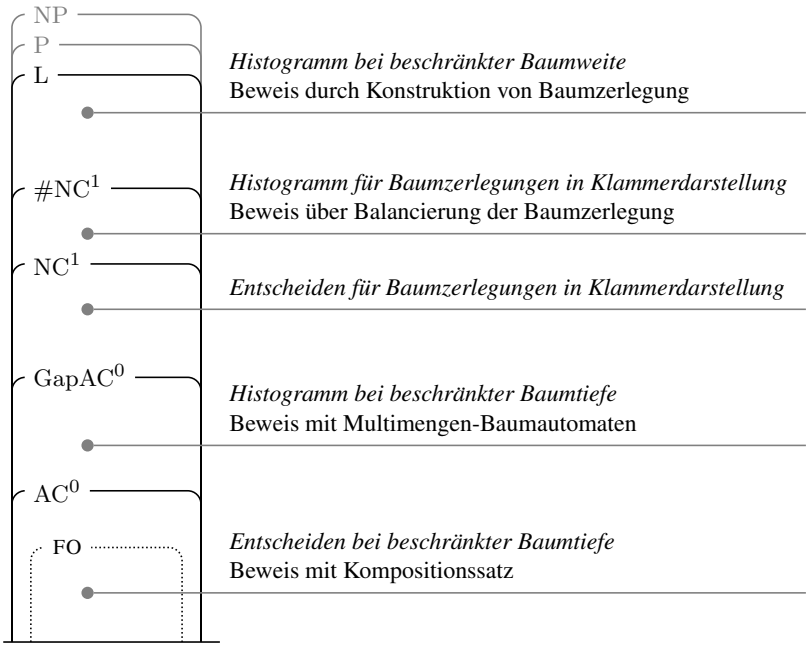


Abbildung 1: Die in der Dissertation entwickelten Klassifizierungen von MSO-beschreibbaren Problemen. Die Probleme unterscheiden sich in der Art ihrer Lösung – Entscheidungs- und Histogrammproblem – und in der Art der betrachteten Eingabe – Graphen mit beschränkter Baumtiefe, Graphen mit gegebener Baumzerlegung in Klammerdarstellung und Graphen mit beschränkter Baumweite.

Es bleiben eine Reihe offener Fragen zurück: Aufbauend auf jedem Satz kann man Fragen, ob der Satz immer noch gilt, wenn man anstatt MSO-Logik eine Logik mit größerer

Ausdrucksstärke verwenden. Auch wäre es interessant zu wissen, ob ein Satz noch gilt, wenn man größere Mengen von Graphen als Eingabe betrachtet. Allgemein stellt sich die Frage, ob es ähnliche Sätze (basierend auf einer Logik, graphentheoretischen Konzepten und vielen Anwendungen) für andere Komplexitätsklassen gibt.

Literatur

[All04] Eric Allender. Arithmetic Circuits and Counting Complexity Classes. In Jan Krajíček, Hrsg., *Complexity of Computations and Proofs*, Jgg. 13 of *Quaderni di Matematica*, Seiten 33–72. Seconda Universita di Napoli, 2004.

[BCGR92] S. Buss, S. Cook, A. Gupta und V. Ramachandran. An optimal parallel algorithm for formula evaluation. *SIAM Journal on Computing*, 21(4):755–780, 1992.

[Cou90] Bruno Courcelle. Graph rewriting: An algebraic and logic approach. In Jan van Leeuwen, Hrsg., *Handbook of Theoretical Computer Science, Volume B: Formal Models and Semantics*, Seiten 193–242. Elsevier and MIT Press, 1990.

[EGT12] Michael Elberfeld, Martin Grohe und Till Tantau. Where First-Order and Monadic Second-Order Logic Coincide. In *Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2012)*, Seiten 265–274. IEEE Computer Society, 2012.

[Elb12] Michael Elberfeld. *Space and Circuit Complexity of Monadic Second-Order Definable Problems on Tree-Decomposable Structures*. Universität zu Lübeck, 2012. Dissertation.

[Imm99] Neil Immerman. *Descriptive complexity*. Springer, 1999.

[NO12] Jaroslav Nešetřil und Patrice Ossona de Mendez. *Sparsity: Graphs, Structures, and Algorithms*. Springer, 2012.

[Rei08] Omer Reingold. Undirected connectivity in log-space. *Journal of the ACM*, 55(4):1–24, 2008.

[Vol99] Heribert Vollmer. *Introduction to Circuit Complexity: A Uniform Approach*. Springer, 1999.



Michael Elberfeld absolvierte von 2002 bis 2007 ein Studium der Informatik an der Universität zu Lübeck, das er im September 2007 als Diplom-Informatiker abschloss. Nach dem Studium war er vom Oktober 2007 bis September 2012 als wissenschaftlicher Mitarbeiter am Institut für Theoretische Informatik der Universität zu Lübeck tätig. Seine Forschung konzentrierte sich Anfangs auf das Design und die Anwendung von Algorithmen in der Bioinformatik. Im Sommer 2009 kam die Forschung im Bereich der Komplexitäts- und Modelltheorie hinzu, die in die hier besprochene Dissertation mündete. Seit September 2012 wird er durch ein Postdoktoranden-Stipendium der DAAD gefördert und arbeitet an platzeffizienten Algorithmen zur Lösung von Pfadproblemen am ICSI in Berkeley und NII in Tokio.

Kulturelle Vielfalt für virtuelle Charaktere*

Birgit Endrass

Institut für Angewandte Informatik
Universität Augsburg
endrass@hcm-lab.de

Abstract: In dieser Dissertation wurden kulturspezifische Verhaltensweisen unterschiedlicher Modalitäten für die Verwendung in Multiagentensystemen aufbereitet. Dabei wurde ein hybrider Ansatz verfolgt, der sowohl generalisierbare Modelle auf Grundlage der Literatur aus den Sozialwissenschaften implementiert als auch Verhaltensweisen auf Grundlage eines Videokorpus simuliert. Kulturelle Unterschiede im Verhalten wurden für die deutsche und japanische Kultur exemplarisch dargestellt und in eine Simulation mit virtuellen Charakteren integriert. In Evaluationsstudien wurde die Wahrnehmung der einzelnen Verhaltensaspekte von Nutzern der beiden Zielkulturen untersucht.

1 Einführung

Kultur spielt eine wichtige Rolle in unserem Leben. Auf meist unterbewusster Ebene beeinflusst sie unsere Entscheidungen und Bewertungen bezüglich unserer Umgebung. Sprache ist meist die größte Barriere, wenn Menschen unterschiedlicher Kulturen miteinander kommunizieren. Aber selbst wenn beide Gesprächspartner dieselbe Sprache sprechen, kann es aufgrund des kulturellen Unterschieds zu Missverständnissen kommen, da menschliche Kommunikation wesentlich mehr beinhaltet, als den Inhalt der gesprochenen Sprache. Ein Beispiel für solch einen Verhaltensunterschied stellt die Art dar, wie eine Konversation geführt wird. Den Kommunikationspartner zu unterbrechen wird in manchen Kulturen, wie z.B. in Deutschland, als unhöflich empfunden. Im Gegensatz dazu wird es in anderen Kulturen, wie z.B. in Ungarn, positiv, als gesteigertes Interesse in die laufende Konversation bewertet. Eine Konversation, in der kontroverse Kulturen aufeinander treffen, birgt hohes Konfliktpotential. Während sich der eine Gesprächspartner beleidigt fühlen kann, da er unterbrochen wurde, könnte der andere den Eindruck haben, dass der Gesprächspartner nicht an der Unterhaltung interessiert ist. In beiden Fällen würde ein negativer Eindruck über das Gespräch entstehen. Dieser Eindruck wird allerdings von Nicht-Experten in interkultureller Kommunikation nicht als kulturelles Missverständnis wahrgenommen, sondern resultiert häufig in einer generellen Ablehnung des Gesprächspartners.

Auf ähnliche Art und Weise können auch computerbasierte Systeme aufgrund des kulturellen Hintergrunds des Benutzers missverstanden werden. Wenn der Programmierer

*Englischer Titel der Dissertation: "Cultural Diversity for Virtual Characters: Investigating Behavioral Aspects across Cultures" [End12]

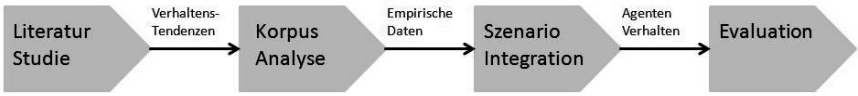


Abbildung 1: Arbeitsfluss des hybriden Ansatzes.

einer Software beispielsweise einen gewissen Eindruck beim Benutzer erwecken will, muss dieser die Intention nicht zwangsläufig verstehen und könnte sie anders wahrnehmen. Bezüglich virtueller Charaktere können diese Unterschiede noch eine entscheidendere Rolle spielen, da die Charaktere darauf abzielen, menschliches Verhalten auf natürliche Art und Weise zu simulieren. Wenn kulturelle Unterschiede bei der Verhaltensmodellierung von virtuellen Charakteren ignoriert werden, wird das Modell unter Umständen von gewissen Nutzergruppen nicht akzeptiert. Nichtsdestotrotz gibt es erst sehr wenige Forschungsprojekte, die kulturspezifisches Verhalten explizit modellieren.

In vorliegender Dissertation wurde die Simulation von Kultur mit virtuellen Charakteren erforscht. Dabei lag der Fokus auf der Generierung von kulturspezifischen Verhaltensweisen, wobei Kultur als Parameter in die Verhaltensmodelle von virtuellen Charakteren integriert wurde, anstatt offensichtliche Unterschiede wie äußere Erscheinung oder Sprache, zu simulieren.

2 Ansatz

Prinzipiell können zwei Ansätze zur Integration von sozialen Aspekten, wie z.B. Kultur, in die Verhaltenssteuerung von virtuellen Charakteren verfolgt werden: modellbasiert oder datengetrieben. Beim modellbasierten Ansatz werden Definitionen von verhaltensbasierten Merkmalen aus der Literatur extrahiert, operationalisiert und in eine Agentenarchitektur integriert, wie es z.B. für Persönlichkeit [AKG+00] oder Emotionen [GRA+02] erfolgreich demonstriert wurde. Im Gegensatz dazu handelt es sich beim datengetriebenen Ansatz um ein statistisches Verfahren, welcher menschliches Verhalten, z.B. aus multimodalen Korpora, analysiert und extrahierte Merkmale anschließend mit virtuellen Agenten simuliert. Datengetriebene Ansätze sind eher selten, da die Sammlung adäquater multimodaler Korpora zeit- und ressourcenintensiv ist. Während frühere Arbeiten sich meist auf ein Verhaltensmerkmal, wie z.B. Gesten während Wegbeschreibungen [Cas07], konzentrieren, ist die Sammlung und Aufbereitung eines standardisierten multimodalen Korpus über mehrere Kulturen, wie in dieser Dissertation verwendet [RAN+07], neuartig.

In dieser Dissertation wurde erstmals ein hybrider Ansatz entwickelt, der die Vorteile des modellbasierten Ansatzes und des datengetriebenen Ansatzes vereint, wobei Aspekte des verbalen Verhaltens, Kommunikationsmanagement, sowie des nonverbalen Verhaltens behandelt und für die deutsche und japanische Kultur implementiert wurden. Durch die Analyse konkreter Beispiele menschlichen Verhaltens werden statistische Daten gewonnen, welche die aus der Literatur extrahierten Tendenzen in empirische Grundlagen manifestiert. Abbildung 1 verdeutlicht diesen Ansatz, der im Folgenden im Detail beschrieben wird.

Literaturstudie Als erster Schritt des Arbeitsflusses wurde einschlägige Literatur aus den Sozialwissenschaften untersucht, um kulturspezifische Unterschiede im Verhalten für die zu untersuchenden Kulturen zu extrahieren. Die daraus resultierenden Verhaltenstendenzen dienen weiter als Grundlage für die empirische Studie.
Korpusanalyse Als nächster Schritt werden die aus der Literatur extrahierten Tendenzen in empirischen Daten grundiert. Dafür wurde ein Videokorpus in den beiden Zielkulturen aufgezeichnet und aufgrund der zuvor gewonnenen Erwartungen analysiert, um zusätzliche statische Informationen zu gewinnen, wie z.B. die Häufigkeit des Auftretens eines Merkmals.
Verhaltensgenerierung Aufgrund der Resultate der Literatur- und Korpusstudien wurden Modelle zur Verhaltenssteuerung von Multiagentensystemen erstellt. Zur Demonstration wurde ein Simulator entwickelt, welcher kulturspezifisches Verhalten für virtuelle Charaktere generiert.
Evaluation Letztlich wurden die kulturellen Unterschiede im Verhalten der virtuellen Charaktere in den Zielkulturen evaluiert, um deren Einfluss auf die Wahrnehmung von menschlichen Beobachtern zu untersuchen.

3 Theoretischer Hintergrund

In den Sozialwissenschaften gibt es unterschiedliche Ansätze um Kultur zu definieren. Für die Integration in Multiagentensysteme sind dimensionale Kulturmodelle (wie z.B. [HHM10]) und Dichotomien (wie z.B. [Hal66] [Hal83]) besonders geeignet, da sie kulturelle Unterschiede strukturiert und formal beschreiben. Verschiedene Kulturtheorien (u.a. [HHM10, Hal66, Hal83, TT99]) wurden in dieser Dissertation verwendet, um die deutsche und japanische Kultur zu kategorisieren.

Für die Simulation in virtuellen Welten sind mehrere Aspekte menschlichen Verhaltens interessant, welche einerseits von Kultur abhängig, und andererseits den Modalitäten von virtuellen Charakteren entsprechen. Bezüglich verbalen Verhaltens wurde in dieser Dissertation das Thema Small Talk fokussiert, da es eine prototypische Konversation darstellt die bei ersten Treffen sowohl innerhalb eines Kulturkreises, als auch bei interkulturellen Zusammentreffen stattfindet. Zur Kontrolle des Gesprächsflusses werden sogenannte verbale Regulatoren verwendet, welche stark vom kulturellen Hintergrund beeinflusst werden [TT99]. In dieser Dissertation wurden Gesprächspausen sowie überlappende Sprache untersucht. Bezüglich des nonverbalen Verhaltens variiert sowohl die Auswahl des gezeigten Verhaltens, als auch deren Ausführung [TT99] abhängig von kulturellem Hintergrund.

Aufgrund der erstellten kulturellen Profile und deren Bezug zu den relevanten Verhaltensaspekten wurden Erwartungen für die deutsche und japanische Kultur erstellt und in Tabelle 1 zusammengefasst [HHM10] [Hal66] [Hal83] [TT99]. Bezüglich Small Talk Verhaltens erwarten wir privatere Themen in prototypischen deutschen Konversationen, und entsprechend weniger private Themen in prototypischen japanischen Gesprächen. Des weiteren erwarten wir einen Unterschied in der Organisation der Gespräche, vor allem in der Reihenfolge der besprochen Themen. Im Kommunikationsmanagement nehmen wir ein Vermeiden von Gespächspausen in der deutschen Kultur an, während viele Pausen in japanischen Konversationen zu erwarten sind, da hier Pausen als Zeichen von Respekt gewertet werden. Bezüglich überlappender Sprache rechnen wir mit mehr Überlappungen in

Verhaltensaspekt	Deutschland	Japan
Themenwahl	privat	weniger privat
Gesprächsfluss	sequenziell	alternierend
Pausen	vermieden	bewusst eingesetzt
Überlappungen	unüblich	üblich als Feedback
Gestentypen	direkte Gesten üblich	metaphorische Gesten üblich
nonverbale Expressivität	expressiv	weniger expressiv

Tabelle 1: Aus der Literatur extrahierte Erwartungen an die deutsche und japanische Kultur.

japanischen Konversationen, da hier konstantes verbales Feedback üblich ist. Außerdem zeigen individualistische Kulturen wie Deutschland mehr persönliche Emotionen in der Öffentlichkeit [TT99]. Darum erwarten wir expressiveres nonverbales Verhalten und mehr direkte Gesten in prototypischen deutschen Konversationen als in japanischen.

4 Verwandte Arbeiten

Durch enorme Fortschritte im Bereich Computergraphik und -animation werden virtuelle Charaktere vom Benutzer zunehmend als belebte eigenständige Wesen mit humanoiden Verhalten wahrgenommen. Um diese Wirkung zu verstärken wurden in früheren Ansätzen persönliche Faktoren, wie Persönlichkeit [AKG+00] oder emotionaler Zustand [PCdC+02], in das Agentenverhalten integriert um dem Benutzer zu ermöglichen die virtuellen Charaktere als Individuen zu identifizieren. Mit der Entwicklung hin zu Multiagentensystemen, in welchen virtuelle Agenten als Gruppe agieren, wurde die Integration von kulturellem Hintergrund in jüngster Zeit zu einem interessanten Forschungsthema.

Die Mehrzahl an Arbeiten, welche sich mit der Integration von kulturellem Hintergrund befassen, fokussieren das Trainieren von interkulturellen Fähigkeiten und ist meist in der Militärdomäne zu finden. In diesen Ansätzen werden typischerweise konkrete Fähigkeiten erlernt. Dabei werden meist nationale Kulturen simuliert. Ein bekanntes Beispiel hierfür ist das Tactical Language Training System (TLTS) [JMV04] das Konversationsfähigkeiten in fremden Sprachen wie Irakisch vermittelt, oder das BiLAT System [KHD+09] welches Verhandlungsgeschick mit fremden Kulturen trainiert. Im Gegensatz dazu zielen didaktische Ansätze für Kinder und Jugendliche, wie z.B. das ORIENT System [APV+09] häufig auf ein generelles kulturelles Verständnis ab, indem sie abstrakte Fantasiekulturen verwenden welche nach ihren eigenen, meist weltfremden, Regeln agieren.

Weitere verwandte Arbeiten befassen sich mit Forschungsstudien um weitere Einsichten darin zu gewinnen, wie virtuelle Charaktere von menschlichen Nutzern wahrgenommen werden. Arbeiten wurden beispielsweise von Koda und Kollegen [KRA08] durchgeführt, wobei die unterschiedliche Wahrnehmung von Gesichtsausdrücken von Avataren über unterschiedliche Kulturen untersucht wurde. Ein weiteres Beispiel ist eine Studie von Yin und Kollegen [YBC10] in der eine Reihe von Aspekten wie äußere Erscheinung, Sprache oder die Art zu argumentieren, für die anglo-amerikanische und latein-amererikanische Kulturen untersucht wurden.

Diese Dissertation ist in die Gruppe der Forschungsstudien einzuordnen, da es ihr Ziel ist kulturspezifische Aspekte des Verhaltens zu modellieren und die Wirkung deren Simulation mit virtuellen Charakteren auf Nutzer der dargestellten Kulturen zu untersuchen. Im Gegensatz zu früheren Arbeiten verwendet sie operationalisierbaren theoretischen Hintergrund in Verbindung mit empirisch fundierten Daten und stellt somit adäquate Modelle zur Generalisierung von kulturspezifischem Verhalten bereit.

5 Empirischer Hintergrund

Um Tendenzen aus der Literatur in empirische Daten zu begründen, wurde die Methode der Annotation und Analyse von multimodalen Korpora angewandt. Diese Methode wurde bereits erfolgreich angewandt um individualisierte virtuelle Charaktere zu kreieren [MAD+05] und erscheint auch für die Integration von kulturellem Hintergrund sehr geeignet.

Diese Dissertation wurde im Rahmen des DFG-Projektes Cube-G durchgeführt [RAN+07] in welchem ein Video Korpus in den deutschen und japanischen Kulturen aufgezeichnet wurde. Die entscheidende Frage hierbei ist ob sich kulturabhängige Merkmale aus einem Datensatz von 20 aufgezeichneten Konversationen pro Kultur extrahieren lassen. Der transkulturelle Korpus wurde hinsichtlich der Verhaltensaspekte untersucht, welche sich zuvor als für unsere Zwecke relevant herausgestellt haben. Dazu mussten die Verhaltensaspekte in geeigneten Annotationsschemen parametriert werden.

Zur Annotation des verbalen Verhaltens wurde die Sprache beider Gesprächspartner transkribiert und übersetzt. Zusätzlich wurden Sprechakte nach dem DAMSL Kodierungsschema [CA97] bezeichnet, wobei Äußerungen wie Frage, Antwort oder Zustimmung kategorisiert wurden. Bezüglich des Inhalts der Sprache wurden Themen welche in den Konversationen vorkamen annotiert und in die Kategorien Umgebung, Extern und Privat eingeteilt [Sch88]. Pausen und Überlappungen wurden nicht explizit annotiert, sondern aus den Annotationen der Sprache berechnet. Zur Annotation des nonverbalen Verhaltens wurden Gesten und Körperhaltungen untersucht. Gesten wurden nach McNeills Gestenklassifizierung [McN92] annotiert, welche Gesten nach Typen, wie z.B. deiktisch oder ikonisch unterscheidet. Zusätzlich wurden Expressivitätsparameter [MAD+05], wie Geschwindigkeit oder räumliche Ausdehnung annotiert. Zur Annotation von Körperhaltung wurde Bulls Kodierungsschema [Bul87] herangezogen, wobei Armhaltungen wie PHEb (Hand hält den Ellenbogen) oder PHB (Hände hinter dem Rücken) untersucht wurden.

Eine Analyse des verbalen Verhaltens ergab signifikante Unterschiede bezüglich der Themenwahl während der Small Talk Situationen. Im Besonderen traten Themen, welche die Umgebung oder externe Situation betrafen in japanischen Konversationen häufiger auf als in deutschen, während private Themen in den deutschen Konversationen häufiger auftraten. Ein Vergleich der Sprechakte ergab signifikante Unterschiede in der Verwendung von Fragen und Antworten sowie Zustimmungs- und Verstehensakten. Zur Analyse des Kommunikationsmanagement wurden entweder Zeitspannen untersucht in welchen keiner der Gesprächspartner sprach oder beide gleichzeitig sprachen. Wie erwartet fanden wir signifikant mehr Pausen in den japanischen Konversationen verglichen mit den deutschen. Bezüglich überlappender Sprache fanden wir nicht die erwarteten Unterschiede in

der Häufigkeit ihres Auftretens. Bisher wurde in der Analyse noch keine Semantik untersucht. Die Analyse des verbalen Verhaltens lässt allerdings auf Unterschiede in der Qualität des Komminkationsmanagements schließen.

Beim Vergleich der Gestentypen ergaben sich signifikant mehr Adaptor Gesten im japanischen Datensatz als im deutschen. Bezüglich der Expressivität der Gesten ergaben sich signifikante Werte für alle untersuchten Parameter. Gesten wurden in den deutschen Konversationen schneller, mit mehr Kraft, höherer räumlicher Ausdehnung, flüssiger und mit weniger Wiederholungen ausgeführt, als in den japanischen Konversationen.

Die Analyse der Körperhaltungen ergab interessante Einblicke dahingehend, welche Körperhaltungen typischerweise in den beiden Kulturen vorkommen. Während beispielsweise verschränkte Arme oder Hände in den Hosentaschen in deutsche Konversationen häufig auftraten, wurden in japanischen Konversationen die Hände oft gefaltet beobachtet (siehe Abbildung 2).

6 Konzeptuelles Design und Implementierung

Bei der technischen Umsetzung mussten nicht nur Herausforderungen gelöst werden die typischerweise in Multiagentensystemen auftreten, wie z.B. Dialogplanung oder die Generierung von realistischem nonverbalen Verhalten, sondern diese zusätzlich parametriert werden, um verschiedene kulturelle Hintergründe zu simulieren.

In der Domäne der Dialoggenerierung haben sich planbasierte Ansätze als sehr geeignet herausgestellt um Aspekte wie z.B. Persönlichkeit zu simulieren [AKG+00]. Planbasierte Ansätze bieten ein hohes Ma an Flexibilität und Erweiterbarkeit. Indem lediglich der Dialogfluss geplant wird, werden Sprechakte auf abstrakter Ebene unabhängig vom konkreten Wortlaut strukturiert. Auf diese Art und Weise können z.B. Templates für weitere Themen zur Wissensbasis hinzugefügt werden ohne den Planungsalgorithmus verändern zu müssen.

Zur Implementierung des verbalen Verhaltens wurde in dieser Dissertation ein hierarchischer Planer [NCLMA99] zu einem verteilten Planungssystem erweitert, welches autonome Dialogplanung zur Laufzeit ermöglicht. Zur Realisierung kulturabhängiger Themenwahl in Small Talk Dialogen, wurden mögliche Themen analog zur empirischen Studie kategorisiert. Der Planungsalgorithmus bestimmt die Wahrscheinlichkeit einer Themenkategorie abhängig vom kulturellen Hintergrund des Agenten um beispielsweise mehr private Themen für eine prototypisch deutsche Unterhaltung zu generieren. Um nicht-monotones Verhalten zu gewährleisten wurden persönliche Motivationen hinzugefügt, welche die Verhaltensselektion zusätzlich beeinflussen. Außerdem wird der Gesprächsfluss im System von kulturellem Hintergrund beeinflusst, indem der Planungsalgorithmus bestimmt wie schwierig es mit einem gegebenen kulturellen Hintergrund ist, ein Thema abzubrechen und damit den Gesprächsfluss zu unterbrechen.

Bezüglich der Anpassung nonverbalen Verhaltens haben sich Ansätze, welche Bayessche Netze verwenden als geeignet herausgestellt [BK09] und werden in dieser Dissertation verwendet, um die Expressivität des nonverbalen Verhaltens anzupassen. Zur Modellierung wurde Hofstedes dimensionales Kulturmodell [HHM10] als Grundlage verwendet.



Abbildung 2: Kulturspezifische Körperhaltungen im Videokorpus sowie in der Agentensimulation.

Der Ansatz mit Bayesschen Netzen ermöglicht mit dem unsicherem Wissen zu arbeiten, welches aus der Tatsache heraus entsteht dass es keine klare Abbildung von kulturellen Dimensionen zum resultierenden nonverbalen Verhalten gibt. Außerdem erlaubt der Ansatz, Verhaltensmerkmale anzupassen ohne eine gewisse Variabilität einzubüßen, welche notwendig ist damit einzelne Charaktere als Individuen wahrgenommen werden. In der Simulation werden, abhängig von den Wahrscheinlichkeiten des Baysesschen Netzes, Animationen an verschiedene Level der Expressivität angepasst, und beispielsweise mit höherer Geschwindigkeit oder höherer räumlichen Ausdehnung abgespielt. Da dieser Ansatz nicht in allen Fällen anwendbar ist, da beispielsweise eine Begrüßungsgeste, wie z.B. winken, nicht durch Anpassung der Expressivität in z.B. eine Verbeugung umgewandelt werden kann, wurden zusätzliche Animationen auf Grundlage des Korpus modelliert. Dies wurde beispielsweise für prototypische Körperhaltungen durchgeführt. Abbildung 2 zeigt prototypische Körperhaltungen aus dem Videokorpus sowie deren Modellierung mit Agenten in einer virtuellen Umgebung [DEH+11].

7 Evaluation

Um zu untersuchen, ob die implementierten Verhaltensunterschiede eine Auswirkung auf menschliche Beobachter haben, wurden Evaluationsstudien in der deutschen und japanischen Kultur durchgeführt, wobei jeder Verhaltensaspekt in Isolation untersucht wurde, um deren Einfluss auf die menschliche Wahrnehmung herauszufinden. Dazu wurden zwei separate Studien aufgesetzt [EARN13]: eine für das verbale Verhalten, und eine andere für Kommunikationsmanagement und nonverbales Verhalten. Diese Unterscheidung war notwendig, da die verschiedenen Faktoren einen Einfluss aufeinander haben und somit die Wahrnehmung der Benutzer beeinflussen können.

Für beide Studien wurden zwei Versionen entworfen, zur Durchführung in Deutschland bzw. in Japan, die jeweils virtuelle Charaktere und Sprachsysteme enthalten, die dem kulturellen Hintergrund der Beobachter entsprechen. In jeder der Studien nahmen wir an, dass menschliche Beobachter Agentenverhalten bevorzugen, welches dem eigenen kulturellen Hintergrund entspricht.

In der ersten Studie wurde kulturabhängige Themenwahl untersucht. Die Ergebnisse zeigen, dass deutsche Beobachter die prototypisch deutsche Dialogversion signifikant angemessener und interessanter empfanden, lieber an dem Dialog teilnehmen würden und dachten, dass die Agenten besser miteinander auskamen. Ergebnisse der japanischen Studie zeigen, dass japanische Teilnehmer die japanischen Versionen signifikant angemessener und interessanter empfanden und dachten, dass die Agenten besser miteinander auskamen.

Die zweite Studie untersucht die unterschiedliche Verwendung von Sprechpausen, Überlappungen, Gestengeschwindigkeit, räumlicher Ausdehnung und Körperhaltung. Die Ergebnisse zeigen, dass deutsche Teilnehmer für manche Aspekte das prototypisch deutsche simulierte Verhalten signifikant bevorzugten (für überlappende Sprache und räumliche Ausdehnung der Gesten). Bei allen anderen Aspekten war ein Trend zur deutschen Verhaltensversion hin erkennbar. Ergebnisse der japanischen Studie zeigen, dass japanische Teilnehmer signifikant die simulierte japanische Körperhaltung bevorzugten. Der einzige gegensätzliche Trend war im Kommunikationsmanagement zu beobachten, wobei japanische Teilnehmer das prototypisch deutsche Pausen- und Überlappungsverhalten bevorzugten, wenn auch nicht signifikant.

8 Beitrag

In dieser Dissertation wurde erstmals ein hybrider Ansatz verfolgt der kulturspezifisches Verhalten für die Verwendung in Multiagentensystemen aufbereitet. Dazu wurden nicht nur operationalisierbare Kulturmodelle aus den Sozialwissenschaften identifiziert, sondern auch eine umfangreiche Korpusanalyse in verschiedenen Kulturen durchgeführt.

Zahlreiche Konzepte, welche im Rahmen dieser Dissertation entwickelt wurden, können weiterhin in der Verhaltensgenerierung Verwendung finden. So wurden validierte Annotationsschemata zur Kodierung menschlichen Verhaltens entworfen, parametrierbare Modelle zur kulturspezifischen Verhaltensgenerierung implementiert, sowie eine Simulationsumgebung mit kulturspezifischen virtuellen Charakteren entwickelt.

Besonders fr diejenigen Verhaltensaspekte bei welchen unsere Evaluationsstudien zeigten, dass sie die Perzeption von Nutzern unterschiedlicher Kulturen positiv beeinflussen, empfehlen wir deren Beachtung bei der Modellierung von virtuellen Charakteren.

Obwohl der Arbeitsfluss dieser interdisziplinären Dissertation auf zwei nationale Kulturen angewandt wurde (Deutschland und Japan), ist der Ansatz von genereller Natur und kann sowohl als Leitfaden für weitere Ansätze der kulturspezifischen Verhaltensgenerierung, als auch für andere Merkmale wie z.B. Integration von Persönlichkeit dienen. Der entwickelte hybride Ansatz wurde bereits erfolgreich auf zwei weitere Kulturen, Arabien und USA, übertragen [EHAG10].

9 Danksagung

Als erstes möchte ich meiner Promotionsbetreuerin Prof. Dr. Elisabeth Andr für ihre Unterstützung und Engagement während der Betreuung meiner Arbeit danken. Mein besonderer Dank gilt auch meinem Zweitbetreuer Prof. Dr. Matthias Rehm für seine Hilfe und Unterstützung während dieser Jahre. Außerdem möchte ich unseren japanischen Kooperationspartnern Yukiko Nakano und Toyoaki Nishida danken.

Literatur

[AKG+00] Elisabeth André, Martin Klesen, Patrick Gebhard, Steve Allen und Thomas Rist. Integrating Models of Personality and Emotions into Lifelike Characters. In *Affective Interactions*, Seiten 150–165. Springer, 2000.

[APV+09] R. Aylett, A. Paiva, N. Vannini, S. Enz, E. André und L. Hall. But that was in another country: agents and intercultural empathy. In *Proc. of 8th Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS 2009)*, 2009.

[BK09] K. Bergmann und S. Kopp. Bayesian Decision Networks for Iconic Gesture Generation. In *Proc. of 9th Int. Conf. on Intelligent Virtual Agents (IVA 2009)*, Seiten 76–89. Springer, 2009.

[Bul87] P.E. Bull. *Posture and Gesture*. Pergamon Press, Oxford, 1987.

[CA97] Mark Core und James Allen. Coding Dialogs with the DAMSL Annotation Scheme. In *Working Notes of AAAI Fall Symposium on Communicative Action in Humans and Machines*, 1997.

[Cas07] J. Cassell. Body Language: Lessons from the Near-Human. In J. Riskin, Hrsg., *Genesis Redux: Essays in the History and Philosophy of Artificial Intelligence*, Seiten 346–374. University of Chicago Press, Chicago, 2007.

[DEH+11] Ionut Damian, Birgit Endrass, Peter Huber, Nikolaus Bee und Elisabeth André. Individualized Agent Interactions. In *Proc. of 4th Int. Conf. on Motion in Games (MIG 2011)*, 2011.

[EARN13] Birgit Endrass, Elisabeth André, Matthias Rehm und Yukiko Nakano. Investigating culture-related aspects of behavior for virtual characters. *Autonomous Agents and Multi-Agent Systems*, 2013.

[EHAG10] B. Endrass, L. Huang, E. André und J. Gratch. A data-driven approach to model Culture-specific Communication Management Styles for Virtual Agents. In *Proc. of 9th Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS 2010)*, Seiten 99–108, 2010.

[End12] Birgit Endrass. *Cultural Diversity for Virtual Characters: Investigating Behavioral Aspects across Cultures*. Dissertation, Augsburg University, Germany, 2012.

[GRA+02] J. Gratch, J. Rickel, E. André, N. Badler, J. Cassell und E. Petajan. Creating Interactive Virtual Humans: Some Assembly Required. *IEEE Intelligent Systems*, 17(4):54–63, 2002.

[Hal66] Edward T. Hall. *The Hidden Dimension*. Doubleday, 1966.

[Hal83] E.-T. Hall. *The Dance of Life*. Doubleday, New York, 1983.

[HHM10] Geert Hofstede, Gert-Jan Hofstede und Michael Minkov. *Cultures and Organisations. SOFTWARE OF THE MIND. Intercultural Cooperation and its Importance for Survival*. McGraw Hill, 2010.

[JMV04] W.-J. Johnson, S. Marsella und H. Vilhjálmsson. The DARWARS Tactical Language Training System. In *Interservice / Industry Training, Simulation, and Education Conference*, 2004.

[KHD+09] J. Kim, R.-W. Hill, P. Durlach, H.-C. Lane, E. Forbell, M. Core, S. Marsella, D. Pynadath und J. Hart. BiLAT: A game-based environment for practicing negotiation in a cultural context. *International Journal of Artificial Intelligence in Education*, 19:289–308, 2009. IOS Press.

[KRA08] T. Koda, M. Rehm und E. André. Cross-Cultural Evaluations of Avatar Facial Expressions Designed by Western Designers. In *Proc. of 8th Int. Conf. on Intelligent Virtual Agents (IVA 2008)*, Seiten 245–252. Springer, 2008.

[MAD+05] Jean-Claude Martin, Sarkis Abrilian, Laurence Devillers, Myriam Lamolle, Maurizio Mancini und Catherine Pelachaud. Levels of Representation in the Annotation of Emotion for the Specification of Expressivity in ECAs. In *Proc. of 5th Int. Conf. on Intelligent Virtual Agents (IVA 2005)*, Seiten 405–417. Springer, 2005.

[McN92] David McNeill. *Hand and Mind What Gestures Reveal about Thought*. University of Chicago Press, Chicago, London, 1992.

[NCLMA99] Dana Nau, Yue Cao, Amnon Lotem und H. Munoz-Avila. SHOP: Simple Hierarchical Ordered Planner. In *Proc. of 16th Int. Joint Conf. on Artificial Intelligence (IJCAI 1999)*, Seiten 968–973, 1999.

[PCdC+02] C. Pelachaud, V. Carofiglio, B. de Carolis, F. de Rosis und I. Poggi. Embodied contextual agent in information delivering application. In *Proc. of 1st Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS 2002)*, Seiten 758 –765. ACM, 2002.

[RAN+07] Matthias Rehm, Elisabeth André, Yukiko Nakano, Toyoaki Nishida, Nikolaus Bee, Birgit Endrass, Hung-Hsuan Huan und Michael Wissner. The CUBE-G approach - Coaching culture-specific nonverbal behavior by virtual agents. In *ISAGA 2007: Organizing and Learning through Gaming and Simulation*, 2007.

[Sch88] K. P. Schneider. *Small Talk: Analysing Phatic Discourse*. Hitzeroth, Marburg, 1988.

[TT99] S. Ting-Toomey. *Communicating across cultures*. The Guilford Press, New York, 1999.

[YBC10] Langxuan Yin, Timothy Bickmore und D.-E. Cortés. The Impact of Linguistic and Cultural Congruity on Persuasion by Conversational Agents. In *Proc. of 10th Int. Conf. on Intelligent Virtual Agents (IVA 2010)*, Seiten 343–349. Springer, 2010.



Birgit Endrass ist akademische Rätin an der Universität Augsburg. Für ihre Dissertation erhielt sie das Zertifikat summa cum laude, den Wissenschaftspreis der Universität Augsburg sowie den IFAAMAS-12 Victor Lesser Distinguished Dissertation Award. Als Doktorandin absolvierte sie mehrmonatige Praktika an renommierten Instituten: INESC-ID (Lissabon, Portugal), National Institute for Informatics (Tokio, Japan) und Institute for Creative Technologies (Los Angeles, USA), und arbeitete aktiv in mehreren internationalen Projekten mit.

Randomisiertes Rumor Spreading auf Sozialen Netwerken und Vollständigen Graphen*

Mahmoud Fouz

Universität des Saarlandes
mahmoudfouz@gmail.com

Abstract: Nicht zuletzt wegen dem Einfluss des Internets ist die Analyse der Verbreitung von Informationen in komplexen Netzwerken ein wichtiger Forschungsbereich. In meiner Dissertation beschäftigen wir uns mit zwei Problemstellungen in diesem Zusammenhang. Im ersten Teil untersuchen wir die Verbreitung von Informationen in sozialen Netzwerken. Hierzu benutzen wir das "Preferential Attachment"-Graph Modell. Wir beweisen, dass ein natürliches Protokoll zur Verbreitung von Informationen sublogarithmische Zeit benötigt in der Größe des Netzwerks, um eine Nachricht von einem Knoten zu allen Knoten zu verbreiten. Im Gegensatz dazu benötigt das Protokoll auf allen vorher untersuchten Netzwerktopologien mindestens logarithmische Zeit. Im zweiten Teil betrachten wir die Verbreitung von Informationen auf vollständigen Graphen. Wir führen ein neues Protokoll ein, das eine Laufzeit von $(1 + o(1)) \log_2 n$ erreicht. Dies ist asymptotisch optimal unter allen Protokollen, bei denen nur informierte Knoten an der Nachrichtenübertragung aktiv beteiligt sind und zudem in jedem Schritt höchstens einen Nachbarknoten informieren können. Dabei braucht es lediglich $O(nf(n))$ Nachrichten, wobei $f(n) = \omega(1)$ beliebig ist.

1 Einleitung

Wir leben im Informationszeitalter. Die Menge an Informationen, die täglich aufkommt, verarbeitet und verbreitet wird, ist enorm. Die weltweit fast unmittelbare Verfügbarkeit von Informationen ist dabei zu einem der stärksten Katalysatoren der Globalisierung geworden. Sie hat unmittelbaren Einfluss darauf, wie wir denken, arbeiten und leben. Es ist daher von großer Bedeutung zu verstehen, wie Informationen sich ausbreiten.

Dabei unterscheiden wir zwei Sichtweisen. Zum einen kann man bestehende Prozesse untersuchen, die bekanntermaßen eine schnelle Informationsausbreitung fördern. Hierzu werden theoretische Modelle der Informationsausbreitung in realen Netzwerken untersucht. Zum anderen kann man neue Algorithmen entwickeln, die eine schnelle Informationsausbreitung garantieren. Beide Sichtweisen ergänzen sich: ein besseres Verständnis der bestehenden Prozesse kann uns dabei helfen, neue Algorithmen zu entwickeln. Andererseits dienen einfache Algorithmen als Modelle für real existierende Prozesse.

In meiner Dissertation tragen wir zu beiden Sichtweisen bei. Im ersten Teil untersuchen

*Originaltitel der Arbeit: Randomized Rumor Spreading in Social Networks and Complete Graphs

wir einen natürlichen Ausbreitungsprozess auf *Preferential Attachment Graphen* (kurz PA-Graphen). Die theoretische Analyse dieses Prozesses zeigt dabei besondere Eigenschaften auf, die in realen Netzwerken eine schnelle Verbreitung von Informationen ermöglichen. Im zweiten Teil stellen wir eine einfache und aymptotisch optimale Lösung für das klassische "Telefonkettenproblem" vor: eine Person möchte eine Nachricht innerhalb einer Gruppe von Leuten so schnell wie möglich verbreiten. Unser Ansatz verbessert vorherige Algorithmen in Bezug auf Laufzeit, Skalierbarkeit und Robustheit.

Formal nehmen wir an, dass in einem gegeben Graphen G zu Beginn genau ein Knoten (*Quelle*) informiert ist. Das Ziel ist diese Information an alle Knoten im Graphen zu verteilen. Der Informationsaustausch kann dabei nur zwischen benachbarten Knoten stattfinden. Wir nennen solche Algorithmen auch *Rumor Spreading* Prozesse oder *Protokolle*.

Gewöhnlich nehmen wir an, dass jeder Knoten höchstens einen Nachbarknoten pro Zeiteinheit (Runde) informiert. In Protokollen, in denen nur informierte Knoten aktiv sind, kann sich die Zahl der informierten Knoten in jeder Runde daher höchstens verdoppeln. Folglich sind mindestens $\lceil \log_2 n \rceil$ Runden nötig, um eine Information an n Knoten zu verteilen. Diese Schranke lässt sich in einigen Netzwerken mittels deterministischer Algorithmen erreichen. Es ist nicht schwierig für bestimmte Graphklassen für jeden Knoten einen Baum zu definieren, der das Verbreitungsprotokoll von diesem Knoten aus festlegt. Solche Algorithmen sind jedoch nicht robust gegenüber Übertragungsfehlern und schlecht skalierbar. Wenn der Graph erweitert wird, muss das Protokoll neu berechnet werden.

Dafür gibt es zahlreiche *randomisierte* Protokolle, die das Problem überraschend gut lösen. Ein sehr einfaches Protokoll ist das sogenannte *Randomisierte Rumor Spreading* (oder Push Protokoll), siehe [FG85, UFU90, RKV00]. Das Protokoll funktioniert wie folgt: in jeder Runde wählt jeder bereits informierte Knoten einen Nachbarknoten gleichverteilt zufällig aus und schickt ihm eine Kopie der Information zu. Jeder Knoten führt somit den gleichen randomisierten Prozess aus unabhängig von der Quelle. Für viele Netzwerktopologien ist diese Strategie eine sehr effiziente Methode eine Nachricht zu verbreiten. Sei n die Zahl der Knoten in einem Graphen. Dann verbreitet das Push Protokoll eine Nachricht mit Wahrscheinlichkeit $1 - o(1)$ an alle Knoten in $\Theta(\log n)$ Runden im vollständigen Graphen [FG85, Pit87], im Hyperwürfel [UFU90], im Erdős-Rényi Zufallsgraph $G_{n,p}$ mit $p \geq (1+\varepsilon)\ \ln(n)/n$ [UFU90], im zufälligen regulären Graphen [FP10] und in Expander-Graphen [FP10]. Ähnliche Resultate wurden ebenfalls gezeigt für zufällige geometrische Graphen [MB], sowie Graphen mit konstanter Conductance [FCP10].

Im Gegensatz zu diesen Resultaten, zeigten Chierichetti, Lattanzi und Panconesi [CLP11], dass das Push Protokoll im PA Modell mit konstanter Wahrscheinlichkeit $\Omega(n^\alpha)$ Runden benötigt for ein konstantes $\alpha > 0$.

Zur Untersuchung der Verbreitung von Informationen in sozialen Netzwerken betrachten wir das *Push-Pull Protokoll*, in dem im Gegensatz zum Push Protokoll auch nicht informierte Knoten aktiv nach neuen Informationen suchen. Dieses Modell geht zurück auf Demers et al. [DGH$^+$88] und wurde von Karp, Schindelhauer, Shenker und Vöcking [RKV00] auf vollständingen Graphen untersucht.

2 Rumor Spreading auf Sozialen Netzwerken

2.1 Einleitung

Soziale Netzwerke wie Facebook und Twitter sind dabei, die Art und Weise zu verändern wie Menschen kollektiv handeln. Sie spielten eine zentrale Rolle in der Protestbewegung des Arabischen Frühlings und der Unruhen in England 2011. Es ist naheliegend anzunehmen, dass die hohe Geschwindigkeit mit der Nachrichten über soziale Netzwerke verbreitet werden zur spontanten Entwicklung dieser Ereignisse beitrug.

Dabei ist es bemerkenswert, dass soziale Netzwerke Nachrichten so schnell verbreiten können. Sowohl die Struktur von sozialen Netzwerken als auch der Prozess zur Verbreitung von Informationen sind nicht speziell für diesen Zweck entworfen, sondern haben sich dezentralisiert und zufällig gebildet.

Stimmt unsere Sicht also, dass soziale Netzwerke in ihrer Struktur die Verbreitung von Informationen erleichtern? Und welche besonderen Eigenschaften von sozialen Netzwerken sind hierfür verantwortlich?

Dazu simulieren wir einen einfachen Prozess zur Informationsausbreitung auf mehreren realen Graphen. Dabei sehen wir, dass lediglich acht Runden benötigt werden, um eine Information von einem zufälligen Knoten des Twitter Netzwerks an durchschnittlich 45.6 Millionen von insgesamt 51.2 Millionen Mitgliedern zu verbreiten.

Wir untersuchen diesen Prozess ebenfalls in einem mathematischen Modell für soziale Netzwerke, dem PA-Graph Modell von Barabási und Albert [BA99]. Wir beweisen, dass sich Informationen in solchen Netzwerken deutlich schneller ausbreiten als in vielen anderen Netzwerktopologien, sogar schneller als in vollständigen Graphen. Wir erklären dies damit, dass Knoten von geringem Grad einen “schnellen” Kommunikationspfad bilden zwischen Knoten mit hohem Grad, die aufgrund der hohen Anzahl iher potenziellen Kommunikationspartner weniger oft direkt miteinander kommunizieren.

Dieser Teil meiner Dissertation basiert auf den Publikationen [DFF11, DFF12b, DFF12a].

2.2 Soziale Netzwerke und Rumor Spreading

Soziale Netwerke werden gebildet von Menschen, die sich kennen, *Facebook* Mitgliedern, die Freunde sind (auf Facebook), wissenschaftlichen Autoren, die eine gemeinsame Publikation haben, oder Schauspielern, die im gleichen Film auftreten. Trotz dieser Vielfalt haben viele dieser realen Netzwerke sehr ähnliche Eigenschaften. Eine dieser Eigenschaften ist der kleine Abstand zwischen zwei beliebigen Knoten im Graphen. Bekannt wurde dies durch Milgram’s “Kleine Welt-Studie” [Mil67]. Für das Internet schätzten Albert, Jeong und Barabási [RAB99] einen Durchmesser von nur 19 Knoten im zugrundeliegenden Graphen.

Andere experimentelle Studien [RAB99] zeigten eine weitere Eigenschaft von zahlreichen sozialen Netzwerken: das Histogramm der Grade der Knoten folgt einem Potenzgesetz,

d.h., die Zahl der Knoten mit Grad k ist umgekehrt proportional zu einem Polynom in k. Um diese Eigenschaft zu erklären, führten Barabás und Albert [BA99] das PA Modell für reale Netzwerke ein. Hierbei werden Graphen zufällig nach einem iterativen Schema generiert: jeder neue Knoten wird mit m bestehenden Knoten verbunden, die zufällig ausgewählt werden. Wir nennen m auch Dichteparameter, da er das Verhältnis von Kanten zu Knoten darstellt. Statt durch eine Gleichverteilung erfolgt diese Auswahl jedoch proportional zu dem bestehenden Grad des Knoten, so dass Knoten mit hohem Grad bevorzugt werden.

Für diese Graphen zeigten Barabási und Albert [BA99] empirisch ein Potenzgesetz von k^{-3}, was später auch mathematisch rigoros von Bollobás, Riordan, Spencer, und Tusnády [BBT01] bewiesen wurde.

In diesen Graphen untersuchen wir das Push-Pull Protokoll, bei dem jeder Knoten in jeder Runde zufällig einen Nachbarknoten auswählt und sich mit ihm austauscht. Allerdings schließen wir dabei für jeden Knoten jenen Nachbarknoten aus, der in der vorherigen Runde kontaktiert wurde. Wir zeigen, dass diese kleine Änderung erstaunlicherweise zu einer aymptotischen Verbesserung der Laufzeit um mehr als einen konstanten Faktor führt.

2.3 Mathematische Analyse

Das Kernstück unserer Arbeit ist eine mathematische Analyse, die beweist, dass die Informationsausbreitung in PA Graphen in sublogarithmischer Zeit erfolgt. Dies bezieht sich sowohl auf die Zeit, um alle Knoten im Graphen zu informieren als auch für jeden konstanten Anteil wie 1%, 10%, 50%.

Sei G_m^n ein PA Graph mit n Knoten und Dichteparameter m. Da der Graph G_m^n ein Zufallsgraph ist, gelten die meisten erwähnten Eigenschaften nur mit einer bestimmten Wahrscheinlichkeit. Diese geht jedoch gegen 1 mit wachsendem n. Wir sagen, die Eigenschaft gilt mit hoher Wahrscheinlichkeit. Im Folgenden sei jede Aussage über einen Zufallsgraph in diesem Sinne zu verstehen.

Für jede Konstante $m > 1$, zeigen wir, dass nach einer erstaunlich kurzen Zeit die Nachricht in G_m^n an alle Knoten verbreitet wird.

Theorem 1 *Die Informationsausbreitung im obigen Prozess auf dem PA Graphen erfolgt von einer Quelle zu allen anderen Knoten des Graphen in* $\Theta(\log n / \log\log n)$ *Runden.*

Dieses Resultat verbessert die beste vorherige Schranke von $O(\log^2 n)$ [CLP11]. Theorem 1 zeigt zum ersten Mal, dass die Informationsausbreitung in PA Graphen viel schneller erfolgt als in anderen Netzwerktopologien. So haben *Random Attachment* Graphen, bei denen jeder Knoten m Nachbarknoten zufällig gleichverteilt auswählt, einen Durchmesser von $\Theta(\log n)$, was eine untere Schranke für die Informationsausbreitung darstellt. Ebenso gilt für jeden Knoten in solchen Graphen, dass ein konstanter Anteil aller Knoten einen Abstand von $\Omega(\log n)$ hat. Folglich sind logarithmisch viele Runden nötig, um einen bestimmten konstanten Anteil aller Knoten zu informieren. Ähnliche Schranken gelten eben-

falls für den Hyperwürfel, der in vielen Kommunikationsnetzwerken Anwendung findet. Es ist jedoch nicht immer der Durchmesser eines Graphen, der entscheidend ist für die Informationsausbreitung. So hat der vollständige Graph einen Durchmesser von 1. Dennoch benötigt eine Nachricht logarithmische Zeit, um von einem Knoten an alle Knoten übertragen zu werden. Dies wurde von Karp et al. [RKV00] für das Push-Pull Protokoll gezeigt, bei dem jeder Knoten auch den in der vorherigen Runde kontaktierten Knoten wiederholt auswählen kann. Es ist einfach zu sehen, dass im Falle von vollständigen Graphen unsere Modifikation keinen Einfluss auf ihren Beweis hat und das Resultat damit weiterhin gültig ist. Ebenso ergibt sich aus ihrem Beweis, dass bereits das Informieren von einem konstanten Anteil logarithmischer Zeit bedarf. Ähnliches gilt für Erdős-Rényi-Graphen. Leider ist der Beweis von Theorem 1 zu lang, um ihn hier wiederzugeben. Wir skizzieren allerdings an dieser Stelle ein zentrales Argument, welches auch erklärt, warum Informationen sich besonders schnell in sozialen Netzwerken ausbreiten.

Es seien A und B zwei Nachbarknoten in G_m^n mit jeweils Grad d_A und d_B (Abbildung 1). Wir nehmen an, dass Knoten A informiert ist, während Knoten B noch nicht informiert ist. Wie verbreitet sich die Information von A nach B? Da A seine Nachbarknoten zufällig auswählt, sind im Erwartungswert etwa d_A Runden erforderlich bis A Knoten B kontaktiert und damit die Information an B weitergibt. Ebenso bedarf es im Erwartungswert etwa d_B Runden bis B Knoten A kontaktiert, um die Nachricht auf diesem Wege zu erfahren. Wenn d_A und d_B groß sind, z.B. $n^{1/3}$, dann sind fast $\frac{1}{2}n^{1/3}$ Runden nötig, damit sich die Nachricht direkt von A auf B überträgt.

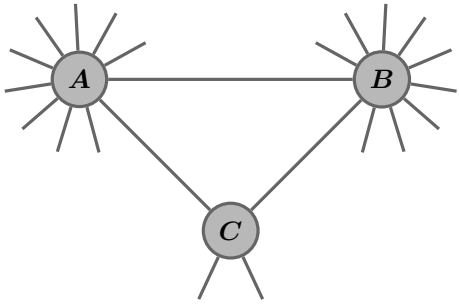


Abbildung 1

Die Laufzeit, die in Theorem 1 genannt wird, ist dagegen viel kleiner. Es muss also einen besseren Weg geben, um die Nachricht von A nach B zu bringen. Interessanterweise sind es die Knoten von kleinem Grad, die dies bewerkstelligen. Nehmen wir an, dass es einen dritten Knoten C gibt, der mit A und B benachbart ist, der nur einen kleinen Grad d_C von 4 hat. In diesem Fall bedarf es im Erwartungswert $d_C = 4$ Runden, damit C Knoten A kontaktiert und dadurch die Information erhält. Nach weiteren 4 Runden im Erwartungswert kontaktiert C Knoten B und informiert B auf diese Weise. Es sind also lediglich etwa $2d_C = 8$ Runden nötig, damit die Nachricht von A zu B über B übertragen wird. Wir zeigen im Beweis, dass ein solcher Knoten C mit hoher Wahrscheinlichkeit existiert, da sich im PA Modell neue Knoten mit ausreichend hoher Wahrscheinlichkeit mit hochgradigen Knoten wie A und B verbinden.

Ein Grund, warum die Informationsausbreitung in sozialen Netzwerken so schnell ist, liegt also darin, dass Knoten von kleinem Grad schnell die Information von einem informierten Nachbarknoten erhalten und dann wiederum schnell an all ihre anderen Nachbarknoten weitergeben. Ein solcher Prozess fehlt in anderen Graphklassen. So hat beispielsweise im

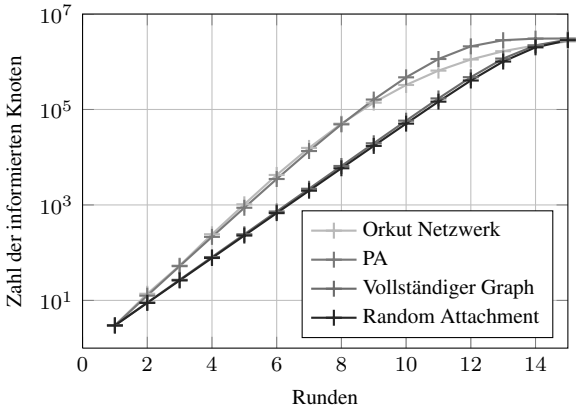


Abbildung 2: Durchschnittliche Zahl der informierten Knoten in Abhängigkeit von der Zahl der Runden für das Orkut Netzwerk, PA Modell, Random Attachment und vollständigem Graphen der gleichen Größe $n = 3,072,441$ und $m = 38$.

vollständingen Graphen jeder Knoten einen hohen Grad von $n - 1$. Für jeden Nachbarn der Quelle A gilt daher, dass die Wahrscheinlickeit, dass er A kontaktiert, gering ist.

Solche "schnellen" Verbindungen sind in PA Graphen dagegen zahlreich vorhanden. Der Einfachheit halber nennen wir einen Knoten *populär*, wenn er $\Omega(\log(n)^2)$ Nachbarn hat. In unserem Beweis zeigen wir, dass es zwischen zwei populären Knoten stets einen Pfad der Länge $O(\log(n)/\log(\log(n)))$ gibt, so dass jeder zweite Knoten den kleinstmöglichen Grad von m hat. Wie oben beschrieben, agieren solche Knoten als schnelle Verbindungen, die die Nachricht im Erwartungswert innerhalb von $2m$ Runden weiterleiten. Folglich ist die erwartete Zeit, in der die Nachricht den Pfad durchläuft $2m$ mal der Länge des Pfades. Durch eine genaue Analyse können wir ferner zeigen, dass zwischen jedem Paar von populären Knoten zahlreiche solcher Pfade bestehen, woraus sich schließlich eine Laufzeit von $O(\log(n)/\log(\log(n)))$ zum Informieren aller populären Knoten ableiten lässt, sobald ein populärer Knoten informiert ist.

Da Knoten dazu tendieren sich mit populären Knoten zu verbinden, verbreitet sich eine Nachricht ausgehend von einem Knoten mit kleinen Grad zu einem populären Knoten sogar noch schneller, nämlich in $O(\log(n)^{3/4}\log(\log(n)))$ Runden. Sobald alle populären Knoten informiert sind, benutzen wir ein Symmetrieargument, um zu zeigen, dass nach ebensovielen Runden, alle verbliebenen Knoten mit kleinem Grad informiert werden. Dies geschieht dann in der Regel durch das Kontaktieren von populären Knoten.

2.4 Experimentelle Resultate

Neben der mathematischen Analyse haben wir ebenfalls Experimente auf den Daten von realen sozialen Netzwerken durchgeführt. Dazu simulierten wir die Informationsausbreitung auf Samples vom *Twitter* und *Orkut* Graphen (basierend auf [Les, BDG]) sowie auf PA Graphen. Zum Vergleich haben wir die Simulation ebenfalls auf vollständigen Graphen und Random Attachment Graphen durchgeführt.

Im Random Attachment und Preferential Attachment Modell legen wir die Dichte der

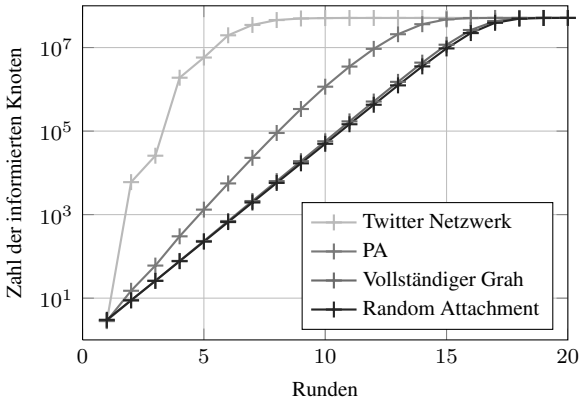


Abbildung 3: Durchschnittliche Zahl der informierten Knoten in Abhängigkeit von der Zahl der Runden für das Orkut Netzwerk, PA Modell, Random Attachment und vollständigem Graphen (Größe $n = 51,217,936$, $m = 32$).

Graphen durch den Parameter m fest. Dadurch können wir Experimente auf Graphen mit der gleichen Anzahl an Knoten und Kanten wie den realen Netzwerken durchführen.

Abbildungen 2 und 3 zeigen, wie sich eine Nachricht, die sich in einem zufällig ausgewählten Knoten befindet, im Graphen des Orkut und Twitter Netzwerkes verbreitet. Beide Abbildungen verdeutlichen, dass sich Nachrichten schneller in realen Netzwerken verbreiten als im vollständigen und Random-Attachment Graphen. Im Falle des Twitter Netzwerkes lässt sich zudem ein klarer Unterschied gegenüber dem PA Model erkennen, was darauf hinweist, dass das Twitter Netzwerk weniger gut durch das PA Modell dargestellt wird.

3 Optimales Randomisiertes Rumor Spreading auf Vollständigen Graphen

3.1 Einführung

Angenommen wir wollen alle Leute in einem Dorf über eine Nachricht informieren. Wir kennen nicht die Email Adressen von allen Leuten und wollen deshalb eine Telefonkette starten. Wie können wir dies effizient tun und trotzdem garantieren, dass am Ende jeder Dorfbewohner einen Anruf erhalten hat? Formal lässt sich dieses Problem als Informationsausbreitung von einem Knoten zu allen Knoten eines vollständigen Graphen beschreiben. Zur Lösung können wir das oben beschriebene Push Protokoll verwenden, bei dem jeder informierte Knoten die Nachricht in jeder Runde an einen zufällig ausgewählten Nachbarknoten weitergibt. Dieses Protokoll verbreitet die Nachricht innerhalb von $(1+o(1))(\log n+\ln n)$ Runden mit hoher Wahrscheinlichkeit ([FG85, UFU90]). Das Push Protokoll hat jedoch zwei Nachteile. Erstens, ein Knoten ist sich nie sicher, dass alle Knoten im Graphen informiert sind. Es gibt folglich keine sichere Terminierungsregel. Zweitens sind $\Theta(n \log n)$ Nachrichten notwendig, um alle n Knoten zu informieren, so dass die Mehrzahl der Nachrichten verschwendet wird. Diese Probleme wurden in der Arbeit von Karp et al. [RKV00] mittels des Push-Pull Algorithmus gelöst. Sie stellten zwei

Varianten dieses Protokolls vor, welches die Nachricht mit nur $O(n \log \log n)$ Nachrichten verbreitet und dabei trotzdem nur $O(\log n)$ Runden benötigt. Die zweite Variante ihres Protokolls ist zudem robust gegenüber Knotenausfällen. Zentral dabei ist die Verwendung von Pull Operationen, bei denen uninformierte Knoten aktiv ihre Nachbarknoten anrufen, um nach möglichen neuen Informationen zu fragen. Solche Pull Operationen haben jedoch den Nachteil, dass sie für eine ständige Banspruchung des Netzwerkes sorgen, auch wenn keine neuen Nachrichten vorhanden sind. Die zugrundeliegende Annahme im Ansatz von Karp et al. [RKV00] ist daher, dass neue Nachrichten fortlaufend im Netzwerk auftreten.

In meiner Dissertation stellen wir eine alternative Lösung für das Problem vor. Es kommt ohne Pull Operationen aus und erreicht dennoch eine Laufzeit von $(1+o(1)) \log n$ Runden. Zudem benötigt das Protokoll nur $O(nf(n))$ Nachrichten, wobei $f = \omega(1)$ eine Funktion ist, die beliebig langsam unbegrenzt wächst. Damit erreichen wir fast die untere Schranke von $\lceil \log_2 n \rceil$ Runden and $n - 1$ Nachrichten. Es weist zudem eine gute Robustheit gegenüber Knotenausfällen auf. Bei einem Ausfall von einem zufälligen konstanten Anteil aller Knoten zu beliebigen Zeiten werden alle funktionierenden Knoten in weiterhin fast optimaler Zeit informiert. Wir stellen ferner eine Variante vor, die auch im Falle von adversariellen Knotenausfällen noch effizient funktioniert. Das Protokoll ist außerdem skalierbar: wenn sich die Netzwerkgröße ändert, sind keine aufwendigen Neuberechnungen nötig. Schließlich besitzt es eine natürliche Terminierungsregel, die sicherstellt, dass alle (fehlerfreien) Knoten am Ende des Protokolls mit Wahrscheinlichkeit 1 informiert sind.

Im Gegensatz zu vorherigen Protokollen nehmen wir allerdings an, dass jeder Knoten einen eindeutigen Namen hat. In vielen Fällen ist dies eine natürliche Annahme.

Dieser Teil meiner Dissertation basiert auf der Veröffentlichung in [DF11].

3.2 Unsere Resultate

Das Protokoll erlaubt folgenden Tradeoff zwischen der Anzahl der benötigten Runden und der Anzahl der benötigten Nachrichten. Für jede Funktion $f : \mathbb{N} \to \mathbb{N}$ geben wir ein Protokoll an, dass mit hoher Wahrscheinlichkeit alle Knoten im vollständigen Graphen in nur $\log(n) + f(n) + O(f(n)^{-1} \log n)$ Runden informiert. Es benötigt hierzu $O(nf(n))$ Nachrichten. Die optimale Laufzeit wird dabei für $f(n) = \Theta(\sqrt{\log n})$ erreicht, was zu einer Laufzeit von $\log n + O(\sqrt{\log n})$ Runden und $O(n\sqrt{\log n})$ Nachrichten führt.

Der Einfachheit halber nehmen wir an, dass die Knoten von 1 bis n nummeriert sind. Tatsächlich benötigen wir lediglich, dass alle Knoten (i) einen zufälligen Knoten auswählen können und (ii) für jeden Knoten, einen eindeutigen Nachfolger bestimmen können gemäß einer zyklischen Ordnung der Knoten.

Sei $f : \mathbb{N} \to \mathbb{N}$ eine gegebene Funktion. Dann verfährt das Protokoll wie folgt. Jeder neu informierte Knoten schickt seine erste Nachricht an einen zufällig ausgewählten Knoten. Falls die vorherige Nachricht an einen nicht informierten Knoten ging, wird die nächste Nachricht an den Nachfolger dieses Knoten geschickt gemäß der zyklischen Ordnung. Falls die vorherige Nachricht dagegen an einen bereits informierten Knoten ging, wird die nächste Nachricht an einen zufälligen Knoten geschickt. Sobald ein Knoten $f(n)$ infor-

mierte Knoten kontaktiert hat, hört der Knoten auf, weitere Nachrichten zu verschicken.

Dieses Protokoll kann als Variante des Quasirandom Rumor Spreading Protokoll interpretiert werden [DFS08]. Im Gegensatz dazu haben alle Knoten im hier betrachteten Protokoll die gleiche zyklische Ordnung und können mehrmals zufällige Knoten kontaktieren.

Die Hauptschwierigkeit in der Analyse des Protokolls liegt darin, dass das Senden der Nachrichten jedes Knoten nicht unabängig voneinander ist. Zur Lösung nutzen wir aus, dass die zufälligen Kommunikationspartnern unabhängig voneinander ausgewählt werden.

Um auf das eingangs erwähnte Problem der Telefonkette zurückzukommen, bietet unser Protokoll folgende einache Lösung an. Wir schlagen unsere Telefonnummer im Telefonbuch nach und rufen die nächste Person an. Danach wählen wir eine zufällige Nummer im Telefonbuch aus und informieren den Anschlussinhaber. Wenn jede informierte Person auf diese Weise zwei Anrufe tätigt, werden alle Personen in nur $(1 + o(1))(\log n + \ln n)$ Runden mit hoher Wahrscheinlichkeit informiert. Beachte, dass diese Lösung nicht identisch mit dem oben beschriebenen Protokoll ist, da wir hier zuerst einen deterministischen Anruf und anschließend erst einen zufälligen Anruf tätigen.

Literatur

[BA99] A.-L. Barabási und R. Albert. Emergence of Scaling in Random Networks. *Science*, 286:509–512, 1999.

[BBT01] J. Spencer B. Bollobás, O. Riordan und G. Tusnády. The degree sequence of a scale-free random graph process. *Random Structures & Algorithms*, 18:279–290, 2001.

[BDG] B. Bhattacharjee, P. Druschel und K. Gummadi. Online social networks research at the MPI for Software Systems.

[CLP11] F. Chierichetti, S. Lattanzi und A. Panconesi. Rumor spreading in social networks. *Theor. Comput. Sci*, 412(24):2602–2610, 2011.

[DF11] B. Doerr und M. Fouz. Asymptotically optimal randomized rumor spreading. In *Proceedings of the 36th Annual International Colloquium on Automata, Languages and Programming (ICALP)*, Seiten 501–513, 2011.

[DFF11] B. Doerr, M. Fouz und T. Friedrich. Social networks spread rumors in sublogarithmic time. In *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing (STOC)*, Seiten 21–30, 2011.

[DFF12a] B. Doerr, M. Fouz und T. Friedrich. Experimental Analysis of Rumor Spreading in Social Networks. In *Proc. of the 1st Medit. Conf. on Algo.*, Seiten 159–173, 2012.

[DFF12b] B. Doerr, M. Fouz und T. Friedrich. Why rumors spread fast in social networks. In *Communications of the ACM*, Seiten 70–75, 2012.

[DFS08] B. Doerr, T. Friedrich und T. Sauerwald. Quasirandom rumor spreading. In *Proc. of the 19th Annual ACM-SIAM Symp. on Discr. Alg. (SODA)*, Seiten 573–781, 2008.

[DGH+88] A. J. Demers, D. H. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. E. Sturgis, D. C. Swinehart und D. B. Terry. Epidemic Algorithms for Replicated Database Maintenance. *Operating Systems Review*, 22:8–32, 1988.

[FCP10] S. Lattanzi F. Chierichetti und A. Panconesi. Almost tight bounds for rumour spreading with conductance. In *Proceedings of the 42nd Annual ACM Symposium on Theory of Computing (STOC)*, Seiten 399–408, 2010.

[FG85] A. M. Frieze und G. R. Grimmett. The Shortest-Path Problem for Graphs with Random Arc-lengths. *Discrete Applied Mathematics*, 10:57–77, 1985.

[FP10] N. Fountoulakis und K. Panagiotou. Rumor spreading on random regular graphs and expanders. In *Proc. of the 14th Annual Workshop on Randomization and Computation (RANDOM)*, Seiten 560–573, 2010.

[Les] J. Leskovec. Stanford large network dataset collection.

[MB] R. Els M. Bradonjic. Efficient Broadcast on Random Geometric Graphs.

[Mil67] S. Milgram. The small world problem. *Psychology Today*, 1:60–67, 1967.

[Pit87] B. Pittel. On Spreading a Rumor. *SIAM J. on Appl. Math.*, 47:12–223, 1987.

[RAB99] H. Jeong R. Albert und A.-L. Barabasi. Diameter of the World-Wide Web. *Nature*, 401:130–131, 1999.

[RKV00] S. Shenker R. Karp, C. Schindelhauer und B. Vöcking. Randomized Rumor Spreading. In *Proceedings of the* 41*st Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, Seiten 565–574, 2000.

[UFU90] P. Raghavan U. Feige, D. Peleg und E. Upfal. Randomized Broadcast in Networks. *Random Structures & Algorithms*, 1:447–460, 1990.



Mahmoud Fouz wurde am 20.07.1984 in Homburg geboren. Das Abitur schloss er als einer der zehn besten Abiturienten des Saarlandes im Jahr 2003 mit der Gesamtnote 1,0 ab. Daraufhin studierte Herr Fouz Informatik an der Universität des Saarlandes und schloss dieses in acht Semestern mit der Gesamtnote 1,0 ab. Nach einem einsemestrigen Gastaufenthalt an der Universität von Waterloo in Kanada, nahm Herr Fouz im März 2008 das Promotionsstudium unter der gemeinsamen Betreuung durch Prof. Dr. Markus Bläser und Prof. Dr. Benjamin Doerr an der Universität des Saarlandes auf. Die Promotionsprüfung legte Herr Fouz am 16. Juli 2012 mit der Gesamtnote *summa cum laude* ab. Das Promotionsstudium wurde gefördert durch ein Stipendium des Graduiertenkollegs.

Constraint Generierung für domänenspezifische Modellierungssprachen

Dagi Geister

Institut für Systems Engineering, Leibniz Universität Hannover
Institut für Flugführung, Deutsches Zentrum für Luft- und Raumfahrt e.V.
dagi.geister@dlr.de

Abstract: Anflugplanungssysteme dienen der Unterstützung von Fluglotsen bei der Planung und Koordinierung des anfliegenden Luftverkehrs innerhalb eines Flughafennahbereichs. In dieser Arbeit wurde die domänenspezifische Modellierungssprache AMAN-ML (Arrival Management Modeling Language) entwickelt, mit der ein Anflugplanungssystem mit geringem Aufwand an veränderte Anforderungen angepasst werden kann. Auf der Grundlage von AMAN-ML wurde ein Ansatz verfasst, um das erfahrungsbasierte Wissen von Fluglotsen in den Modellierungsprozess einer Software zu integrieren. Eine im Rahmen dieser Arbeit formulierte Grammatik für natürliche Sprache dient als Basis für eine Transformation in die Constraint-Beschreibungssprache OCL (Object Constraint Language). Aspekte der Vagheit und Unbestimmtheit der natürlichen Sprache werden bei der Transformation erkannt und entsprechend bei der Generierung von Constraints an die Modellierungssprache berücksichtigt. Zur Abbildung von linguistischen Variablen und unscharfen Ausdrücken wurde das Konzept der Fuzzy Mengen herangezogen und in die Syntax der OCL integriert. Das Constraint System von AMAN-ML wird für die Verifikation (*Model Verification*) und die Vervollständigung (*Model Completion*) von Modellen eingesetzt.

1 Einführung

Ein Anflugplanungssystem wird für die Anflugkontrolle (engl. Approach Control) eines Flughafens eingesetzt und dient der Unterstützung der Flugverkehrskontrolle bei der sicheren, effizienten und kapazitätsorientierten Führung des Luftverkehrs. An ein Anflugplanungssystem werden hierbei hohe Anforderungen hinsichtlich einer korrekten und stets zuverlässigen Funktionalität gestellt. Diese Anforderungen basieren u.a. auf rechtlichen Vorschriften aus dem Geltungsbereich der Luftfahrt (u.a. LuftVO, ICAO-Dokumente), spezifischen Vorgaben und Informationen für einen Flughafen (Luftfahrthandbuch, Nachrichten für Luftfahrer) und den geltenden Verfahrensweisen der Flugverkehrskontrolle (BA-FVD). Die Umsetzung dieser Anforderungen in einem Anflugplanungssystem stellt sicher, dass einem Fluglotsen die für eine Planung und Koordinierung des Luftverkehrs erforderlichen Informationen und Unterstützungsfunktionen zur Verfügung gestellt werden können. Zudem sollte ein Anflugplanungssystem ohne erheblichen Aufwand an neue oder auch veränderte Rahmenbedingungen anpassbar sein. Dies bezieht sich zum einen auf die Anpassbarkeit von existierenden Funktionalitäten an neue Flughafentopologien und damit

der Übertragbarkeit eines Anflugplanungssystems auf weitere Flughafen, zum anderen auf die Erweiterbarkeit vorhandener Unterstützungsfunktionen hinsichtlich neu entstehender oder veränderlicher Aufgabenstellungen in der Flugverkehrskontrolle. Weiterhin ist eine Adaptierbarkeit des Anflugplanungssystems in Bezug auf individuelle Präferenzen und heuristische Verfahrensweisen der Fluglotsen von ebenso hoher Bedeutung. Diese Adaptierbarkeit stellt nicht nur eine Möglichkeit der Annäherung der Funktionalitäten des Anflugplanungssystems an die realen Handlungsweisen und Entscheidungen des Fluglotsen dar, sondern bildet bei diesen ebenfalls die Grundlage für die Bildung von Vertrauen und Akzeptanz.

Die Anpassung der Software eines Anflugplanungssystems an flughafenspezifische Vorgaben, geltende gesetzliche Vorschriften und mögliche Heuristiken von Fluglotsen ist bisher mit einem erheblichen Arbeitsaufwand verbunden. Umfangreiche Reengineering-Maßnahmen müssen vorgenommen werden, um problemspezifische Codekomponenten zu extrahieren und diese an neue Anforderungen anzupassen. Die hierbei geforderte Korrektheit muss über eine Vielzahl von generellen und flughafenspezifischen Vorgaben sichergestellt werden. Dies erschwert die Entwicklung flexibler und anpassungsfähiger Anflugplanungssysteme. Zum Zeitpunkt dieser Arbeit sind daher die meisten Anflugplanungssysteme auf die spezifischen Anforderungen eines einzelnen Flughafens ausgerichtet. In dieser Arbeit wird ein Ansatz vorgestellt, der eine flexible Anpassung von Anflugplanungssystemen erlaubt und zugleich eine Integration von Erfahrungswissen in den Entwicklungsprozess ermöglichen soll.

2 Motivation und Hintergrund

Als eine elementare Grundlage für die Entwicklung eines anforderungsgerechten Anflugplanungssystems gilt das formale und erfahrungsbasierte Wissen der Fluglotsen. Dieses Wissen ermöglicht ein umfassendes Verständnis über die Zusammenhänge und Abläufe in der Flugverkehrskontrolle. Das Erfahrungswissen wird meist in erzählender Form unter Verwendung von natürlicher Sprache weitergegeben. Natürliche Sprache hat die Eigenschaften von Vagheit und Unbestimmtheit, die sich lediglich über den situativen Kontext verstehen und in ihrer Bedeutung vervollständigen lassen. Dennoch ist Erfahrungswissen von elementarer Bedeutung, um das situative Verhalten eines Fluglotsen in einem Anflugplanungssystem bestmöglich nachbilden zu können. Bei der Konzeption eines Anflugplanungssystems ist es demzufolge nicht nur erforderlich eine Anpassungsfähigkeit an flughafenspezifische Vorgaben und gesetzliche Vorschriften vorzusehen, sondern ebenso wichtig das Erfahrungswissen von Fluglotsen für den Entwicklungsprozess und die entstehenden Unterstützungsfunktionen zu erfassen und zu formalisieren. Mögliche individuell formulierte Verfahrensweisen oder Heuristiken ermöglichen eine bessere Vorhersagbarkeit und Abbildbarkeit von situativ bedingten Entscheidungen eines Fluglotsen. Zudem kann das Erfahrungswissen auch als Anforderung an ein Anflugplanungssystem interpretiert und als Grundlage zur Bestimmung der Korrektheit des Systems verwendet werden. Dies kann zu einer höheren Akzeptanz der Fluglotsen beitragen, die über die Formulierung von erfahrungsbasierten Verfahrensweisen und Informationen ein Anflugplanungssystem ihren

Bedürfnissen anpassen und direkt Auswirkungen in Form adaptierter Planungen nach ihren eigenen Vorgaben beobachten können.

In dieser Arbeit wird insgesamt ein Ansatz zur Integration von Erfahrungswissen in den Modellierungsprozess und in die Komponenten eines Softwaresystems vorgestellt. Dieser Ansatz basiert auf der Zielsetzung

- eine funktionale und strukturelle Anpassbarkeit eines Softwaresystems (hier eines Anflugplanungssystems),
- eine Generierung von Constraints aus Erfahrungswissen,
- eine Formulierung von Constraints in natürlicher Sprache sowie
- eine Verwendung der generierten Constraints zur Verifikation und Vervollständigung von Modellen

zu ermöglichen. Hierfür wurden in dieser Arbeit verschiedene Konzepte erarbeitet, zu denen

- die Entwicklung einer Modellierungssprache zur Anpassung eines Anflugplanungssystems nach flughafen- und anwenderspezifischen Anforderungen,
- die Erweiterung bestehender Warteschlangenmodelle für eine generische Landebahnzuweisung,
- die Ableitung einer Grammatik für natürliche Sprache zur Abbildung von natürlichsprachigen Anforderungen an eine Modellierungssprache,
- die Erweiterung der Syntax der OCL zur Abbildung von unscharfen Ausdrücken der natürlichen Sprache sowie
- die Ausarbeitung eines Constraint Reasoning auf Basis unscharfer Ausdrücke der OCL zur Integration einer Modellverifikation und -vervollständigung

gehören. Diese einzelnen Konzepte wurden einerseits in einer Modellierungssprache und andererseits in einer Komponente zur Constraint Generierung umgesetzt und in ein bestehendes Anflugplanungssystem integriert. Das entstandene Gesamtsystem wurde auf Basis verschiedener Experimente validiert und wird derzeit operational im Deutschen Zentrum für Luft-und Raumfahrt eingesetzt.

3 Die Modellierungssprache AMAN-ML

Die Motivation zur Erstellung von AMAN-ML liegt in der Möglichkeit ein generisches Anflugplanungssystem zu entwickeln, welches mit geringem Aufwand an neue Flughäfen und deren spezifische Vorgaben und Randbedingungen angepasst werden kann. Darüber hinaus können neue Aufgabenstellungen in der Flugverkehrskontrolle in einem Modell

dargestellt und in die Unterstützungsfunktionalitäten des Planungssystems integriert werden. Neben der Zeitersparnis, die die Anwendung von AMAN-ML ermöglicht, liegt ein weiterer Vorteil der Modellierungssprache in der Visualisierung von domänenspezifischen Zusammenhängen. Abhängigkeiten und Beziehungen zwischen einzelnen Elementen des realen Systems und die mit ihnen verbunden rechtlichen, flughafentopologischen, verfahrensbezogenen und individuellen Vorgaben können modellbasiert abgebildet und analysiert werden. Die Elemente und Beziehungen eines realen Systems können in einem Modell abgebildet und als Basis für die Generierung von Programmkomponenten herangezogen werden. Die Auswirkung einer Veränderung einzelner Parameter kann innerhalb der Modelle und Programmkomponenten nachvollzogen werden. Die Modellierungssprache AMAN-ML besteht aus einzelnen Komponenten, die eine Abbildung von Flughafenmodellen, Landebahnsystemen, Zuweisungsstrategien, Luftraumstrukturen und heuristischer Verfahrensweisen ermöglichen. Bestehende Warteschlangenmodelle zur effizienten Verteilung von anfliegenden Luftfahrzeugen auf verfügbare Landebahnen wurden hierzu erweitert, um eine Zuweisung auf verschiedene Arten von Landebahnsystemen und die mit ihnen korrespondierenden Separationsvorschriften zu ermöglichen. In Anlehnung an eine optimierte Verteilung, wie in [BEFK06] für ein abhängiges Zweibahnensystem beschrieben, kann beispielsweise eine Zuweisungsstrategie für verschiedene Landebahnensysteme unter Beachtung aktueller Arbeitslasten definiert werden. Gemäß Gleichung 1 wird in der Zuweisungsstrategie δ^{JLL+} das ankommende Luftfahrzeug k der Landebahn r zugewiesen, auf der es die geringste Wartezeit $(u^r + b(i^r, k))$ zu erwarten hat. Hierzu werden die bestehenden Arbeitslasten u^r mit der notwendigen Separation $b(i^r, k)$ zwischen letztem Luftfahrzeug auf der Landebahn r und dem aktuellen Luftfahrzeug k addiert.

$$\delta^{JLL+}(u^r, i^r; k) = \{r \mid (u^r + b(i^r, k)) \leq min\{(u^I + b(i^I, k)), (u^{II} + b(i^{II}, k)), \ldots, (u^N + b(i^N, k))\}\} \quad (1)$$

Die einzelnen Komponenten der AMAN-ML lassen sich individuell an die spezifischen Vorgaben eines Flughafens und die Verfahrensweisen der Fluglotsen anpassen.

4 Constraint Generierung

Das Erfahrungswissen kann bei hier vorgestellten Ansatz zum einen innerhalb einer eigenständigen Komponente von AMAN-ML abgebildet und damit in die Funktionalitäten des Anflugplanungssystems direkt integriert werden, zum anderen kann ein Fluglotse individuelle Anforderungen an ein Anflugplanungssystem in natürlicher Sprache formulieren. Die natürlichsprachigen Formulierungen werden dann analysiert, interpretiert und in eine Constraint-Beschreibungssprache transformiert. Im Rahmen dieser Arbeit wird eine Grammatik zur Beschreibung der englischen Sprache (Standard-Sprache in der Flugverkehrskontrolle) zur Formulierung von Erfahrungswissen definiert, die den Einschränkungen einer kontextfreien Grammatik genügt. Dieser Ansatz wurde gewählt, da die englische Sprache keine kreuzenden Abhängigkeiten besitzt und die strukturellen Abhängigkeiten der Sprache über eine kontextfreie Grammatik ebenfalls dargestellt werden können [Cho57]

[Shi85]. Bei der Entwicklung der Grammatik G_{NL} wurde insbesondere Wert auf die geeignete Abbildung der besonderen Merkmale von natürlichen Sprachen, wie Kontextbindung, Variabilität, Ausdrucksfähigkeit und Vagheit, gelegt. Hierzu wurde basierend auf der Universalgrammatik von N. Chomsky [Cho57] sowie Arbeiten von Y. X. Wang [Wan09], in denen Produktionsregeln zur Definition grundlegender englischsprachiger Satzstrukturen erarbeitet wurden, die Grammatik G_{NL} ausgearbeitet. In der G_{NL} sind dabei gleichwertige Satzaussagen über unterschiedliche Satzarten, alternative Beschreibungsformen, mögliche Synonymbildungen und Formulierungen unter Verwendung unterschiedlicher Zeitformen möglich. Mit der entwickelten Grammatik G_{NL} ist es zudem durch die Definition von linguistischen Variablen möglich, die hohe Variabilität und Ausdrucksfähigkeit der natürlichen Sprache hinreichend genau nachzubilden. Die Formulierungen von Fluglotsen unterliegen somit kaum Einschränkungen in Bezug auf alternative Ausdrucksformen und eine verwendete Terminologie.

$$\Big[\,[From\ my\ experience]_{parenthesis}\,\Big[\Big[\,[two]_{determinative}\ [runways]_{noun}\,\Big]_{noun\_phrase} \tag{1}$$
$$\Big[\,[\,[should]_{auxiliary}\,[\,be\ considered]_{compound}\,]_{verb}\ [dependant]_{adjective}\,\Big]_{verb\_phrase}\Big]_{sentence}$$
$$[if]_{conj}\Big[\Big[\,[their]_{determinative}\ [distance]_{noun}\,\Big]_{noun\_phrase}\Big[\,[is]_{simplePresent}$$
$$\Big[[less\ than]_{comparison}\,[1035\ metres]_{numExpression}\Big]_{adverbial\_phrase}\Big]_{verb\_phrase}\Big]_{sentence}\Big]_{sentence}$$

Das Erfahrungswissen eines Experten und die situative Erläuterung von Zusammenhängen kann nicht immer anhand präziser Angaben formuliert werden. Eine natürlichsprachige Formulierung enthält daher oft unsichere und vage Beschreibungen, die zu einer Unbestimmtheit in der Satzbedeutung führen. Diese können innerhalb eines Satzes insbesondere durch eine Verwendung von linguistischen Werten, Gradpartikeln (z.B. *very, slightly*), Temporal- und Modaladverbien (z.B. *almost, often*) sowie Auxiliarverben (z.B. *could, should*) erkannt werden. Bei der Formulierung von Erfahrungswissen können derartige Unbestimmtheiten aufgrund von ungenauen Angaben, einem indirekten Situationsbezug oder fehlenden Informationen entstehen und müssen bei einer Formalisierung und Transformation in Constraints geeignet abgebildet werden. Die Constraint-Beschreibungssprache OCL wurde aus diesem Grund im Rahmen dieser Arbeit um ein mehrwertiges Konzept erweitert. Zur Abbildung von linguistischen Variablen und unscharfen Ausdrücken wurde das Konzept der Fuzzy Mengen herangezogen und formal in die Syntax der OCL integriert. Die hierbei entwickelte Grammatik $G_{OCLFuzzy}$ ermöglicht die Transformation der einzelnen Constraints in Konstrukte der Programmiersprache C++. Die Formulierung von Anforderungen an ein Anflugplanungssystem setzt eine Identifikation von linguistischen Variablen voraus, mit denen Zusammenhänge in der Anflugplanung beschrieben werden können. Die Elemente und Beziehungen von AMAN-ML werden in dieser Arbeit daher mit diesen linguistischen Variablen und ihren möglichen Werten versehen, welche sie am geeignetsten beschreiben. Den identifizierten linguistischen Variablen werden charakteristische Funktionen zugeordnet, die eine Zugehörigkeit eines gegebenen linguistischen Wertes zu der hierüber definierten Fuzzy Menge festlegen. Die Vagheit in einer

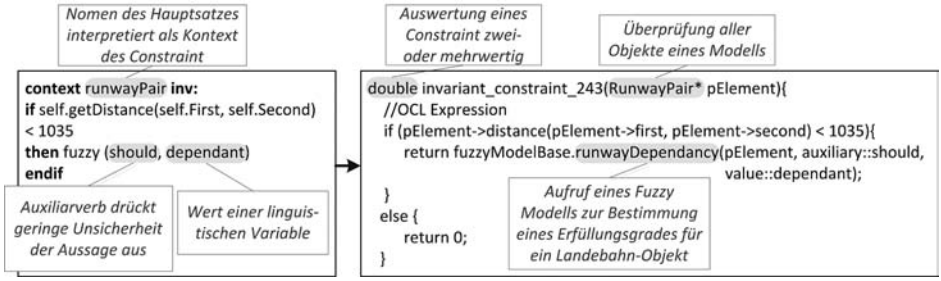


Abbildung 1: Transformation eines Constraints von OCL zu C++

natürlichsprachigen Formulierung kann über diesen Ansatz in eine Relation zu den Elementen und Zusammenhängen eines Modells in AMAN-ML gesetzt, entsprechend interpretiert und in OCL transformiert werden. Die Abbildung 1 enthält eine exemplarische Darstellung der Transformation eines Satzes in natürlicher Sprache (vgl. Satz 1) in eine Constraint-Beschreibungssprache sowie in einem nachfolgenden Schritt in Methoden einer Programmiersprache.

5 Constraint Reasoning

In AMAN-ML werden die definierten Constraints für zwei verschiedene Arten von Aufgaben in der Modellierung eingesetzt. Zum einen können die Constraints verwendet werden, um Anforderungen an die Gültigkeit von definierten Objekten, Beziehungen sowie deren Attribute zu formulieren. Die einzelnen Constraints werden hierbei mit Elementen des Metamodells assoziiert und stellen eine erweiterte Form der Spezifikation der Modelle dar. Zusätzlich lassen sich auf Basis der formulierten Constraints logische Schlussfolgerungen zur Vervollständigung von teilweise erstellten Modellinstanzen ableiten. Die grundlegende Aufgabe einer *Modell-Verifikation* ist die Überprüfung der Korrektheit eines Modells. Diese beinhaltet in AMAN-ML zunächst eine separate Verifikation der einzelnen Constraints, die den Elementen des Modells zugeordnet werden. Da die einzelnen Constraints in AMAN-ML nicht dem zweiwertigen Konzept entsprechen, wird der Auswertung eine Abbildung in eine scharfe Ergebnismenge auf Basis eines definierten Schwellenwertes zugrunde gelegt. Werden bei einer Verifikation fehlerhafte Modellelemente erkannt, ist es zudem von Bedeutung, den Ursprungsfehler sowie das verursachende Modellelement zu identifizieren. In den Modellen von AMAN-ML bestehen Hierarchien in der Fehlerfortsetzung, die als Basis zur Definition von Constraint Hierarchien gemäß [BDFBK87] herangezogen wurden. Die Verwendung von Constraint Hierarchien ermöglicht eine Analyse von möglichen Zusammenhängen in den Fehlern einer Modellinstanz und damit die Identifikation eines verursachenden Modellelements. Die *Modell-Verifikation* sollte weiterhin Methoden beinhalten, die eine Erkennung widersprüchlicher Constraints und damit

unbestimmter Constraint Systeme ermöglicht. Werden zu viele Constraints für ein Modell definiert bzw. enthalten die Constraints zu große Einschränkungen gültiger Werte, ist es möglich, dass keine gültige Lösung in Form einer Modellinstanz bestimmt werden kann. Bei der Formulierung von Constraints für eine Modellierungssprache ist es daher von Bedeutung, Constraints zu identifizieren, deren Anforderungen den Lösungsraum eines Constraint Systems zu stark einschränken. In dieser Arbeit wurde ein Verfeinerungs-Modell verwendet, welches ausgehend von einer gegeben Modellstruktur, erlaubte Werte auf Basis der Constraints sukzessive einschränkt. Enthalten die resultierenden Wertebereiche mehr als einen gültigen Eintrag, können diese verschiedene Wertebelegungen bilden und damit eine Menge an gültigen Modellinstanzen definieren.

Das Constraint System von AMAN-ML kann zudem eingesetzt werden, um teilweise erstellte Modelle zu einer vollständigen und korrekten Modellinstanz zu ergänzen. Auf Basis grundlegender Informationen über das zu erstellende Modell, werden die fehlenden Modellelemente und Beziehungen unter Beachtung der geltenden Anforderungen identifiziert und dem Modell hinzugefügt. Der Zeitaufwand für die Erstellung einer Modellinstanz wird deutlich reduziert und die resultierende Modellösung entspricht den geltenden Anforderungen. In dieser Arbeit wurden für die *Modell-Vervollständigung* zunächst einzelne Modellierungsschritte für die Komponenten von AMAN-ML festgelegt, die bei der Erstellung eines Modells regulär durchlaufen werden. Für jeden einzelnen Modellierungsschritt bestehen in AMAN-ML verschiedene Alternativen, die auf Basis der Constraints bewertet werden müssen. Hierzu wurden für jeden Modellierungsschritt geeignete FCSPs definiert, die eine Bewertung alternativer Modellierungsschritte vornehmen und die Bestimmung einer präferierten Lösung unter den alternativen Wertebelegungen ermöglichen.

Definition 1. $\vec{d_A} \geq_{\mathcal{P}}^{lex} \vec{d_A}$ *iff* $List(\vec{d_A}, \mathcal{P}) \geq_{lex} List(\vec{d_B}, \mathcal{P})$

Die Auswahl einer präferierten Lösung eines FCSP wird, wie in Definition 1 angegeben, über einen vollständigen lexikographischen Vergleich der geordneten Listen über die Erfüllungsgrade der einzelnen Constraints, basierend auf [FLS93], vorgenommen.

6 Das Gesamtsystem

Die Generierung von Constraints aus Erfahrungswissen und deren Integration in die Modellierungssprache sind in einen Entwicklungsprozess eingebettet, der sich aus zwei Phasen zusammensetzt. In der ersten Phase erfolgen die Spezifikation und die Modellierung des zu erstellenden Anflugplanungssystems, während der zweiten Phase die Integration der erzeugten Komponenten in das Gesamtsystem und deren Nutzung zugeordnet sind. In der ersten Phase erfolgen diejenigen Schritte des Entwicklungsprozesses, bei denen der Ausführungszeit keine Bedeutung zukommt. Die Generierung von Constraints an die Modellierungssprache aus formalem und erfahrungsbasiertem Wissen, die Erstellung flughafenspezifischer Modelle sowie deren Überprüfung und Vervollständigung gehören folglich in diese Phase. Hingegen gehören die Integration von erzeugten Codekomponenten und die Ausführung des erstellten Anflugplanungssystems der zweiten Phase an. Diese Trennung

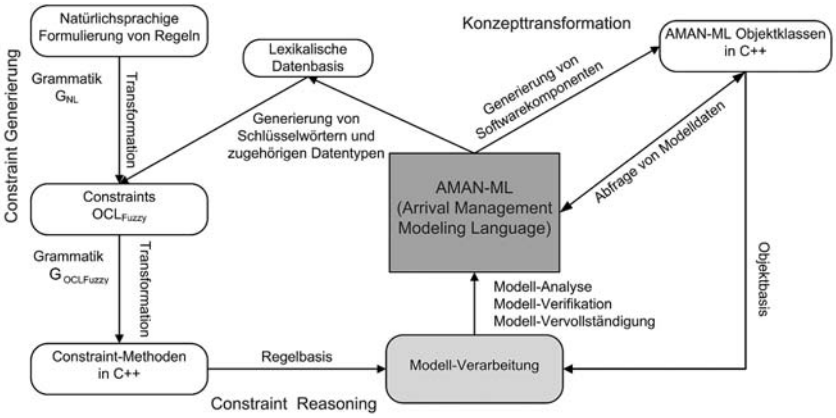


Abbildung 2: Systemkomponenten und Entwicklungsprozess

wurde in dieser Arbeit aufgrund der geforderten Echzeitfähigkeit für Anflugplanungssysteme vorgenommen. Der Entwicklungsprozess zur Generierung eines adaptierbaren Anflugplanungssystems sowie die in dieser Arbeit entwickelten Komponenten als Teil eines Gesamtsystems werden in Abbildung 2 dargestellt. Der Modellierungsprozess beginnt mit der Erstellung verschiedener Modellinstanzen zur Abbildung von Landebahnensystem, Luftraumstruktur, optimierender Zuweisungsstrategie und heuristischer Verfahrensweisen eines zu erstellenden Anflugplanungssystems. Die Grundlage für die Ermöglichung einer verlässlichen Modellverarbeitung und -auswertung bildet dabei die Transformation der Modellelemente und Constraints dieser Modellinstanzen in eine einheitliche Beschreibungsform. Die einzelnen Elemente (Objekte und Beziehungen) einer Modellkomponente werden daher auf Basis eines Transformationskonzepts für domänenspezifische Modellierungssprachen in korrespondierende Klassen einer objektorientierten Programmiersprache übersetzt. Eine Abfrage von konkreten Daten einer Modellinstanz aus AMAN-ML führt zu Objektinstanziierungen, die einer Objektgruppe für einen bestimmten Flughafen zugeordnet werden und damit eine Objektbasis für weitere Modellverarbeitungschritte repräsentieren (vgl. Abbildung 2).

Die Transformation von natürlicher Sprache wird in dieser Arbeit auf Basis einer Grammatik realisiert, deren Vokabular mit Schlüsselworten ergänzt wird, die aus dem Metamodell der Modellierungssprache abgeleitet werden. Mögliche Wortgruppen in einem natürlichsprachigen Satz können hierdurch besser eingegrenzt und erkannt werden. Ein formulierter Satz in natürlicher Sprache wird in dieser Arbeit zunächst in eine Constraint-Beschreibungssprache transformiert (Grammatik G_{NL}). Sprachliche Unbestimmtheiten werden dabei über die Verwendung verschiedener Sprachkonzepte und Worte angedeutet. Diese können wiederum erkannt und verwendet werden, um die Transformation in ein Zielformat entsprechend anzupassen. Die natürlichsprachigen Aussagen werden über die OCL formalisiert, deren standardisierte Syntax in dieser Arbeit um die Möglichkeit einer Verwendung von mehrwertigen Mengen (Fuzzy Sets) erweitert wurde. Vagheiten in einer

Aussage können daher direkt beschrieben und bei einer Verifikation berücksichtigt werden. In einem weiteren Schritt erfolgt eine Transformation der OCL-basierten Anforderungen in Methoden einer objektorientierten Programmiersprache (Grammatik $G_{OCLFuzzy}$). Diese Methoden beziehen sich gemäß der zugrunde liegenden OCL-basierten Anforderung auf eine bestimmte Gruppe von Objekten der Modellierungssprache und werden in einer gemeinsamen Regelbasis hinterlegt.

Die Objektbasis und die Regelbasis gehen in die *Modell-Verarbeitung* ein. Die einzelnen Elemente einer Modellinstanz werden gegen die, über die Regelbasis definierten, Anforderungen verifiziert. Mögliche Fehler in der Modellierung können auf diese Weise identifiziert werden (*Modell-Verifikation*). Darüber hinaus kann ein teilweise erstelltes Modell anhand der Regelbasis über mehrere Schritte zu einem gültigen Modell vervollständigt werden (*Modell-Vervollständigung*). Diese Aufgaben erfordern eine Schlussfolgerung (*Constraint Reasoning*) anhand einer gegebenen Modellinstanz und der darauf anwendbaren Teilmenge des Constraint Systems. Die einzelnen Komponenten zur Generierung von Constraints auf Basis von natürlicher Sprache sowie deren Integration in die Verarbeitung von Modellen werden in Abbildung 2 abgebildet.

7 Fazit und Ausblick

Die einzelnen Komponenten von AMAN-ML wurden von Fluglotsen validiert und in einem iterativen Prozess an die Erfordernisse der Anflugplanung angepasst. Verschiedene Experimente auf dem entstandenen System auf Basis der generierten Programmkomponenten wurden durchgeführt und mit vorab definierten Prognosen über das Systemverhalten verglichen. Die Grammatik wurde gegen verschiedene natürlichsprachige Formulierungen und die dabei erfolgte Erkennung spezifischer Merkmale validiert.

In den durchgeführten Experimenten und Studien konnte eine hohe Akzeptanz der Benutzer hinsichtlich der Verwendung von AMAN-ML festgestellt werden. Die Modellerstellung ist intuitiv gestaltet, da diese die Terminologie der Domäne verwendet und die Strukturen von AMAN-ML eng an die Elemente und Zusammenhänge des realen Systems angelehnt sind. Eine Generierung von Programmkomponenten wird Benutzern mit geringen Kenntnissen in Bezug auf das Anflugplanungssystem durch die Abstraktion von der Programmebene erleichtert. Dies konnte in den Validierungsstudien belegt werden. Die Fluglotsen ordneten die Modellierungssprache als gut verständlich ein und konnten bereits nach kurzer Zeit eigenständig erste Modelle erstellen. Die Methodik zur Integration von Erfahrungswissen in den Modellierungsprozess wurde von den Fluglotsen ebenfalls gut angenommen. Insbesondere die Möglichkeit zur Abbildung von erfahrungsbasierten Verfahrensweisen in einem Modell und deren Integration in die Planungen des Anflugplanungssystems wurde positiv bewertet. Die Modellierungssprache AMAN-ML wird seit 2010 am Deutschen Zentrum für Luft- und Raumfahrt e.V. operational eingesetzt. Dabei haben exemplarische Modellierungen für verschiedene Flughäfen eine hohe Zeitersparnis durch die Verwendung von AMAN-ML bestätigt. Während eine Anpassung des Anflugplanungssystems 4D-CARMA (4-Dimensional Coorperative Arrival Management System) für einen neuen Flughafen sonst mit einem Zeitaufwand von mehreren Monaten

verbunden ist, konnten im Rahmen dieser Arbeit verschiedene flughafenspezifische Modelle mit AMAN-ML bereits in wenigen Stunden erstellt und implementiert werden. Anhand des definierten Constraint Systems konnte zudem die korrekte und stets zuverlässige Funktionalität der generierten Programmkomponenten sichergestellt werden. Während der Experimente zeigten sich die Fluglotsen sehr interessiert an dem vorgelegten System und zeigten eine hohe Bereitschaft an der Mitarbeit zu dessen Verbesserung. Insbesondere die Möglichkeit zur Erfassung von Erfahrungswissen wurde positiv aufgenommen und bewertet. Dabei wurde jedoch von den Fluglotsen oft angemerkt, dass es wünschenswert wäre, neue Anforderungen auch während des operationalen Betriebs formulieren und direkt in die Planungen des Systems integrieren zu können.

Die hier entwickelte Grammatik für die natürliche Sprache wurde im Rahmen eines Projektes zur Spracherkennung an die Phraseologie von Fluglotsen im Sprechfunk angepasst und wird seither zur Erfassung von Anweisungen für eine Erkennung von Lotsenabsichten in der Anflugplanung eingesetzt.

Literatur

[BDFBK87] A. Borning, R. Duisberg, B. Freeman-Benson und A. Kramer. Constraint Hierarchies. In *Proceedings of the ACM Conference on Object-Oriented Programming Systems, Languages and Applications (OOPSLA'87)*, 1987.

[BEFK06] N. Bäuerle, O. Engelhardt-Funke und M. Kolonko. On the Waiting Time of Arriving Aircrafts and the Capacity of Airports with One or Two Runways. *European Journal of Operational Research*, 177 (Issue 2):1180–1196, 2006.

[Cho57] N. Chomsky. *Syntactic Structures*. Mouton de Gruyter, 1. Auflage, 1957.

[FLS93] H. Fargier, J. Lang und T. Schiex. Selecting preferred solutions in Fuzzy Constraint Satisfaction Problems. In *Proceedings of EUFIT'93*, 1993.

[Gei12] D. Geister. *Constraint Generierung für domänenspezifische Modellierungssprachen*. Forschungsbericht 2012-15, Deutsches Zentrum für Luft- und Raumfahrt e.V., 2012.

[Shi85] S. M. Shieber. Evidence against the context-freeness of natural languages. *Linguistics and Philosophy*, 8:333–343, 1985.

[Wan09] Y. X. Wang. A Formal Syntax of Natural Languages and the Deductive Grammar. *Fundamenta Informaticae*, 90(4):353–368, 2009.



Dagi Geister hat ihr Studium der Wirtschaftswissenschaften mit Schwerpunkt Informatik an der Leibniz Universität Hannover im April 2005 abgeschlossen. Ihre Diplomarbeit verfasste sie zum Thema XML-basierte Datenaustauschformate im B2B-Bereich in Kooperation mit der IBM Deutschland. Seit 2007 arbeitet sie am Deutschen Zentrum für Luft- und Raumfahrt e.V. und hat dort ihre Promotionsarbeit über die natürlichsprachige Anpassung von Assistenzsystemen für Fluglotsen angefertigt. Seitdem ist sie u.a. für die Entwicklung neuer Konzepte für die Luftfahrt, insbesondere Unbemannter Luftfahrzeugsysteme (UAS) und deren Integration in den zivilen Luftraum, verantwortlich.

Von überwachten zu unüberwachten Support-Vektor-Maschinen und Anwendungen in der Astronomie*

Fabian Gieseke

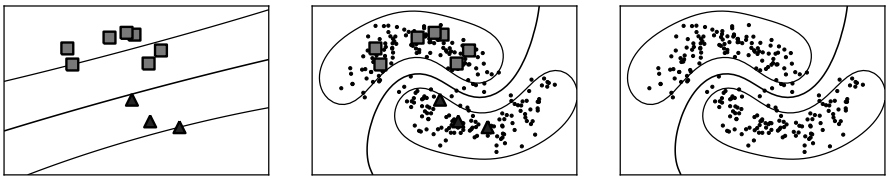
Department für Informatik
Carl von Ossietzky Universität Oldenburg
f.gieseke@uni-oldenburg.de

Abstract: Ein bekanntes Problem des maschinellen Lernens ist die Klassifikation von Objekten. Entsprechende Modelle basieren dabei meist auf Trainingsdaten, welche aus Mustern mit zugehörigen Labeln bestehen. Die Erstellung eines hinreichend großen Datensatzes kann sich für gewisse Anwendungsfälle jedoch als sehr kosten- oder zeitintensiv erweisen. Eine aktuelle Forschungsrichtung des maschinellen Lernens zielt auf die Verwendung von (zusätzlichen) ungelabelten Mustern ab, welche oft ohne großen Aufwand gewonnen werden können. In diesem Beitrag wird die Erweiterung von sogenannten Support-Vektor-Maschinen auf solche Lernszenarien beschrieben. Im Gegensatz zu Support-Vektor-Maschinen führen diese Varianten jedoch zu kombinatorischen Optimierungsproblemen. Die Entwicklung effizienter Optimierungsstrategien ist daher ein erstrebenswertes Ziel und soll im Rahmen dieses Beitrags diskutiert werden. Weiterhin werden mögliche Anwendungsgebiete der entsprechenden Verfahren erläutert, welche sich unter anderem im Bereich der Astronomie wiederfinden.

1 Einleitung

Das Gebiet des *maschinellen Lernens* [HTF09] hat innerhalb der letzten Jahren stark an Bedeutung gewonnen. Einer der Gründe hierfür ist die Tatsache, dass die Datenvolumina in den verschiedensten Bereichen dramatisch zugenommen haben. Dies ist beispielsweise in der Astronomie der Fall, wo aktuelle und zukünftige Projekte Daten im Tera- und Petabytebereich liefern und liefern werden [ITA+11, YAAA00]. Die Analyse dieser Datenmengen „per Hand“ ist im Allgemeinen nicht mehr möglich und erfordert maschinelle Lernverfahren zur (halb-)automatisierten Wissensextraktion. Die Klassifikation von Objekten zählt mit zu den wichtigsten Problemen des maschinellen Lernens. Als Ausgangspunkt stehen hier im Allgemeinen Trainingsdaten in Form von *Mustern* und zugehörigen *Labeln* zur Verfügung. Das Ziel des Lernprozesses besteht darin, auf Basis der bekannten Trainingsdaten entsprechende Modelle zu erstellen, welche bisher unbekannte Muster klassifizieren können. Diese Form wird als *überwachtes Lernen* [HTF09] bezeichnet.

*Der vorliegende Text stellt eine Kurzfassung meiner Dissertation [Gie11] mit dem Originaltitel *„From Supervised to Unsupervised Support Vector Machines and Applications in Astronomy“* dar.



(a) Überwacht (b) Halbüberwacht (c) Unüberwacht

Abbildung 1: Das Ziel einer SVM besteht darin, auf Basis gelabelter Muster (rote Quadrate und blaue Dreiecke) diejenige Hyperebene zu finden (mittlere Linie), welche den Abstand zu den Mustern maximiert, vgl. Abb. (a). Oft sind gelabelte Muster jedoch nur in geringem Umfang vorhanden; ungelabelte Muster (schwarze Punkte) können hingegen meist leicht erhalten werden. Halbüberwachte SVM können auf Basis dieser zusätzlichen Informationen zu besseren Modellen führen, vgl. Abb. (b). Sind keine gelabelten Muster vorhanden, so kann zwar die „Struktur" der Daten erfasst werden, die Klassenzugehörigkeit ist allerdings nicht mehr ersichtlich, vgl. Abb. (c).

Das Konzept einer *Support-Vektor-Maschine* (SVM) [SS01, SC08] zählt mit zu den erfolgreichsten Methoden im Bereich des maschinellen Lernens. Sind hinreichend viele Trainingsdaten vorhanden, so weisen die zugehörigen Modelle oft eine exzellente Klassifikationsgüte auf; die Erstellung eines solchen Trainingsdatensatzes erweist sich in vielen Anwendungsfällen jedoch oft als sehr aufwendig. Im Gegensatz zu gelabelten Trainingsdaten können ungelabelte Muster meist ohne großen Aufwand gewonnen werden. Um auch letztere in der Trainingsphase zu verwenden, wurden in der Literatur unter anderem *halb-* und *unüberwachte Support-Vektor-Maschinen* vorgestellt [BD99, Joa99, VS77, XNLS05]. In vielen Fällen ermöglichen diese Erweiterungen die Generierung von Modellen mit einer deutlich besseren Güte. Die konkrete Anwendung dieser Erweiterungen auf reale Fragestellungen wird jedoch dadurch erschwert, dass hierzu *kombinatorische Optimierungsprobleme* citeBoydV2004 gelöst bzw. möglichst gut approximiert werden müssen.

Im Folgenden werden Support-Vektor-Maschinen und deren Erweiterungen sowie Optimierungsansätze skizziert. Zudem werden Anwendungsgebiete der Verfahren beschrieben.

2 Support-Vektor-Maschinen

In ihrer ursprünglichen Form zielen Support-Vektor-Maschinen auf die *binäre Klassifikation* ab, welche in diesem Abschnitt näher erläutert werden soll.

2.1 Überwachte Lernszenarien

Für solche Lernszenarien stehen Muster zweier Klassen zur Verfügung, welche durch einen *Trainingsdatensatz* $T_L = \{(\mathbf{x}'_1, y'_1), \ldots, (\mathbf{x}'_l, y'_l)\} \subset \mathbb{R}^d \times \{-1, +1\}$ repräsentiert werden können. Das Ziel einer Support-Vektor-Maschine besteht darin, diejenige Hyperebene zu finden, welche die Muster beider Klassen am besten „trennt", und zwar so, dass

die induzierte Distanz zwischen der Hyperebene und den Mustern maximal ist. Weiterhin sollen nur wenige Muster in dem induzierten Korridor liegen. Aus mathematischer Sicht führt dies zu einem effizient lösbaren *quadratischen Programm* [BV04] der Form

$$\begin{aligned} \underset{\mathbf{w}\in\mathbb{R}^d,\, b\in\mathbb{R},\, \boldsymbol{\xi}'\in\mathbb{R}^l}{\text{minimiere}} \; & \frac{1}{2}\|\mathbf{w}\|^2 + C\sum_{i=1}^{l}\xi_i' \\ \text{s.d. } & y_i'(\langle \mathbf{w}, \mathbf{x}_i'\rangle + b) \geq 1 - \xi_i',\ \xi_i' \geq 0, \end{aligned} \tag{1}$$

wobei der erste Term mit der Maximierung des Abstandes und der zweite Term mit der „Bestrafung“ von Mustern im Korridor korrespondiert [SS01, SC08]. Der Parameter $C > 0$ bestimmt hierbei den Kompromiss zwischen diesen beiden Teilzielen.

Mit Hilfe von *Kernfunktionen* $k : \mathbb{R}^d \times \mathbb{R}^d \to \mathbb{R}$ kann dieses Konzept auf nicht-lineare Hyperebenen erweitert werden [SS01, SC08]. In Abb. 1 (a) ist eine solche nicht-lineare Support-Vektor-Maschine dargestellt. Hierbei stellen die roten Quadrate und die blauen Dreiecke die gelabelten Muster und die mittlere Linie die nicht-lineare Hyperebene dar. Der Rand ist durch die beiden äußeren Linien skizziert. Neue, bisher nicht betrachtete Muster können nun mittels dieses Modells in die beiden Klassen eingeteilt werden.

2.2 Halbüberwachte Lernszenarien

Support-Vektor-Maschinen zählen zu den überwachten Lernverfahren [HTF09], da nur auf gelabelte Muster zurückgegriffen wird. Die Verwendung von gelabelten und ungelabelten Mustern $T_U = \{\mathbf{x}_1, \ldots, \mathbf{x}_u\} \subset \mathbb{R}^d$ führt zu den *halbüberwachten Support-Vektor-Maschinen* [BD99, Joa99, VS77]. Ziel dieser Variante ist, diejenige Partition der ungelabelten Muster in zwei Klassen zu finden, so dass eine anschließende Anwendung einer (modifizierten) Support-Vektor-Maschine zu dem bestmöglichen Ergebnis führt, siehe Abb. 1 (b). Ähnlich zu dem überwachten Fall weist die Hyperebene einen großen Abstand zu den gelabelten Mustern auf, jedoch verläuft diese *nicht* durch die von den ungelabelten Mustern (schwarze Punkte) erzeugten Überdichten. In diesem Fall bieten die ungelabelten Muster also wertvolle zusätzliche Informationen über die „Struktur“ der Daten. Es ist direkt ersichtlich, dass das finale Modell eine bessere Qualität aufweist.

2.3 Unüberwachte Lernszenarien

Die sogenannten *unüberwachten Support-Vektor-Maschinen* greifen nur auf eine Menge $T_U = \{\mathbf{x}_1, \ldots, \mathbf{x}_u\} \subset \mathbb{R}^d$ ungelabelter Muster zurück, beziehen also keine gelabelten Muster ein. Das Lernziel dieser Variante besteht darin, diejenige Partition der ungelabelten Muster in zwei Klassen zu finden, so dass eine anschließende Anwendung einer Support-Vektor-Maschine zu dem optimalen Ergebnis führt, siehe Abb. 1 (c). Es wird also ein zu dem halbüberwachten Fall sehr ähnliches Ziel verfolgt. Ursprünglich wurde diese Modifikation unter dem Namen *Maximum Margin Clustering* [XNLS05] vorgestellt.

Algorithmus 1 Exakte Suche in polynomieller Zeit

1: Konstruiere den *Graphen* $\mathcal{G}$ (bestehend aus $\mathcal{O}(u^d)$ Knoten)
2: **for** jeden Knoten v in $\mathcal{G}$ **do**
3: Sei $\mathbf{y} \in \{-1, +1\}^u$ der zugehörige Partitionsvektor.
4: Teste $\mathbf{y}$ mittels Anwendung einer Support-Vektor-Maschine (in $\mathcal{O}(u^3)$ Zeit).
5: Merke Ergebnis, falls besser als vorher.
6: **end for**

3 Kombinatorische und nicht-konvexe Optimierung

Beide oben skizzierten Erweiterungen führen zu kombinatorischen Optimierungsproblemen, da die optimale Partition der ungelabelten Muster im Vorfeld nicht bekannt ist. Aus mathematischer Sicht erhält man für den unüberwachten Fall beispielsweise ein Optimierungsproblem der Gestalt

$$\begin{aligned} \underset{\substack{\mathbf{y}\in\{-1,+1\}^u,\\ \mathbf{w}\in\mathbb{R}^d,\, b\in\mathbb{R},\, \boldsymbol{\xi}\in\mathbb{R}^u}}{\text{minimiere}} \quad & \frac{1}{2}\|\mathbf{w}\|^2 + C\sum_{i=1}^{u}\xi_i \\ \text{s.d.} \quad & y_i(\langle \mathbf{w}, \mathbf{x}_i\rangle + b) \geq 1 - \xi_i,\ \xi_i \geq 0, \end{aligned} \tag{2}$$

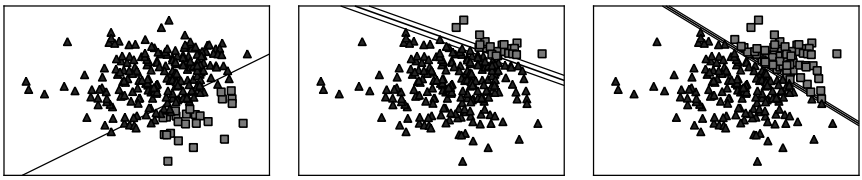
Eine mögliche Partition ergibt sich durch Zuordnung aller Muster zu genau einer Klasse. Diese unerwünschte Lösung kann durch eine Hinzunahme einer weiteren Nebenbedingung der Form $\left|\frac{1}{u}\sum_{i=1}^{u}\max(0, y_i) - b_c\right| < \varepsilon$ mit entsprechenden Parametern $b_c \in [0, 1]$ und $\varepsilon > 0$ verhindert werden.

Die Suche nach einer geeigneten Belegung des Vektors $\mathbf{y}$ stellt die wesentliche Herausforderung im Kontext des obigen Optimierungsproblems dar. Da es sich bei dieser Erweiterung um ein gemischt-ganzzahliges Optimierungsproblem [Flo95] handelt, kann zur Lösung auf Standardverfahren für diese Problemklasse zurückgegriffen werden. Da Probleme dieser Problemklasse jedoch im Allgemeinen NP-schwer sind [Flo95], ist die Bestimmung von Lösungen in polynomieller Zeit nicht sichergestellt. Ein trivialer Ansatz besteht zudem darin, jede mögliche Belegung des Partitionsvektors mittels einer Support-Vektor-Maschine zu „testen“. Diese Herangehensweise ist jedoch aufgrund der exponentiellen Laufzeit nur für sehr kleine Probleminstanzen geeignet. Aus theoretischer Sicht stellt sich deshalb die Frage, ob Lösungsverfahren mit polynomieller Laufzeit existieren.

3.1 Exakte Lösungen in polynomieller Laufzeit

Wie in diesem Abschnitt beschrieben wird, ist dies für den Spezialfall einer linearen Kernfunktion und Mustern aus $\mathbb{R}^d$ möglich. Der entsprechende Lösungsansatz greift dabei auf komplexe Ergebnisse aus dem Bereich der *Algorithmischen Geometrie* [Ede87] zurück.

Theorem 1 *[[Gie11, GVJ12]] Sei $T_U = \{\mathbf{x}_1, \ldots, \mathbf{x}_u\} \subset \mathbb{R}^d$. Dann kann für eine lineare*



(a) $C = 0.001$ (b) $C = 1$ (c) $C = 1000$

Abbildung 2: Unüberwachte Support-Vektor-Maschinen: Exakte Lösungen für eine Menge von Punkten im $\mathbb{R}^2$ und verschiedene Belegungen des Parameters C.

Kernfunktion $k(\mathbf{x}_i, \mathbf{x}_j) = \langle \mathbf{x}_i, \mathbf{x}_j \rangle$ eine exakte Lösung (bis auf Maschinengenauigkeit) für das Optimierungsproblem (2) in $\mathcal{O}(u^{d+3})$ Laufzeit bestimmt werden.

Beweisidee: Die Kernidee besteht darin, eine Bijektion zwischen allen (überhaupt) in Frage kommenden Partitionen der ungelabelten Muster und den Knoten eines speziellen Graphen $\mathcal{G}$ herzustellen. Jede möglich optimale Partition $\mathbf{y}$ korrespondiert also mit genau einem Knoten v von $\mathcal{G}$. Ein bekanntes (nicht-triviales) Ergebnis aus der Algorithmischen Geometrie ist, dass dieser Graph höchstens $\mathcal{O}(u^d)$ Knoten enthalten kann. Dadurch ergibt sich das in Algorithmus 1 dargelegte Verfahren. Die Konstruktion des Graphen benötigt dabei $\mathcal{O}(u^d)$ Laufzeit. Da jede induzierte Partition mittels einer Support-Vektor-Maschine in $\mathcal{O}(u^3)$ Laufzeit getestet werden kann, ergibt sich die obere Laufzeitschranke. □

Das obige Ergebnis ist vor allem aus theoretischer Sicht interessant. Der zugrundeliegende Algorithmus kann jedoch auch zur Generierung von Benchmark-Datensätzen verwendet werden, siehe Abb. 2. Für hochdimensionale Datensätze ist das Verfahren jedoch von wenig praktischer Relevanz. Im Folgenden werden daher zwei Heuristiken entwickelt, welche möglichst gute Lösungen in praktikabler Laufzeit bestimmen können.

3.2 Matrizenbasierte beschleunigte lokale Suche

Aus anwendungstechnischer Sicht ist vor allem der halbüberwachte Fall interessant, der nachfolgend betrachtet werden soll. Diese Variante führt erneut zu einem gemischt-ganzzahligen Optimierungsproblem der Gestalt:

$$\begin{aligned} \underset{\substack{\mathbf{y}\in\{-1,+1\}^u,\\ \mathbf{w}\in\mathbb{R}^d,\, b\in\mathbb{R},\, \boldsymbol{\xi}'\in\mathbb{R}^l,\, \boldsymbol{\xi}\in\mathbb{R}^u}}{\text{minimiere}} \quad & \frac{1}{2}\|\mathbf{w}\|^2 + C' \sum_{i=1}^{l} \xi_i' + C \sum_{i=1}^{u} \xi_i \\ \text{s.d.} \quad & y_i'(\langle \mathbf{w}, \mathbf{x}_i' \rangle + b) \geq 1 - \xi_i',\ \xi_i' \geq 0, \\ \text{und} \quad & y_i(\langle \mathbf{w}, \mathbf{x}_i \rangle + b) \geq 1 - \xi_i,\ \xi_i \geq 0, \end{aligned} \tag{3}$$

mit Modellparametern $C' > 0$ und $C > 0$ [VS77]. Einer der ersten Optimierungsansätze wurde von Joachims [Joa99] vorgestellt und ist in Algorithmus 2 skizziert: Nach

Algorithmus 2 Beschleunigte lokale Suche

1: Initialisiere Partitionsvektor $\mathbf{y} \subseteq \{-1, +1\}^n$.
2: **while** nicht konvergiert **do**
3: $\quad \bar{\mathbf{y}} \leftarrow \mathbf{y}$ mit einzelner „vertauschter“ Koordinate
4: $\quad$ **if** $F(\bar{\mathbf{y}}) < F(\mathbf{y})$ **then**
5: $\quad\quad \mathbf{y} \leftarrow \bar{\mathbf{y}}$
6: $\quad$ **end if**
7: **end while**

der Initialisierung des Partitionsvektors $\mathbf{y}$ mit einer sinnvollen Belegung wird diese erste „Schätzung“ iterativ verbessert, indem pro Iteration eine Koordinate vertauscht wird.[1] Hierbei bezeichne $F(\mathbf{y})$ die Zielfunktion (3) für einen fest-gewählten Partitionsvektor $\mathbf{y}$.

Eine direkte Implementation ist jedoch sehr rechenintensiv, da im Allgemeinen eine große Anzahl an Vertauschungen vorgenommen werden muss bis das Verfahren konvergiert (ein einzelner Funktionsaufruf in Schritt 4 benötigt $\mathcal{O}(n^3)$ Laufzeit, wobei $n = l + u$). Die lokale Suchstrategie lässt sich allerdings sehr effizient umsetzen; Kernidee ist hierbei, Varianten der ursprünglichen Support-Vektor-Maschinen zu betrachten, welche auf der quadratischen Verlustfunktion basieren [Rif02]. Dies führt zu einer Zielfunktion der Form

$$F(\bar{\mathbf{y}}) = \bar{\mathbf{y}}^{\mathrm{T}} \mathbf{\Lambda} \underbrace{\left(\mathbf{I} - \overline{\mathbf{K}}\mathbf{G} - \mathbf{G}\overline{\mathbf{K}} + \mathbf{G}\overline{\mathbf{K}}\overline{\mathbf{K}}\mathbf{G} + \lambda \mathbf{G}\overline{\mathbf{K}}\mathbf{G}\right)}_{=:\mathbf{H}} \mathbf{\Lambda}\bar{\mathbf{y}}, \tag{4}$$

wobei $\mathbf{K} \in \mathbb{R}^{n \times n}$ die Kernelmatrix, $\mathbf{\Lambda} \in \mathbb{R}^{n \times n}$ eine Diagonalmatrix mit Einträgen der Form $[\mathbf{\Lambda}]_{i,i} = \sqrt{\frac{1}{l}}$ für $i = 1, \ldots, l$ und $[\mathbf{\Lambda}]_{i,i} = \sqrt{\frac{\gamma}{u}}$ für $i = l+1, \ldots, n$, und $\overline{\mathbf{K}} := \mathbf{\Lambda}\mathbf{K}\mathbf{\Lambda}$ und $\mathbf{G} := (\mathbf{\Lambda}\mathbf{K}\mathbf{\Lambda} + \lambda\mathbf{I})^{-1}$ entsprechende Matrizen sein. Diese Zerlegung ermöglicht eine effizientes „Updaten“ der Funktionswerte pro Iteration:

Theorem 2 *([Gie11, GPK09, GKAP12, GKAP11]) Jede Iteration (Schritte 3–6) von Algorithmus 2 kann in $\mathcal{O}(n)$ Laufzeit getätigt werden.*

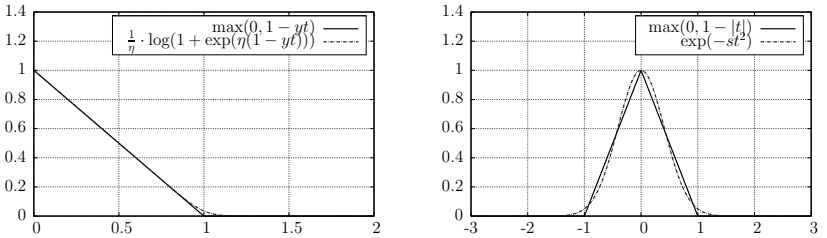
Beweisidee: Die Kernidee besteht darin, zunächst die Matrix $\mathbf{H}\mathbf{\Lambda}$ in $\mathcal{O}(n^3)$ Zeit zu berechnen und anschließend den Vektor $\mathbf{H}\mathbf{\Lambda}\mathbf{y} \in \mathbb{R}^n$ pro Iteration mittels

$$\mathbf{H}\mathbf{\Lambda}\bar{\mathbf{y}} = \mathbf{H}\mathbf{\Lambda}\mathbf{y} - 2y_j(\mathbf{H}\mathbf{\Lambda})_{[n],\{j\}} \tag{5}$$

zu erneuern, wobei j die vertauschte Koordinate und $(\mathbf{H}\mathbf{\Lambda})_{[n],\{j\}}$ die j-te Spalte von $\mathbf{H}\mathbf{\Lambda}$ sei. Dieses Update kann in linearer Zeit getätigt werden. Anschließend kann $F(\bar{\mathbf{y}})$ ebenfalls in linearer Laufzeit bestimmt werden (Multiplikation zweier Vektoren) [Gie11]. □

Die obige Auswertung der Zielfunktion in linearer Laufzeit ermöglicht somit eine hocheffiziente Umsetzung der lokalen Suche, welche pro Iteration nur $\mathcal{O}(n)$ anstatt $\mathcal{O}(n^3)$ Laufzeit benötigt. Dies ermöglicht eine deutlich bessere Exploration des Suchraums und somit eine bessere Güte der bestimmten Lösung.

[1] Als Schätzung kommt z.B. die durch Anwendung einer auf den gelabelten Mustern trainierten Support-Vektor-Maschine induzierte Partition in Frage; zudem können jeweils mehrere Koordinaten vertauscht werden.



(a) (b)

Abbildung 3: In Abb. (a) ist der *hinge loss* $\mathcal{L}(y,t) = \max(0, 1-yt)$ und seine differenzierbare Ersatzfunktion $\mathcal{L}(y,t) = \frac{1}{\eta}\log(1+\exp(\eta(1-yt)))$ mit $y = +1$ und $\eta = 20$ gezeigt. Die zugehörige effektive Verlustfunktion $\mathcal{L}(t) = \max(0, 1-|t|)$ und deren Ersatzfunktion $\mathcal{L}_e(t) = \exp(-st^2)$ mit $s = 3$ sind in Abb. (b) gezeigt.

3.3 Gradientenbasierte Optimierung

Eine spezielle Eigenschaft des Optimierungsproblems (3) ist die Tatsache, dass es als *kontinuierliches* Optimierungsproblem formuliert werden kann, und zwar in der Form

$$\underset{\mathbf{c}\in\mathbb{R}^n,\, b\in\mathbb{R}}{\text{minimiere}} \qquad \frac{1}{l}\sum_{i=1}^{l}\mathcal{L}\big(y_i', f(\mathbf{x}_i')+b\big) + \gamma\frac{1}{u}\sum_{i=1}^{u}\mathcal{L}_e\big(f(\mathbf{x}_i)+b\big) + \lambda\mathbf{c}^{\mathrm{T}}\mathbf{K}\mathbf{c} \tag{6}$$

wobei $\bar{\mathbf{x}}_i = \mathbf{x}_i'$ für $i = 1,\ldots,l$ und $\bar{\mathbf{x}}_i = \mathbf{x}_{i-l}$ für $i = l+1,\ldots,n$, und $f(\cdot) = \sum_{j=1}^{n} c_j k(\cdot, \bar{\mathbf{x}}_j)$ sei. Die Qualität des Modells wird dabei mittels zweier Verlustfunktionen bestimmt, wobei $\mathcal{L}$ der sogenannte *hinge loss* und $\mathcal{L}_e(t) = \mathcal{L}(\mathrm{sgn}(t), t)$ die zugehörige *effektive Verlustfunktion* ist, siehe Abb. 3.

Da die Funktion $\mathcal{L}_e$ nicht konvex ist, ist auch die Zielfunktion nicht konvex. Weiterhin existieren die partiellen Ableitungen nicht; dies schließt eine direkte Anwendung effizienter gradientenbasierter Optimierungsstrategien aus. Eine mögliche Herangehensweise besteht darin, auf differenzierbare Ersatzfunktionen für $\mathcal{L}$ und $\mathcal{L}_e$ zurückzugreifen [CZ05], siehe Abb. 3. Dies führt zu einer alternativen (aber sehr ähnlichen) Zielfunktion der Gestalt

$$\begin{aligned} F_\gamma(\mathbf{c}) = \; & \frac{1}{l}\sum_{i=1}^{l}\frac{1}{\eta}\log\left(1+\exp(\eta(1-y_i' f(\bar{\mathbf{x}}_i)))\right) \\ & + \frac{\gamma}{u}\sum_{i=1}^{u}\exp(-3(f(\bar{\mathbf{x}}_{l+i}))^2) + \lambda\sum_{i=1}^{n}\sum_{j=1}^{n} c_i c_j k(\bar{\mathbf{x}}_i, \bar{\mathbf{x}}_j), \end{aligned} \tag{7}$$

Das folgende Theorem zeigt, dass sowohl die Ersatzfunktion $F_\gamma(\mathbf{c})$ als auch deren Gradient $\nabla F_\gamma(\mathbf{c})$ effizient für eine beliebige Zwischenlösung $\mathbf{c} \in \mathbb{R}^n$ bestimmt werden kann:

Theorem 3 *([Gie11, GAPK12]) Für eine lineare Kernfunktion mit Mustern aus $\mathbb{R}^d$ und Datenmatrix $\mathbf{X} \in \mathbb{R}^{n\times d}$ mit $s \ll nd$ von Null verschiedenen Einträgen kann $F_\gamma(\mathbf{c})$ und $\nabla F_\gamma(\mathbf{c})$ in $\mathcal{O}(s)$ Laufzeit und Speicherplatz für ein beliebiges $\mathbf{c} \in \mathbb{R}^n$ bestimmt werden.*

Datensatz	l	u	LIBSVM	UniverSVM	S^2RLSC	QN-S^3VM
USPS(2,5)	16	806	10.5 ± 4.7	5.6 ± 3.6	6.3 ± 2.8	5.4 ± 1.7
USPS(2,7)	17	843	4.9 ± 2.9	2.3 ± 1.0	1.4 ± 0.2	3.6 ± 3.3
USPS(3,8)	15	751	12.9 ± 8.3	8.0 ± 3.5	6.2 ± 2.7	10.8 ± 8.9
USPS(8,0)	22	1108	5.0 ± 2.0	2.8 ± 2.2	1.8 ± 0.6	3.4 ± 1.3
TEXT	48	924	24.8 ± 9.6	6.7 ± 0.9	6.2 ± 0.9	8.2 ± 3.2
TEXT	389	584	4.9 ± 0.7	4.7 ± 0.4	5.0 ± 1.1	4.6 ± 0.6

Tabelle 1: Klassifikationsfehler von überwachten (LIBSVM) und halbüberwachten Support-Vektor-Maschinen (UniverSVM, S^2RLSC, QN-S^3VM) für Ziffern- und Texterkennung. Für die Trainingsphase kann dabei auf jeweils l gelabelte und u ungelabelte Muster zurückgegriffen werden. Angegeben ist der mittlere Fehler sowie die Standardabweichung über 10 Partitionen der Trainingsmuster.

Beweisidee: Der Gradient kann geschrieben werden als

$$\nabla F_\gamma(\mathbf{c}) \quad = \quad \mathbf{K}\mathbf{a} + 2\lambda\mathbf{K}\mathbf{c} \tag{8}$$

mit einem entsprechenden Vektor $\mathbf{a} \in \mathbb{R}^n$ [GAPK12]. Aufgrund der linearen Kernfunktion kann $\mathbf{K}\mathbf{c} = \mathbf{X}(\mathbf{X}^{\mathrm{T}}\mathbf{c})$ in $\mathcal{O}(s)$ Laufzeit bestimmt werden. Dies ermöglicht die effiziente Berechnung von $F_\gamma(\mathbf{c})$ und $\nabla F_\gamma(\mathbf{c})$ in $\mathcal{O}(s)$ Laufzeit, siehe [Gie11] für Details. □

Ähnliche Berechnungen können auch für andere Datenszenarien (und nicht-lineare Kernfunktionen) erzielt werden. Hinsichtlich der lokalen Suche kann anschließend auf Blackbox-Verfahren zur gradientenbasierten Optimierung zurückgegriffen werden. Als besonders geeignet haben sich hier spezielle Varianten des Newton-Verfahrens erwiesen, welche die Hesse-Matrix nicht explizit bestimmen sondern nur approximieren [Gie11, GAPK12].

4 Anwendungen und Ausblick

In Tabelle 1 sind die Klassifikationsergebnisse einer überwachten Support-Vektor-Maschine (LIBSVM) und drei halbüberwachten Implementationen gezeigt (S^2RLSC ist die beschleunigte lokale Suche und QN-S^3VM das gradientenbasierte Verfahren; Universvm eine weitere halbüberwachte Vergleichsmethode). Die betrachteten Datensätze stammen aus zwei Anwendungsgebieten: Handschriftenerkennung (USPS, siehe Abb. 4) und Textklassifikation (Text). Die Ergebnisse zeigen, dass ein deutlich geringerer Klassifikationsfehler mit den halbüberwachten Varianten erzielt werden kann (um teilweise ca. 20%).

Exemplarisch sei noch ein Beispiel aus der Astronomie skizziert: Abb. 4 zeigt Bilddaten des *Sloan Digital Sky Survey* [YAAA00], wobei eine der Klassifikationsaufgaben darin besteht, elliptische Galaxien von Spiralgalaxien zu trennen. Falls nur wenige gelabelte Muster zur Verfügung stehen (hier: 10), so liefert eine Support-Vektor-Maschine einen Fehler von mehr als 30%; durch Hinzunahme von (117) ungelabelten Mustern kann dieser

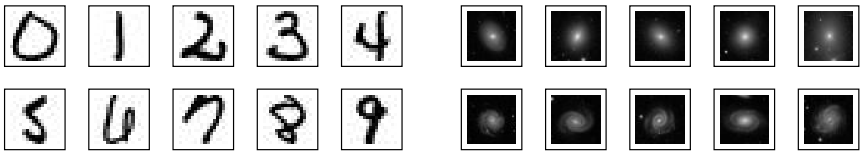


Abbildung 4: USPS-Zifferndatensatz [HTF09] und photometrische Daten von Galaxien [YAAA00].

mit der halbüberwachten Variante (QN−S^{3}VM) auf ca. 20% gesenkt werden.[2]

Da solche gelabelten Muster im Bereich der Astronomie für spezielle Fragestellungen oft nur in einem geringen Umfang zur Verfügung stehen, bieten halbüberwachte Ansätze ein enormes Potential. Dies trifft nicht nur auf Klassifikations- sondern auch auf z.B. Regressionsszenarien zu, wie aktuelle Arbeiten im Kontext der Schätzung der Rotverschiebung von sogenannten *Quasaren* [PZG13] eindrucksvoll zeigen. Der Bedarf entsprechender Techniken wird in naher Zukunft stark ansteigen, beispielsweise im Rahmen des *Large Synoptic Survey Telescope* [ITA$^+$11], welches *pro Nacht* 50 Terabyte an Daten liefern wird. Neben den riesigen Datenmengen wird hier vor allem der Mangel an gesicherten Label-Informationen ein großes Problem darstellen.

Danksagung. Teile der in diesem Beitrag vorgestellten Ergebnisse wurden von der *Deutschen Forschungsgemeinschaft* (DFG) unterstützt (KR 3695/2-1).

Literatur

[BD99] Kristin P. Bennett und Ayhan Demiriz. Semi-supervised support vector machines. In *Advances in Neural Information Proc. Systems 11*, Seiten 368–374. MIT Press, 1999.

[BV04] Stephen Boyd und Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[CZ05] Olivier Chapelle und Alexander Zien. Semi-Supervised Classification by Low Density Separation. In *Proc. of the 10th Int. Work. on Art. Intell. and Stat.*, Seiten 57–64, 2005.

[Ede87] Herbert Edelsbrunner. *Algorithms in Combinatorial Geometry*. Springer-Verlag, New York, NY, USA, 1987.

[Flo95] Christodoulos A. Floudas. *Nonlinear and Mixed-Integer Optimization: Fundamentals and Applications*. Oxford University Press, USA, 1995.

[GAPK12] Fabian Gieseke, Antti Airola, Tapio Pahikkala und Oliver Kramer. Sparse Quasi-Newton Optimization for Semi-Supervised Support Vector Machines. In *Proc. of the 1st Int. Conf. on Pattern Recognition Applications and Methods*, Seiten 45–54, 2012.

[Gie11] Fabian Gieseke. *From Supervised to Unsupervised Support Vector Machines and Applications in Astronomy*. Dissertation, Department für Informatik, Carl von Ossietzky Universität Oldenburg, 2011.

[2] Eine Support-Vektor-Maschine trainiert mit allen 127 Bildern liefert hier einen Fehler von ca. 15%.

[GKAP11] Fabian Gieseke, Oliver Kramer, Antti Airola und Tapio Pahikkala. Speedy Local Search for Semi-Supervised Regularized Least-Squares. In *Proc. of the 34th Annual German Conf. on Artificial Intelligence*, Seiten 87–98. Springer, 2011.

[GKAP12] Fabian Gieseke, Oliver Kramer, Antti Airola und Tapio Pahikkala. Efficient Recurrent Local Search Strategies for Semi- and Unsupervised Regularized Least-Squares Classification. *Evolutionary Intelligence*, 5(3):189–205, 2012.

[GPK09] Fabian Gieseke, Tapio Pahikkala und Oliver Kramer. Fast Evolutionary Maximum Margin Clustering. In *Proceedings of the 26th International Conference on Machine Learning*, Seiten 361–368, 2009.

[GVJ12] Fabian Gieseke, Jan Vahrenhold und Xiaoyi Jiang. On the Complexity of Exact Linear Semi- and Unsupervised Support Vector Machines. 2012. Manuskript.

[HTF09] Trevor Hastie, Robert Tibshirani und Jerome Friedman. *The Elements of Statistical Learning*. Springer, 2. Auflage, 2009.

[ITA+11] Z. Ivezic, J. A. Tyson, E. Acosta, R. Allsman und andere. LSST: from Science Drivers to Reference Design and Anticipated Data Products. 2011.

[Joa99] Thorsten Joachims. Transductive Inference for Text Classification using Support Vector Machines. In *Proc. of the Int. Conf. on Machine Learning*, Seiten 200–209, 1999.

[PZG13] Kai Lars Polsterer, Peter-Christian Zinn und Fabian Gieseke. Finding New High-Redshift Quasars by Asking the Neighbours. *Monthly Notices of the Royal Astronomical Society*, 428(1):226–235, 2013.

[Rif02] Ryan Michael Rifkin. *Everything Old is New Again: A Fresh Look at Historical Approaches in Machine Learning*. Dissertation, MIT, 2002.

[SC08] Ingo Steinwart und Andreas Christmann. *Support Vector Machines*. Springer, 2008.

[SS01] Bernhard Schölkopf und Alexander J. Smola. *Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond.* MIT Press, 2001.

[VS77] V. Vapnik und A. Sterin. On structural risk minimization or overall risk in a problem of pattern recognition. *Automation and Remote Control*, 10(3):1495–1503, 1977.

[XNLS05] Linli Xu, James Neufeld, Bryce Larson und Dale Schuurmans. Maximum margin clustering. In *Adv. in Neural Inf. Proc. Systems 17*, Seiten 1537–1544, 2005.

[YAAA00] Donald G. York, J. Adelman, John E. Anderson und Scott F. Anderson. The Sloan Digital Sky Survey: Technical Summary. *The Astron. Journal*, 120(3):1579–1587, 2000.



Fabian Gieseke wurde am 4. April 1981 in Emsdetten, Deutschland, geboren. Er erhielt seine Diplome in Mathematik und Informatik von der Westfälischen Wilhelms-Universität Münster und den Doktor der Naturwissenschaften von der Carl von Ossietzky Universität Oldenburg. Während seines Promotionsstudiums beschäftige er sich mit den in diesem Beitrag vorgestellten Erweiterungen von Support-Vektor-Maschinen auf unüberwachte und halbüberwachte Lernszenarien, sowie mit Klassifikations- und Regressionsmodellen für konkrete Fragestellungen aus dem Bereich der Astronomie.

Maschinelle Verifikation von parametrisierten Echtzeitsystemen*

Thomas Göthel

Technische Universität Berlin
thomas.goethel@tu-berlin.de

Abstract: Sicherheitskritische Echtzeitsysteme umfassen häufig nicht nur eine statische, sondern eine parametrisierte, beliebig große Anzahl von nebenläufigen Prozessen. Ein Echtzeitbetriebssystem z.B. verwaltet beliebig viele Threads. Solche Systeme enthalten prinzipiell zwei Quellen von Unendlichkeit: Es existieren einerseits unendlich viele Systeminstanzen, die andererseits durch die Betrachtung von Echtzeit jeweils einen unendlich großen Zustandsraum besitzen. Mit formaler Verifikation kann die Korrektheit in allen Systemabläufen nachgewiesen werden. Dies ist jedoch für derartige unendliche Systeme mit komplexen Systemstrukturen automatisch prinzipiell nicht möglich. Bisher fehlt es an maschinellen, teilautomatisierten Verifikationsansätzen, die weiterhin die Korrektheit von Beweisen selbst sicherstellen. Um dies zu ermöglichen, haben wir ein Rahmenwerk entwickelt, das die Verifikation in einem interaktiven Theorembeweiser erlaubt. Dadurch können Teilbeweise automatisiert werden und es wird sichergestellt, dass (möglicherweise kritische) Randfälle nicht übersehen werden können. Um den damit verbundenen interaktiven Verifikationsaufwand zu reduzieren, ermöglichen wir es weiterhin, Systeminstanzen automatisch zu validieren. Damit können eventuelle Gegenbeispiele vor der Verifikation im Theorembeweiser genutzt werden, um das parametrisierte Gesamtsystem entsprechend zu korrigieren.

1 Einleitung

Echtzeitsysteme müssen oftmals in der Lage sein, mit beliebig vielen (nebenläufigen) Komponenten umgehen zu können. Der Scheduler eines Echtzeitbetriebssystem z.B. verwaltet beliebig viele Threads. Solche Systeme fallen in die Klasse der parametrisierten Systeme, bei denen der Parameter der Anzahl der Komponenten darstellt. Deren maschinengestützte Verifikation ist besonders schwierig, da sie im allgemeinen nicht automatisch verifiziert werden können und weiterhin sichergestellt werden muss, dass Beweise für ihre Korrektheit lückenlos sind, d.h. möglicherweise kritische Randfälle nicht übersehen werden. Bisherige Ansätze für die automatische Verifikation spezieller Subklassen von parametrisierten Systemen schränken die Struktur der betrachteten Systeme stark ein, indem z.B. die einzelnen Komponenten selbst nicht von der Anzahl der Komponenten abhängen dürfen (z.B. [GL08]) oder sie können nicht mit Echtzeit umgehen (z.B. [BLW05]). Weiterhin stellen diese Ansätze nicht sicher, dass die Beweise selbst korrekt sind. Bisherige

*Englischer Titel der Dissertation: “Mechanical Verification of Parameterized Real-Time Systems”

Theorembeweiser-basierte Ansätze, die prinzipiell mit unendlichen Systemen umgehen können und die Korrektheit von Beweisen sicherstellen, betrachten entweder keine Echtzeit (z.B. [IR05]) oder stellen sehr eingeschränkte bzw. unvollständige Mechanisierungen dar (z.B. [WWB10]). Bisher fehlt es an Ansätzen für die umfassende und maschinelle Verifikation von parametrisierten Echtzeitsystemen mit komplexen Systemstrukturen.

In [Göt12] präsentieren wir ein Rahmenwerk zur automatischen Validierung und maschinellen, umfassenden und semi-automatischen Verifikation parametrisierter Echtzeitsysteme mit komplexen Systemstrukturen. Den Kern unseres Rahmenwerks bildet der Prozesskalkül Timed CSP, mit dem funktionales und nicht-funktionales (zeitliches) Verhalten von nebenläufigen Systemen modelliert werden kann. Unsere wichtigsten Beiträge sind: Erstens, eine Formalisierung der operationalen Semantik von Timed CSP sowie Bisimulationsäquivalenzen im Theorembeweiser Isabelle/HOL. Bisimulationen eignen sich, um die Konformität zwischen Systemen zu beschreiben und zu verifizieren. Zweitens stellen wir eine in Isabelle/HOL mechanisierte zeitbehaftete Erweiterung der Hennessy-Milner Logik (HML) zur Verfügung, mit der zeitbehaftete Systemanforderungen beschrieben und maschinell verifiziert werden können. Da wir sowohl konformitäts- als auch eigenschaftsbasierte Verifikation unterstützen, ermöglichen wir insbesondere, das Verifikationsproblem in Teilprobleme zu zerlegen, was die Verifikation erheblich vereinfacht. Zusätzlich stellt der Theorembeweiser sicher, dass alle Beweise lückenlos und garantiert korrekt sind. Unser dritter wesentlicher Beitrag ist die Unterstützung des Verifikationsprozesses durch automatische Verifikationswerkzeuge zur Validierung. Dazu integrieren wir Transformationswerkzeuge in unseren Theorembeweiser-Ansatz, mit denen (endliche) Timed CSP Spezifikationen automatisch in einen diskreten Dialekt von CSP und in zeitbehaftete Automaten transformiert werden können. Somit können der Verfeinerungschecker FDR2 und der Model Checker UPPAAL eingesetzt werden, um Systeminstanzen automatisch zu simulieren und zu verifizieren. Dies hat den Vorteil, Designfehler schon vor dem relativ aufwändigen interaktiven Theorembeweisen aufdecken zu können. Wir wenden unser Rahmenwerk auf die Fallstudie des Schedulers eines Echtzeitbetriebssystems an. Damit demonstrieren wir einerseits den Gewinn durch unsere Transformationen von Timed CSP in automatisch analysierbare Sprachen und andererseits die Effektivität unseres Theorembeweiser-Ansatzes zur maschinellen Verifikation parametrisierter Echtzeitsysteme.

2 Integriertes Validierungs- und Verifikations-Rahmenwerk

In diesem Abschnitt präsentieren wir unser Rahmenwerk zur maschinellen Verifikation von parametrisierten Echtzeitsystemen. In [GG10b] haben wir eine frühere Version davon vorgestellt. Wir betrachten insbesondere parametrisierte Echtzeitsysteme, in denen ein ausgezeichneter Kontrollprozess C_n ein Netzwerk von beliebig vielen Netzwerkprozessen $P_{i,n}$ steuert. Das Verhalten sowohl des Kontrollprozesses als auch der einzelnen Netzwerkprozesse können dabei von der Gesamtgröße des Netzwerks n abhängen. Die generelle von uns betrachtete Struktur von parametrisierten Echtzeitsystemen ist:

$$C_n \otimes_0 (P_{1,n} \otimes P_{2,n} \otimes \cdots \otimes P_{n,n})$$

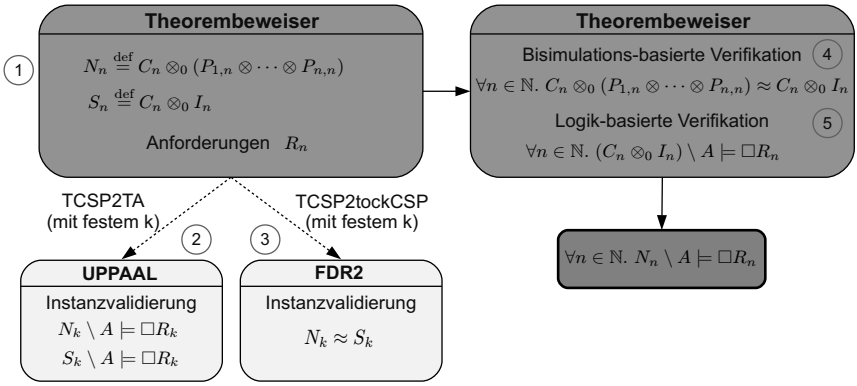


Abbildung 1: Übersicht unsres integrierten Validierungs- und Verifikations-Rahmenwerks

In diesem Kontext ist $\otimes_0$ ein Kompositionsoperator zum Verbinden des Kontrollprozesses mit dem Netzwerk. Dieser Operator beschreibt die Schnittstelle, über die der Kontrollprozess die Netzwerkprozesse steuern kann. Die Netzwerkprozesse werden über einen Kompositionsoperator $\otimes$ verbunden. Mittels dieses Operators wird zum Beispiel der Nachrichtenaustausch zwischen einzelnen Netzwerkprozessen beschrieben.

Unserer Rahmenwerk zielt darauf ab, den Verifikationsprozess für derartige Systeme mit unterschiedlichen Verifikationstechniken und -werkzeugen zu unterstützen. Der wesentliche Ablauf besteht aus einer Modellierungsphase, einer Validierungsphase und schließlich einer (umfassenden) Verifikationsphase. Für die Modellierung von parametrisierten Echtzeitsystemen setzen wir den Prozesskalkül Timed CSP [Sch99] innerhalb des Theorembeweisers Isabelle/HOL [NPW02] ein. Zur Validierung setzen wir die automatischen Verifikationswerkzeuge UPPAAL [BY04] und FDR2 [GRA05] ein. Schließlich führen wir die umfassende Verifikation in Isabelle/HOL durch.

Unser Validierungs- und Verifikationsrahmenwerk ist in Abbildung 1 dargestellt. Die aufeinanderfolgenden Schritte sind durch die Nummerierung gekennzeichnet.

① Ein Entwickler erstellt zunächst eine formale Beschreibung eines konkreten parametrisierten Echtzeitsystems N_n mit einem Netzwerk bestehend aus beliebig vielen Netzwerkprozessen. Weiterhin legt er Anforderungen R_n fest, die alle Instanzen des parametrisierten Systems erfüllen sollen. Um die Verifikation der Anforderungen zu erleichtern bietet unser Rahmenwerk weiterhin die Möglichkeit ein abstraktes parametrisiertes System S_n anzugeben, das zum konkreten Modell konform (im Sinne von *schwacher zeitbehafteter Bisimilarität*) ist. Es dient dazu die parallele Komplexität des konkreten Systems zu reduzieren. Sowohl das konkrete als auch das abstrakte System werden in Timed CSP beschrieben und in unserer Isabelle/HOL Formalisierung mechanisiert. Zur uniformen Beschreibung der Anforderungen bieten wir eine zeitbehaftete Erweiterung von HML an, die wir ebenfalls in Isabelle/HOL mechanisiert haben. Das übergeordnete Verifikationsziel ist, zu zeigen, dass das konkrete parametrisierte Echtzeitsystem mit gegebenenfalls versteckten Ereignissen $N_n \setminus A$ für alle möglichen Netzwerkgrößen die (lokalen) Anforderungen R_n in allen jeweils erreichbaren Zuständen erfüllt ($\Box R_n$).

② Im ersten Validierungsschritt nutzt der Entwickler unsere automatische Transformation *TCSP2TA* von endlichen Timed CSP Prozessen in zeitbehaftete Automaten, um Instanzen des Systems ($N_k \setminus A$ and $S_k \setminus A$) für eine festgelegte Netzwerkgröße k zu übersetzen. Dadurch können diese simuliert und bezüglich der gegebenen Anforderungen unter Verwendung des UPPAAL Model Checkers überprüft werden.

③ Der zweite Validierungsschritt dient der Überprüfung semantischer Konformität zwischen Systeminstanzen N_k und S_k für eine festgelegte Netzwerkgröße k. Dazu transformiert der Entwickler entsprechende Instanzen in eine diskret zeitbehaftete Variante von CSP (tock CSP) mit unserer automatischen Transformation *TCSP2tockCSP*. Unter anschließender Verwendung des Verfeinerungschecker FDR2, kann semantische Konformität bezüglich des timed traces Modells automatisch nachgewiesen werden.

Wenn Checks in einem der beiden Validierungsschritte nicht erfolgreich sind, können generierte Gegenbeispiele von UPPAAL oder FDR2 genutzt werden, um die ursprünglichen parametrisierten Systeme in Timed CSP entsprechend zu korrigieren. Wenn die Checks hingegen erfolgreich sind, besteht eine gute Evidenz dafür, dass das konkrete parametrisierte System sich auch *für alle* Instanzen korrekt verhält. Der formale Nachweis dafür wird in der nachfolgenden umfassenden Verifikationsphase erbracht.

④ Im ersten Verifikationsschritt wird die semantische Konformität *aller* Systeminstanzen N_n und S_n nachgewiesen. Dies geschieht unter Verwendung der Beweistechnik von (schwachen zeitbehafteten) Bisimulationen. Dafür gibt der Entwickler eine entsprechende Bisimulationsrelation an, formalisiert diese in Isabelle/HOL und zeigt mit maschineller Unterstützung, dass die üblichen Beweisverpflichtungen für Bisimulationen erfüllt sind.

⑤ Die zweite Verifikationsschritt besteht darin, maschinell nachzuweisen, dass das abstrakte System $S_n \setminus A$ für alle Instanzen die gegebenen (lokalen) Anforderungen R_n in jeweils allen erreichbaren Zuständen erfüllt. Für diesen Nachweis, gibt der Entwickler, ähnlich wie im Fall der Bisimulationen, eine Invarianzmenge an, die den Initialzustand des Systems beinhaltet. Anschließend wird gezeigt, dass jeder Zustand des Systems die (lokalen) Anforderungen R_n erfüllt. Weiterhin muss nachgewiesen werden, dass jeder Prozess der Invarianzmenge über Schritte der operationalen Semantik von Timed CSP wieder nur Prozesse der Invarianzmenge erreichen kann.

Wir haben maschinell nachgewiesen, dass Formeln unserer zeitbehafteten HML von Bisimulationen bewahrt werden. Dadurch folgt mit den beiden Verifikationsschritten, dass das konkrete parametrisierte Echtzeitsystem $N_n \setminus A$ die Anforderungen in allen erreichbaren Zuständen erfüllt, womit schließlich das übergeordnete Verifikationsziel gezeigt ist.

Die Vorteile unseres Rahmenwerks sind, dass konformitäts- und eigenschaftsbasierte Korrektheitsaussagen maschinell im Theorembeweiser nachgewiesen werden können. Dadurch wird sichergestellt, dass möglicherweise kritische Randfälle bei der Verifikation der betrachteten parametrisierten Echtzeitsysteme nicht übersehen werden können. Weiterhin können Teilbeweise durch die Benutzung von Taktiken in Isabelle automatisiert werden. Da das maschinelle Beweisen in einem interaktiven Theorembeweiser jedoch trotzdem relativ zeitaufwendig ist, setzen wir automatische Verifikationwerkzeuge zur Validierung ein. Dies ermöglicht das Aufdecken und Beheben von möglichen Design-Fehlern *vor* der nachfolgenden umfassenden Verifikationsphase im Theorembeweiser.

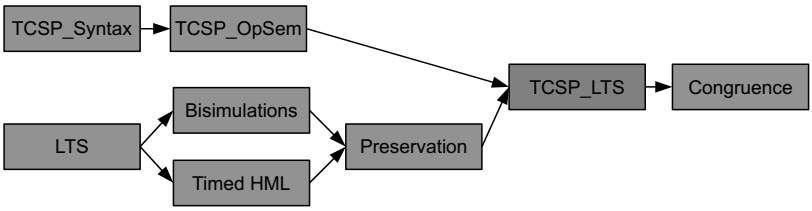


Abbildung 2: Abhängigkeiten zwischen unseren Isabelle-Theorien

3 Mechanisierung in Isabelle/HOL

Im folgenden geben wir einen Überblick unserer Formalisierungen von Timed CSP, einer zeitbehafteten HML und Bisimulationen im Theorembeweiser Isabelle/HOL. Auf dieser Grundlage ist es möglich, (parametrisierte) Echtzeitsysteme in einer mechanisierten Umgebung zu beschreiben sowie Eigenschaften und die semantische Konformität kompositional mit maschineller Unterstützung nachzuweisen. Teile unserer Formalisierungen haben wir in [GG10a] vorgestellt.

In Abbildung 2 zeigen wir die Abhängigkeiten zwischen unseren Isabelle-Theorien. Unabhängig voneinander haben wir zum einen Timed CSP und zum anderen die zeitbehaftete HML sowie Bisimulationen formalisiert und jeweils grundlegende Eigenschaften nachgewiesen. Die Theorie *LTS* definiert den grundlegenden Begriff der zeitbehafteten beschrifteten Transitionssysteme, die im wesentlichen einen Zustandsraum sowie diskrete und zeitbehaftete Transitionen zwischen Zuständen umfassen. Auf dieser Ebene haben wir gezeigt, dass Formeln in unserer zeitbehafteten HML von Bisimulationen bewahrt werden. Durch den anschließenden Nachweis, dass (die operationale Semantik von) Timed CSP als zeitbehaftetes beschriftetes Transitionssystem interpretiert werden kann, werden alle Theorien und Eigenschaften auf den Kontext von Timed CSP übertragen. Schließlich haben wir gezeigt, dass die von uns betrachteten Ausprägungen von Bisimulationen Kongruenzrelationen sind, was die kompositionale Verifikation von Timed CSP Prozessen ermöglicht.

Für den Aufbau der Isabelle/HOL Theorien haben wir das Konzept der *Locales* verwendet. Dies hat den wesentlichen Vorteil, dass die Teiltheorien hochgradig wiederverwendbar sind. Zum Beispiel wäre es möglich unsere Formalisierungen von Bisimulationen und der zeitbehafteten HML für andere Prozesssprachen neben Timed CSP wiederzuverwenden.

3.1 Timed CSP

Timed CSP ist eine Erweiterung des Prozesskalküls CSP [Sch99]. Zur Beschreibung von Echtzeitsystemen wurden zeitbehaftete Operatoren definiert und mit einer kontinuierlichen zeitbehafteten Semantik versehen. Timed CSP eignet sich, um möglicherweise unendliche Systeme kompositional zu beschreiben und zu verifizieren. Der Fokus liegt auf der Interaktion von nebenläufigen Prozessen, die über Nachrichten miteinander kommunizieren.

```
inductive_set evstep :: (('v,'a)Process , 'a eventplus)lts
  ...
| Hiding_step1: ⟦ (P , ev a , P') ∈ evstep ; a∈A ; a∈obs ⟧
                ⟹ (P\A , τ_a , P'\A) ∈ evstep
| Hiding_step2: ⟦ (P , ev a , P') ∈ evstep ; a∈A ; a∉obs ⟧
                ⟹ (P\A , τ , P'\A) ∈ evstep
| Hiding_step3: ⟦ (P , ev a , P') ∈ evstep ; a∉A ⟧
                ⟹ (P\A , ev a , P'\A) ∈ evstep
| Hiding_step4: ⟦ (P , e , P') ∈ evstep ; e=√ ∨ internal e ⟧
                ⟹ (P\A , e , P'\A) ∈ evstep
  ...

inductive_set tstep :: (('v,'a)Process , 'a eventplus)lts
  ...
| Hiding_step1: ⟦ (P , time t , P') ∈ tstep ;
                 ∀ a∈A. ¬(∃ Q. (P , ev a , Q) ∈ evstep) ⟧
                ⟹ (P\A , time t , P'\A) ∈ tstep
  ...
```

Abbildung 3: Mechanisierung der Operationalen Semantik von Timed CSP (Auszug)

Syntax Wir repräsentieren die abstrakte Syntax von Timed CSP mit Hilfe eines Isabelle-Datentyps. Weiterhin nutzen wir die Möglichkeit, konkrete Syntax für Prozessterme anzugeben. Damit ist es nicht nur möglich Prozesse formal zu erfassen, sondern diese auch annähernd wie in der Timed CSP Literatur innerhalb von Isabelle darzustellen.

Semantik In der ursprünglichen operationalen Semantik von Timed CSP haben lediglich interne τ Ereignisse, die für umgebende Prozesse unsichtbar und damit nicht beeinflussbar sind, Priorität über zeitbehafteten Schritten. Dies hat zur Konsequenz, dass sichtbare Ereignisse bis zum nächsten möglichen internen Schritt zeitlich verzögert werden können. Um geschlossene Systeme zu modellieren wird der *Hiding* Operator verwendet, was bedeutet dass alle versteckten Ereignisse nun nicht mehr von einer Umgebung beeinflusst und demnach auch nicht mehr zeitlich verzögert werden können. Konsequenterweise sind versteckte Ereignisse nach außen nicht mehr sichtbar und werden in der Semantik in τ Ereignisse transformiert. Das Problem mit dieser Behandlung ist jedoch, dass das interne Verhalten von Prozessen nicht analysiert werden kann, da die operationale Semantik lediglich ununterscheidbare τ Ereignisse nach außen propagiert.

Um auch das interne Verhalten analysierbar zu machen, haben wir die Semantik leicht angepasst, indem *Hiding* zwar weiterhin interne Ereignisse nicht-verzögerbar macht, aber diese zum Teil über die operationale Semantik unterscheidbar gemacht werden. Um dies zu erreichen parametrisieren wir die operationale Semantik mit einer globale Menge obs von sichtbaren Ereignissen, die sichtbar bleiben selbst nachdem sie versteckt wurden. Der Vorteil ist, dass das Transitionssystem der ursprünglichen Semantik im wesentlichen erhalten bleibt. Lediglich originale τ Kanten werden gegebenenfalls durch τ_a ersetzt. Im Falle, dass $obs = \emptyset$ sind beide Transitionssysteme sogar identisch. Diese Art der konservativen Erweiterung, erlaubt es die komfortablen kompositionalen Eigenschaften von Timed CSP zu erhalten.

Zur Formalisierung der angepassten operationalen Semantik in Isabelle/HOL nutzen wir induktive Mengendefinitionen für diskrete Ereignisschritte und kontinuierliche zeitbehaftete Schritte. Wir zeigen exemplarisch die semantischen Regeln für *Hiding* in Abbildung 3. Die vollständige operationale Semantik ist die Vereinigung von Ereignisschritten und zeitbehafteten Schritten. Sie beschreibt ein zeitbehaftetes beschriftetes Transitionssystem, auf dem wir grundlegende Eigenschaften von Timed CSP maschinell nachgewiesen haben.

3.2 Zeitbehaftete Hennessy-Milner Logik

Mit Hennessy-Milner Logik [HM80] können Eigenschaften von Zuständen (auch Prozesse genannt) in beschrifteten Transitionssystemen beschrieben werden. Um über Echtzeitsysteme argumentieren zu können, haben wir eine zeitbehaftete HML basierend auf zeitbehafteten beschrifteten Transitionssystemen entwickelt und in Isabelle/HOL mechanisiert.

Im folgenden sei p ein Prädikat auf zeitbehafteten Ereignissen (t, a). Weiterhin schreiben wir $(t, a)_p$, wenn (t, a) das Prädikat p erfüllt. Wir definieren, dass ein Prozess P mit dem zeitbehafteten Ereignis (t, a) den Prozess P'' erreichen kann, wenn P in t Zeiteinheiten zu einem P' übergehen kann und P' mit Ereignis a zu P'' übergehen kann.

Definition[Syntax der zeitbehafteten Hennessy-Milner Logik] Die Formeln unserer zeitbehafteten HML sind wie folgt rekursiv definiert: $\phi := tt \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \langle\langle p \rangle\rangle\phi \mid [[p]]\phi$

Die Semantik der letzten beiden Operatoren ist am interessantesten: $P \models \langle\langle p \rangle\rangle\phi$ ist erfüllt, wenn ein zeitbehaftetes Ereignis $(t, a)_p$ existiert, so dass P mit $(t, a)_p$ einen Prozess P'' erreichen kann und P'' die Formel ϕ erfüllt. $P \models [[p]]\phi$ ist erfüllt, wenn *alle* Prozesse P'', die von P mit einem zeitbehafteten Ereignis $(t, a)_p$ erreicht werden können, ϕ erfüllen. Über abgeleitete Operatoren können Formeln wie z.B. $[[a]]_{\leq t} ff$ beschrieben werden, die ausdrückt, dass a nicht innerhalb der nächsten t Zeiteinheiten kommuniziert werden kann.

3.3 Bisimulationen

Bisimulationen eignen sich zur Beschreibung und Verifikation semantischer Konformität zwischen Prozessen. Im wesentlichen sind zwei Prozesse bisimilar, wenn sie ihre beschrifteten Transitionen gegenseitig nachahmen können und dabei jeweils wieder bisimilare Prozesse erreichen. Wir haben Bisimulationen abstrakt definiert und erhalten verschiedene Ausprägungen (stark, schwach, schwach zeitbehaftet) durch jeweilige Instantiierung. Eigenschaften auf der abstrakten Ebene, wie Reflexivität, Symmetrie und Transitivität, werden dadurch vererbt und müssen nicht jeweils erneut bewiesen werden. Damit ist unsere Bisimulationstheorie sehr modular aufgebaut und dadurch äußerst wiederverwendbar.

Unsere Mechanisierungen erlauben es parametrisierte Echtzeitsysteme interaktiv und kompositional im Theorembeweiser zu verifizieren. Wenn Design-Fehler jedoch erst spät im Beweis gefunden werden, muss dieser u.U. komplett überarbeitet werden. Um diese Gefahr zu reduzieren, integrieren wir automatische Beweiswerkzeuge in unser Rahmenwerk.

4 Automatische Validierung

Um automatische Simulations- und Verifikationswerkzeuge wie UPPAAL [BY04] und FDR2 [GRA05] nutzbar zu machen, haben wir Transformationen von Timed CSP in zeitbehaftete Automaten und nach tock CSP entwickelt. Diese Transformationsansätze basieren auf den Arbeiten aus [DHQ+08] und [Oua01]. Da diese Ansätze jedoch nicht alle Timed CSP Operatoren unterstützen und zum Teil die Semantik von Timed CSP inkorrekt behandeln, haben wir diese korrigiert, adaptiert, erweitert und schließlich implementiert. Weiterhin haben wir gezeigt, wie typische Eigenschaften in unserer zeitbehafteten HML in UPPAAL codiert werden können.

Wir verwenden den Echtzeit-Model Checker UPPAAL, um Eigenschaften automatisch auf Instanzen der gegebenen parametrisierten Echtzeitsysteme nachzuweisen. Um die Konformität zwischen Instanzen des konkreten und abstrakten parametrisierten Systems automatisch nachzuweisen verwenden wir den FDR2 Verfeinerungschecker, der über Möglichkeiten verfügt, interne τ Ereignisse gegenüber $tock$ Ereignisse zu priorisieren, um die Semantik von Timed CSP korrekt zu berücksichtigen (interne Ereignisse können nicht verzögert werden). Damit bieten wir die Möglichkeit, beide Verifikationsschritte in unserem Rahmenwerk durch die Verwendung automatischer Verifikationswerkzeuge vorzubereiten.

5 Fallstudie: Verifikation eines Echtzeitbetriebssystem-Schedulers

Um die Anwendbarkeit unseres Rahmenwerks nachzuweisen, haben wir die Fallstudie des Echtzeitbetriebsystem-Schedulers von BOSS [MBK06] betrachtet. Dieser Scheduler kann beliebig viele Threads verwalten und ist somit ein parametrisiertes Echtzeitsystem in unserem Sinn. Wir haben eine vereinfachtes Modell davon in Timed CSP entwickelt, das einen prioritäts- und rundenbasierten präemptiven Scheduler realisiert. Weiterhin nutzen wir die Eigenschaft aus, dass maximal ein Thread zu einem bestimmten Zeitpunkt aktiv sein kann. Dies hat es uns ermöglicht, ein zusätzliches abstraktes Modell zu entwickeln, in dem das konkrete Netzwerk von Threads durch einen sequentiellen Prozess dargestellt wird und somit die parallele Komplexität deutlich reduziert ist. Die Anforderungen, die wir exemplarisch betrachtet haben sind, dass ein Thread weder zu kurz noch zu lang die Kontrolle erhält und dass der Scheduler die Prioritäten der Threads korrekt berücksichtigt.

Zunächst haben wir relativ kleine Instanzen des Systems automatisch mit UPPAAL und FDR2 validiert. Dabei sind uns bei der Entwicklung z.B. kleinere Fehler in unserem Modell bezüglich der inkorrekten Behandlung von Prioritäten aufgefallen, die wir mit Hilfe der generierten Gegenbeispiele simulieren, analysieren und entsprechend beheben konnten. In der anschließenden umfassenden Verifikationsphase in Isabelle/HOL haben wir über Konformitätsverifikation sowie Eigenschaftsverifikation schließlich gezeigt, dass das konkrete Scheduler-Modell die gegebenen Anforderungen erfüllt. Die interaktive Beweiserstellung hat ca. 35 Stunden in Anspruch genommen. Wir sind uns jedoch sicher, dass dieser Verifikationsaufwand deutlich höher ausgefallen wäre, wenn die vorherige Validierungsphase nicht gegeben gewesen wäre.

6 Fazit und Ausblick

In dieser Arbeit haben wir einen integrierten Valdierungs- und maschinellen Verifikationsansatz für parametrisierte Echtzeitsysteme entwickelt. Damit ist es möglich, unendliche Echtzeitsysteme maschinell im Theorembeweiser Isabelle/HOL zu verifizieren und somit auszuschließen dass Randfälle übersehen werden können. Dabei unterstützen wir sowohl eigenschaftsbasierte Verifikation mittels unserer zeitbehafteten HML sowie konformitätsbasierte Verifikation mittels verschiedener Ausprägungen von Bisimulationen. Die unterliegenden Isabelle-Theorien sind möglichst generisch gehalten, um unsere Beiträge z.B. auch für andere Prozesssprachen verfügbar zu machen. Weiterhin können vor der relativ aufwendigen interaktiven Verifikation im Theorembeweiser Instanzen validiert werden, um den maschinellen Verifikationsaufwand möglichst gering zu halten. Dazu stellen wir Transformationen von Timed CSP in zeitbehaftete Automaten und nach tock CSP zur Verfügung, um automatische Verifikationswerkzeuge wie z.B. UPPAAL und FDR2 nutzbar zu machen. Damit stellen wir also einen umfassenden maschinellen Verifikationsansatz sowie einen integrierten Validierungsansatz für unendliche Echtzeitsysteme bereit.

In weiterführenden Arbeiten wollen wir unseren Ansatz auf weitere Fallstudien wie z.B. Bussysteme und Multicore-Architekturen anwenden. Weiterhin wäre es interessant zu untersuchen, inwieweit sich unsere Isabelle/HOL-Mechanisierungen und unsere Transformationsansätze auf andere Prozesssprachen wie Timed CCS übertragen lassen. Um schwächere Konfomitätsbegriffe zu betrachten, könnten Bisimulationen durch z.B. Verfeinerungsbegriffe ersetzt werden und untersucht werden, welche Anteile unseres Rahmenwerks wie übernommen werden können bzw. geändert werden müssen. Schließlich wäre es interessant zu untersuchen, wie automatische Verifikationsergebnisse im Theorembeweiser wiederverwendet werden könnten, ohne die Theorembeweiser-Sicherheit zu verlieren. Es wäre z.B. möglich SMT-basierte Techniken für die Verifikation von Teilprozessen einzusetzen und automatisch gefundene Beweise zurück in den Theorembeweiser zu transferieren. Damit wäre es möglich, diese automatisch und maschinell im Theorembeweiser zu prüfen und somit, trotz der Verwendung potentiell unsicherer Implementierungen automatischer Verifikationswerkzeuge, einen lückenlosen maschinellen Beweis zu erhalten.

Literatur

[BLW05] Ahmed Bouajjani, Axel Legay und Pierre Wolper. Handling Liveness Properties in (ω-) Regular Model Checking. *Electronic Notes in Theoretical Computer Science*, 138:101–115, 2005.

[BY04] Johan Bengtsson und Wang Yi. Timed Automata: Semantics, Algorithms and Tools. In *Lectures on Concurrency and Preti Nets*, Seiten 87–124. Springer, 2004.

[DHQ+08] Jin Song Dong, Ping Hao, Shengchao Qin, Jun Sun und Wang Yi. Timed Automata Patterns. *IEEE Transactions on Software Engineering*, 34:844–859, 2008.

[GG10a] Thomas Göthel und Sabine Glesner. An Approach for Machine-Assisted Verification of Timed CSP Specifications. *Innovations in Systems and Software Engineering - A NASA Journal*, 7:181–193, 2010.

[GG10b] Thomas Göthel und Sabine Glesner. Towards the Semi-Automatic Verification of Parameterized Real-Time Systems using Network Invariants. In *Proceedings of the 8th IEEE International Conference on Software Engineering and Formal Methods*, Seiten 310–314. IEEE Computer Society, 2010.

[GL08] Olga Grinchtein und Martin Leucker. Network Invariants for Real-Time Systems. *Formal Aspects of Computing*, 20(6):619–635, 2008.

[Göt12] Thomas Göthel. *Mechanical Verification of Parameterized Real-Time Systems*. Dissertation, Technische Universität Berlin, 2012.

[GRA05] Michael Goldsmith, Bill Roscoe und Philip Armstrong. Failures-Divergence Refinement - FDR2 User Manual, 2005.

[HM80] Matthew Hennessy und Robin Milner. On Observing Nondeterminism and Concurrency. In *Proceedings of the 7th Colloquium on Automata, Languages and Programming (ICALP)*, Seiten 299–309. Springer, 1980.

[IR05] Yoshinao Isobe und Markus Roggenbach. A Generic Theorem Prover of CSP Refinement. In *Proceedings of the 11th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, Seiten 108–123. Springer, 2005.

[MBK06] S. Montenegro, K. Briess und H. Kayal. Dependable Software (BOSS) for the BEESAT Pico Satellite. In *DASIA 2006*, Data Systems In Aerospace - DASIA 2006, May 2006, Berlin. ESTEC, 2006.

[NPW02] Tobias Nipkow, Lawrence C. Paulson und Markus Wenzel. *Isabelle/HOL — A Proof Assistant for Higher-Order Logic*, Jgg. 2283 of *LNCS*. Springer, 2002.

[Oua01] Joël Ouaknine. *Discrete Analysis of Continuous Behaviour in Real-Time Concurrent Systems*. Dissertation, Oxford University, 2001.

[Sch99] Steve Schneider. *Concurrent and Real Time Systems: The CSP Approach*. John Wiley & Sons, Inc., New York, NY, USA, 1999.

[WWB10] Kun Wei, Jim Woodcock und Alan Burns. Embedding the Timed Circus in PVS. Bericht, University of York, 2010.



Thomas Göthel wurde am 09. Februar 1984 in Radebeul geboren. Von 2002 bis 2007 studierte er Informatik an der Technischen Universität Berlin und schloss sein Studium „mit Auszeichnung“ ab. Im Anschluss arbeitete er als wissenschaftlicher Mitarbeiter im DFG-geförderten Projekt VATES (Verification and Transformation of Embedded Systems) und betreute Lehrveranstaltungen im Bachelor- und im Master-Studium der Informatik. Seine Promotion zum „Doktor der Ingenieurwissenschaften“ schloss er 2012 am Fachgebiet „Programmierung eingebetteter Systeme“ der Technischen Universität Berlin „mit Auszeichnung“ ab. Seine Forschungsinteressen liegen u.a. auf den Gebieten der formalen maschinellen Verifikation, der Echtzeitsysteme und der Kombination von automatischen und interaktiven Verifikationstechniken. Seit seiner Promotion arbeitet er als Postdoktorand am Fachgebiet „Programmierung eingebetteter Systeme“. Seit Mai 2013 forscht er, gefördert durch ein DAAD-Stipendium, am Department of Computer Science an der University of Oxford.

Analyse von Zeitreihen unter Verwendung orthogonaler Polynome am Beispiel der Online-Motivsuche und ihrer Anwendungen

Thiemo Gruber

Universität Kassel
Fachbereich Elektrotechnik/Informatik
Fachgebiet Intelligente Eingebettete Systeme
gruber@uni-kassel.de

Abstract: Die Analyse von Zeitreihen umfasst ein weites Spektrum an Zielsetzungen wie etwa die Zuordnung zu bereits bekannten Gruppen, die Suche nach einem enthaltenen und vorab festgelegten Muster oder die Erkennung neuer und bisher unbekannter Verläufe. Aufgrund der immer stärker zunehmenden Datenmengen sind insbesondere Effizienz und Geschwindigkeit der dabei eingesetzten Verfahren von zentraler Bedeutung. Bei einer Online-Analyse besteht die Herausforderung speziell in der Notwendigkeit, zu jedem Zeitpunkt eine Entscheidung treffen zu können, auch wenn die zu verarbeitenden Daten noch nicht vollständig vorliegen. Durch eine Ermittlung ähnlich wiederkehrender charakteristischer Abschnitte, sogenannter Motive, und die Überprüfung ihrer An- oder Abwesenheit in gegebenen Zeitreihen ist eine Vielzahl von Problemstellungen adressierbar. In der diesem Beitrag zugrundeliegenden Dissertation werden neuartige Lösungsansätze für alle notwendigen Schritte einer Online-Motivsuche basierend auf einer Approximation der Zeitreihen mit orthogonalen Polynomen vorgestellt. Die Besonderheit in der Verwendung orthogonaler Polynome besteht dabei in der Möglichkeit der Anwendung sehr schneller Approximationsverfahren sowie der besonderen Interpretierbarkeit der ermittelten Ergebnisse.

1 Problemstellung

Eine wichtige Eigenschaft vieler Daten ist zeitliche Information. Insbesondere in Form von *Zeitreihen*, bei denen die Zeitkomponente eine Totalordnung der Elemente definiert, sind diese Daten in einer Vielzahl von Anwendungen zu finden. Einige typische Beispiele hierfür sind EKG (Elektrokardiogramm) und EEG (Elektroenzephalogramm) aus den Bereichen der Medizin bzw. der Biometrie, Temperaturkurven und Windgeschwindigkeiten aus dem Gebiet der Meteorologie, Börsenkurse in der Finanzwirtschaft, akustische Signale wie Musik oder Sprache sowie technische Sensorzeitreihen aus den Gebieten der Robotik oder der Prozessüberwachung. Durch das sog. *Ubiquitous Computing* und die damit immer stärker wachsende Anzahl an eingebetteten Systemen, beispielsweise in Mobiltelefonen, Fahrzeugen, Geräten der Unterhaltungselektronik oder Kleidung, sowie dem damit

verbundenen ansteigenden Einsatz von Sensoren ergeben sich fortlaufend neue Anwendungsfelder. Mögliche Analyseziele sind dabei die Erkennung von bestimmten Zeitpunkten oder Zeitabschnitten, die Ermittlung von Übereinstimmungen mit anderen Signalen oder Signalabschnitten, die Vorhersage der weiteren Entwicklung eines Signalverlaufs oder die Erkennung von Anomalien oder Unregelmäßigkeiten. So sind zum Beispiel die Erkennung von Störungen im Signalverlauf eines EKG, die Vorhersage von Windgeschwindigkeiten oder Börsenkursen oder die Erkennung von Sprache oder des Genres eines Musikstücks typische Aufgabenstellungen. Für eine ausführlichere Betrachtung der unterschiedlichen Aspekte des sog. *Temporal Data Mining* sowie möglicher Herausforderungen und Lösungsansätze sei beispielsweise auf [LS06] verwiesen.

Neben den grundlegenden Eigenschaften der Daten muss bei der Analyse von Zeitreihen einigen Besonderheiten geeignet Rechnung getragen werden. Hierzu zählen verschiedene Komponenten, aus denen sich die jeweilige Zeitreihe zusammensetzt, die häufig in zyklische oder saisonale Anteile, Trendkomponenten sowie zufällige Einflüsse wie Signalrauschen oder Messfehler unterteilt werden. Eine weitere Besonderheit vieler Zeitreihen ist die Tatsache, dass sie sehr viel überflüssige Information enthalten. Je nach Anwendung ist damit der Anteil einer Zeitreihe, in dem die notwendige Information, die für die Erledigung einer bestimmten Aufgabe nötig ist, in wenigen, meist kurzen Abschnitten zu finden und von etlichen, teilweise deutlich längeren Abschnitten ohne signifikante Information durchzogen.

Die besondere Herausforderung der *Online-Zeitreihenanalyse* besteht in der Tatsache, dass zu Beginn des Vorgangs nicht alle Daten verfügbar sind, sondern diese kontinuierlich bereitgestellt werden. Dies ist insbesondere dann der Fall, wenn die Gewinnung der Daten zum Zeitpunkt der Analyse noch nicht abgeschlossen ist. Trotz der damit unter Umständen sehr eingeschränkten Sichtweise auf die Daten muss zu jedem Zeitpunkt eine Entscheidung getroffen werden können. Häufig werden zusätzliche Anforderungen hinsichtlich des verfügbaren Speicherplatzes sowie bezüglich der maximal erlaubten Rechenschritte oder Rechenzeit je Aktualisierungs- oder Entscheidungsschritt an die eingesetzten Verfahren gestellt. Typische Beispiele sind die Online-Überwachung eines EKG-Signals mittels eines portablen Systems, der Spurhalteassistent in Form eines eingebetteten Echtzeitsystems in einem Fahrzeug oder die Überwachung und Steuerung industrieller Fertigungsprozesse.

Eine zentrale Aufgabe der Zeitreihenanalyse ist es, ähnlich wiederkehrende Sequenzen oder charakteristische Abschnitte, sog. *Motive*, zu finden und deren An- oder Abwesenheit in unbekannten Zeitreihen oder Abschnitten zu prüfen. Im Wesentlichen entsprechen Zeitreihenmotive damit den aus der Musik bekannten Motiven und ihren in der Bioinformatik oder Genetik gebräuchlichen, diskreten Gegenstücken auf DNS- oder RNS-Sequenzen. Das Problem der Motivsuche wird dabei mit unterschiedlichen Techniken adressiert, wobei Motive unter verschiedenen Begriffen wie „zeitliches Muster“, „Episode“ oder „Subsequenz“ bekannt sind. Allen Ansätzen gemeinsam ist jedoch der Versuch, durch die Bestimmung des Vorhandenseins oder Fehlens eines oder mehrerer Motive in einer Zeitreihe oder einem Zeitreihenabschnitt, Aussagen über die Zeitreihe, ihren weiteren Verlauf, die Zugehörigkeit zu einer bekannten Gruppe oder Zusammenhänge zwischen verschiedenen Zeitreihen zu treffen. Diese Darstellung einer Zeitreihe über charakteristische Anteile ist eng mit dem Ziel vieler Datenverarbeitungsverfahren verwandt, redundante und überflüssige Informationen aus Daten zu entfernen und nur die signifikanten Anteile weiterzuverarbeiten.

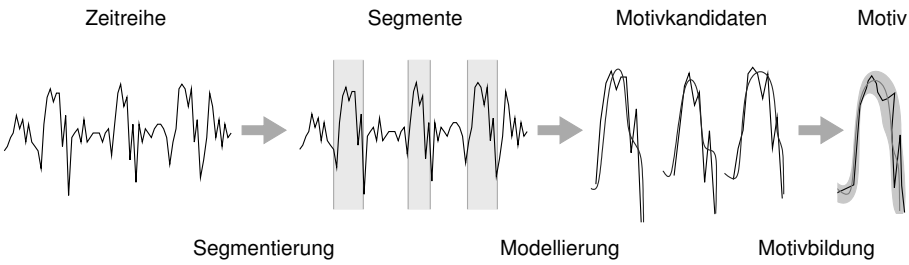


Abbildung 1: Grundlegender Ablauf der Motivdefinition durch Segmentierung der Trainingszeitreihe, Auswahl geeigneter Motivkandidaten, hier anhand von Zusatzinformationen in Form von Labels, gefolgt von deren Modellierung und der Motivbildung, hier durch Überlagerung, zu einem Zeitreihenmotiv.

Die Online-Motivsuche gliedert sich in zwei wesentliche Phasen. Grundlegendes Ziel der ersten Phase, der sog. *Motivdefinition*, ist die Gewinnung eines Motivs aus Beispieldaten, wobei zwischen überwachter und unüberwachter Motivdefinition unterschieden werden kann. Im Fall der überwachten Motivdefinition sind die zu betrachtenden Abschnitte und damit die Positionen für eine sinnvolle Segmentierung der Beispielzeitreihen durch Zusatzinformationen wie Labels vorgegeben, während diese bei einer unüberwachten Motivdefinition, beispielsweise durch die Bestimmung häufig wiederkehrender Teilsequenzen, ausschließlich aus Beispieldaten gewonnen werden müssen. Nach der Bestimmung relevanter Abschnitte, sog. *Motivkandidaten*, aus denen ein Motiv gebildet werden kann, müssen diese geeignet weiterverarbeitet werden, um möglichst viel der Information zu erfassen, die in allen Beispielen zusammen vorhanden ist. Hierzu werden die Abschnitte zunächst geeignet modelliert und anschließend entsprechend selektiert oder überlagert, um die Bildung eines Motivs für die gewählten wiederkehrenden und charakteristischen Abschnitte zu ermöglichen. Je nach Überlagerungs- oder Auswahlmethode gehört dazu ebenfalls die Definition eines geeigneten Ähnlichkeitsbegriffs auf den Zeitreihenmodellen. Zur Verdeutlichung sind in Abbildung 1 die grundlegenden Schritte der Motivdefinition zusammen mit den jeweiligen Zwischenergebnissen dargestellt.

In der zweiten Phase, der eigentlichen *Motivsuche*, besteht die Aufgabe anschließend darin, in einer zuvor unbekannten Zeitreihe Abschnitte zu identifizieren, die dem gegebenen Motiv entsprechen, d. h. ihm ausreichend ähnlich sind. Um das definierte Motiv suchen zu können, muss daher zunächst ein geeigneter Ähnlichkeitsbegriff zwischen dem Zeitreihenmotiv und den zu überprüfenden Abschnitten bzw. ihren Modellen gewählt werden. Für die eigentliche Bestimmung ähnlicher Abschnitte wird die zu durchsuchende Zeitreihe analog zur ersten Phase segmentiert, die resultierenden Segmente werden anschließend modelliert und mit dem Motiv unter Verwendung des gewählten Ähnlichkeitsmaßes abgeglichen. Liegt die ermittelte Ähnlichkeit dabei beispielsweise oberhalb eines festgesetzten Schwellwerts oder entspricht die Übereinstimmung den aus Trainingsdaten für Positivbeispiele bekannten Werten, ist das Motiv an der entsprechenden Stelle in der Testzeitreihe vorhanden. Abbildung 2 veranschaulicht die notwendigen Schritte der Motivsuche.

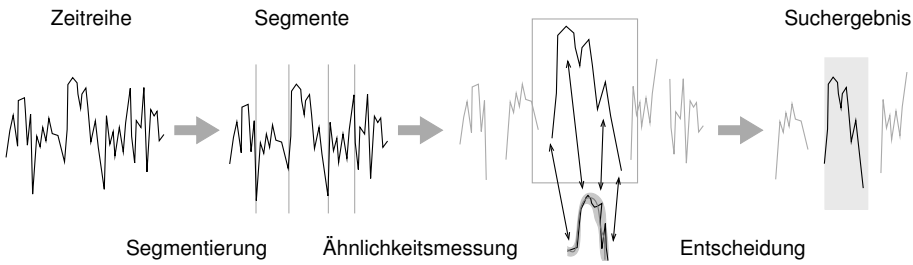


Abbildung 2: Grundlegender Ablauf der Motivsuche durch Segmentierung der Testzeitreihe, Ähnlichkeitsbestimmung zwischen den entstehenden Segmenten und dem gegebenen Zeitreihenmotiv, gefolgt von einer auf den ermittelten Werten basierenden Entscheidung über eine An- oder Abwesenheit des gesuchten Motivs an der entsprechenden Position.

2 Lösungsansatz

In den Phasen Motivdefinition und -suche sind insgesamt vier wesentliche Aufgaben zu erledigen, die im Folgenden zusammen mit den entwickelten Lösungsansätzen, welche die jeweiligen Herausforderungen geeignet adressieren, erläutert werden (siehe auch Abbildung 3). Einen zentralen Bestandteil bilden dabei sog. *diskrete orthogonale Polynome*. Diese bestehen aus einer Folge von Polynomen, die bezüglich eines gegebenen Skalarprodukts an diskreten Positionen, den sog. *Stützstellen*, orthogonal sind. Ein derartiges diskretes *orthogonales Polynomsystem* besitzt einige positive Eigenschaften, die bei der Online-Verarbeitung und -Analyse von Zeitreihen ausgenutzt werden können.

Repräsentation: Die direkte Verarbeitung von Zeitreihen anhand ihrer Rohdaten weist etliche Nachteile auf. Neben den schwierigen und meist nur rechenintensiv realisierbaren Vergleichen verschieden langer oder unterschiedlich abgetasteter Zeitreihen stellt vor allem die niedrige Robustheit gegenüber Störeinflüssen, wie Rauschen oder Ausreißern, ein erhebliches Problem für die weitere Analyse dar. Eine Abstraktion von den Datenwerten, die eine wichtige Voraussetzung für nachfolgende Verarbeitungsschritte darstellt, wird daher unter Verwendung einer Polynomapproximation nach der sog. *Methode der kleinsten Quadrate* (engl. *least squares*) realisiert. Die Repräsentation erfolgt anschließend mit Hilfe der Attribute der ermittelten Lösung, wie beispielsweise den Werten des approximierenden Polynoms, der Polynomkoeffizienten oder des Approximationsfehlers. Die Verwendung einer orthogonalen Polynombasis erlaubt dabei die Verwendung sehr effizienter Verfahren, mit deren Hilfe eine schnelle Berechnung der Approximation sowie ein *Update* der Lösung durch Hinzufügen eines neuen Datenpunkts mit einer konstanten Laufzeitkomplexität möglich ist. Zusätzlich ist über sog. *Orthogonalkoeffizienten* ein getrennter Zugriff auf die in einem Signal enthaltenen Trendanteile wie Durchschnitt, Steigung oder Krümmung möglich, da in einer derartigen Approximation alle Lösungen niedrigeren Grades enthalten sind.

Segmentierung: Eine zentrale Eigenschaft des eingesetzten Segmentierungsverfahrens ist, neben der Fähigkeit, die Eingabedaten online verarbeiten zu können, die Konsistenz der Ergebnisse. Dies bedeutet im Wesentlichen, dass ähnliche Abschnitte in Zeitreihen zu

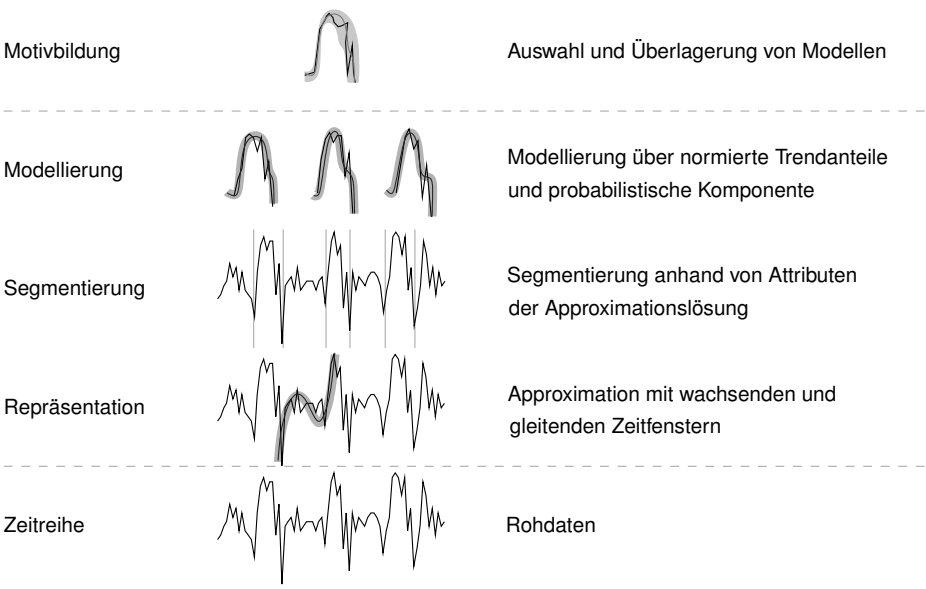


Abbildung 3: Wesentliche Gesichtspunkte der Repräsentation, Segmentierung und Modellierung von Zeitreihen sowie einer anschließenden Motivbildung.

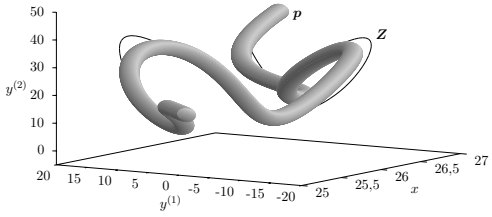
ähnlichen Resultaten der Segmentierung führen, insbesondere wenn diesen unterschiedliche Verläufe vorangehen. Basierend auf der Repräsentation einer gegebenen Zeitreihe unter Verwendung orthogonaler Polynome kann eine entsprechende Segmentierung formuliert werden. Grundidee ist dabei die Betrachtung der Approximation eines bestimmten Abschnitts oder deren Überwachung während einer inkrementellen Entwicklung bzw. eines Updates. Hierbei sind die beiden grundlegenden Sichtweisen eines *gleitenden Zeitfensters* (engl. *sliding window*) und eines *wachsenden Zeitfensters* (engl. *growing window*) möglich. Im Fall eines wachsenden Zeitfensters wird der Approximation in jedem Update-Schritt ein neuer Datenwert hinzugefügt. Bei Verwendung eines gleitenden Zeitfensters wird in jedem Schritt zusätzlich der, bezüglich seiner zeitlichen Position, älteste Datenwert entfernt. Beide Ansätze lassen sich unter Verwendung orthogonaler Polynome mit konstantem Zeitaufwand in jedem Update-Schritt realisieren. Die somit anhand einer fortlaufend aktualisierten Polynomapproximation von prinzipiell beliebigem Grad definierbaren Kriterien ermöglichen nicht nur eine einfache Formulierung der gewünschten Segmentierung, wie beispielsweise an lokalen Minima oder Maxima, sondern sind online und sehr effizient auswertbar.

Modellierung und Ähnlichkeitsmessung: Die Modellierung von Zeitreihen oder einzelnen Abschnitten kann aufbauend auf einer Repräsentation der Rohdaten durch eine Polynomapproximation realisiert werden. Dabei modellieren die Koeffizienten der Linearkombination der Basispolynome den wesentlichen Verlauf der jeweiligen Zeitreihe. Dieser Ansatz wird, vor allem aufgrund seiner kompakten Form, sehr häufig zur Modellierung aufeinanderfolgender Abschnitte einer Zeitreihe verwendet, meist jedoch nur mit sehr niedrigen Graden, was zu einer abschnittsweisen konstanten oder linearen Darstellung führt.

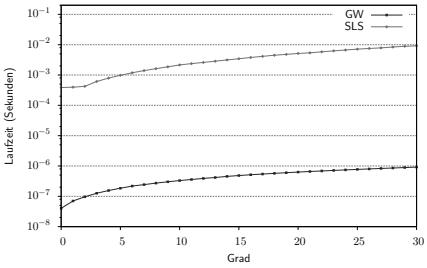
Die Verwendung orthogonaler Polynome hingegen erlaubt die einfache Approximation mit wesentlich höheren Graden, bei der gleichzeitigen Möglichkeit, auf Trendinformationen niedrigerer Grade zuzugreifen. Das Ziel ist dabei, die deterministische Komponente der Zeitreihe durch das Approximationspolynom explizit zu modellieren und die stochastische Komponente des Signals in Form eines probabilistischen Anteils, der auf dem Residuum des Ausgleichsproblems basiert, darzustellen. Aufgrund der linearen Unabhängigkeit der Komponenten der Lösung ist zusätzlich eine Normierung und damit eine Abstraktion von Faktoren wie Skalierungen und Translationen im Zeit- und Wertebereich möglich. Dies unterstützt vor allem die Definition von robusten Ähnlichkeitsmaßen zwischen Modellen, da somit gewährleistet ist, dass ähnliche Signalverläufe, die dadurch vergleichbare Trendanteile besitzen, zu ähnlichen Modellen führen. Werden die entsprechenden Modelle bereits während der Segmentierung mitentwickelt, erlaubt dies die Formulierung komplexerer Kriterien und ermöglicht die Erzeugung von Modellen der ermittelten Segmente ohne zusätzlichen Rechenaufwand direkt im Anschluss an eine Segmentierungsentscheidung.

Motivbildung: Ist eine geeignete Menge von Motivkandidaten ermittelt, können diese zur Definition eines Zeitreihenmotivs verwendet werden. Grundlegende Anforderung ist dabei, sowohl möglichst viel Information der Gesamtheit aller Modelle zu erfassen als auch darin enthaltene Redundanz zu entfernen. Neben der Auswahl geeigneter Repräsentanten ist die Bildung eines Motivs aus mehreren Modellen durch deren Überlagerung möglich. Dabei ist zusätzlich zu einer Verrechnung der bereits vorhandenen Informationen, wie das durchschnittliche Approximationspolynom oder der gemittelte Fehler, auch die Gewinnung neuer Informationen möglich. Hierzu gehört die Definition einer zeitabhängigen Unsicherheit, die analog zum probabilistischen Anteil der Modelle aus der Übereinstimmung bzw. Streuung innerhalb der Menge der Modelle an unterschiedlichen zeitlichen Positionen abgeleitet werden kann. Die Ermittlung von Durchschnitt und Streuung von Attributen, wie zum Beispiel den verschiedenen Trendanteilen, ermöglicht zudem die Bildung multivariater Wahrscheinlichkeitsverteilungen. Darauf aufbauend ist die Definition von Ähnlichkeitsmaßen, beispielsweise zwischen den Durchschnittswerten eines Zeitreihenmotivs und eines Zeitreihenmodells, unter Berücksichtigung der zeitabhängigen Unsicherheit oder die Ermittlung der Likelihood eines Modells bezüglich eines Motivs möglich. Aufgrund der Kompaktheit der Modelle und damit auch eines daraus generierten Motivs sind die so definierten Abstandsmaße größtenteils vom zugrundeliegenden Signal, insbesondere von der Anzahl der Datenwerte, unabhängig und somit sehr effizient auswertbar.

Teile der Dissertation wurden bereits in mehreren Beiträgen zu internationalen Konferenzen und Zeitschriften veröffentlicht. In [FGPS10] wird die Repräsentation von Zeitreihen unter Verwendung orthogonaler Polynome beleuchtet und diese zusammen mit einem darauf basierenden Abstandsmaß am Beispiel einiger Anwendungen untersucht. Hierbei wird insbesondere deutlich, dass aufgrund des enormen Geschwindigkeitsvorteils der Einsatz höherer Polynomgrade und damit eine genauere und robustere Modellierung mit deutlich geringeren Fehlern möglich ist. Die Arbeit [FGNS10] präsentiert die Segmentierung von Zeitreihen basierend auf einer Approximation mit orthogonalen Polynomen, wobei die beiden wesentlichen Sichtweisen der gleitenden und wachsenden Zeitfenster detailliert dargestellt werden. In [FGNS09] wird eine ausführliche Erläuterung der Online-Motivsuche basierend auf der Repräsentation und Segmentierung von Zeitreihen unter Verwendung



(a) Mehrdimensionales Modell $\boldsymbol{p}$ mit aus dem Approximationsfehler abgeleiteter Unsicherheit einer multivariaten Zeitreihe $\boldsymbol{Z}$.



(b) Laufzeit je Datenpunkt des GW-Verfahrens sowie eines Standard-Least-Squares-Ansatzes (SLS).

Abbildung 4: Mehrdimensionales Modell einer Zeitreihe und Geschwindigkeitsvorteil einer inkrementellen Approximation bei dessen Erstellung gegenüber herkömmlichen Ansätzen.

orthogonaler Polynome gegeben. Im Fokus steht hierbei die Modellierung einer Zeitreihe durch gezielte Repräsentation ihrer deterministischen und stochastischen Anteile. Die Einsatzmöglichkeiten der Modellierung von Zeitreihen unter Verwendung orthogonaler Polynome werden in [FGS11] in Kombination mit einem generativen Klassifikator ausführlich am Beispiel der Erzeugung menschenverständlicher Klassifikationsregeln gezeigt. Die Arbeit [BSK+10] präsentiert speziell die Anwendung der Modellierung im Bereich des sog. *Activity Spotting*, dem Auffinden bestimmter Bewegungen oder Bewegungsabläufe einer Person, an deren Körper Sensoren zur Aufzeichnung geeigneter Zeitreihen angebracht sind. Für eine detailliertere Beschreibung der vorgestellten Verfahren sowie weitere Literaturhinweise sei außerdem auf den Gesamttext der Dissertation [Gru12] verwiesen.

3 Ergebnisse

Im Vergleich mit herkömmlichen Approximationsverfahren ergeben sich durch Verwendung orthogonaler Polynome und entsprechender Update-Algorithmen bereits etwa 10^4-fach höhere Geschwindigkeiten einer Approximation in wachsenden und 10^2-fach höhere Geschwindigkeiten in gleitenden Zeitfenstern. Insbesondere in Kombination mit der im Rahmen der Arbeit vorgestellten inkrementellen Entwicklung des Residuums lassen sich alle für eine Modellierung notwendigen Informationen auch für große Datenmengen sehr effizient ermitteln (siehe auch Abbildung 4). Nachteilig an einer inkrementellen Entwicklung der Approximation sind numerische Instabilitäten, die insbesondere bei der Entfernung eines Datenwerts aus einer bestehenden Lösung, etwa beim Verschieben eines gleitenden Zeitfensters, auftreten. Durch geeignetes Zurücksetzen der Approximation in regelmäßigen Abständen ist eine Begrenzung des auftretenden Fehlers und damit eine Verarbeitung beliebig langer Zeitreihen jedoch mit sehr geringem Aufwand möglich.

Die Verwendung normierter, trendbeschreibender Orthogonalkoeffizienten sowie eines probabilistischen Modells erlaubt eine robuste und im Zeit- und Wertebereich translations-

und skalierungsinvariante Verarbeitung von Zeitreihen. Unter Verwendung eines 1NN-Klassifikators, der aufgrund seiner Parameterfreiheit und Robustheit gewählt wurde, zeigt sich auch im Vergleich zum euklidischen Abstand anhand von Auswertungen auf 20 Benchmark-Datensätzen, dass mit den im Rahmen der Arbeit vorgestellten, auf der Modellierung aufbauenden Ähnlichkeitsmaßen sehr gute Ergebnisse erzielt werden können. Eine experimentelle Untersuchung der präsentierten Segmentierungskriterien zeigt insgesamt, dass sich eine sehr vielseitige und auf unterschiedliche Problemstellungen anpassbare Segmentierung realisieren lässt, die herkömmlichen Verfahren in vielen Aspekten überlegen ist. Vor allem die Effizienz bei der Verarbeitung größerer Datenmengen sowie die einfache Formulierbarkeit, auch in Kombination mit komplexeren und über Nebenwissen fest vorgegebenen Segmentgrenzen, werden dabei an etlichen Beispielen deutlich. Aus einer Untersuchung der beschriebenen Ansätze zur Definition von Zeitreihenmotiven sowie der zugehörigen Ähnlichkeitsmaße zeigt sich insbesondere im Vergleich mit einem klassischen Ansatz basierend auf dem euklidischen Abstand deutlich, dass unter Verwendung der auf der Orthogonaldarstellung basierenden *Shape-Space-Sichtweise* sehr gute Ergebnisse erzielt werden können und sich eine probabilistische Formulierung in Kombination mit der Auswertung einer auf der Likelihood von Zeitreihenmodellen basierenden Ähnlichkeitsmessung ebenfalls gut für die Definition und Suche von Motiven eignet. Im direkten Vergleich mit den Klassifikationsergebnissen unter alleiniger Verwendung von Zeitreihenmodellen zeigt sich außerdem, dass sich für etliche Datensätze ein deutlicher Vorteil aus der gemeinsamen Betrachtung der Trainingszeitreihen ergibt.

Die Anwendung der Online-Motivsuche in der Zeitreihenklassifikation zeigt am Beispiel zweier bekannter Datensätze, dass über eine Repräsentation unterschiedlicher Klassen durch ein oder mehrere Zeitreihenmotive auch unter Verwendung eines einfachen Klassifikatorparadigmas wie 1NN sehr gute Ergebnisse erzielt werden können. Auf beiden Datensätzen wurden dabei Klassifikationsraten von über 99% erreicht und die Leistungsfähigkeit des vorgestellten Ansatzes damit auch im Vergleich zu anderen Verfahren bestätigt. Die Suche nach Motiven, die über eine Segmentierung gelabelter Trainingsdaten und eine Überlagerung der gewonnenen Motivkandidaten gebildet wurden, zeigt, dass die vorgestellten Ansätze vergleichbare Verfahren sowohl hinsichtlich der erzielten Ergebnisse als auch bezüglich der dafür notwendigen Rechenzeit deutlich übertreffen können. Auf einem Datensatz aus dem Bereich der Aktivitätserkennung konnten dabei Erkennungsraten von über 96% bei einer personenspezifischen Verarbeitung sowie von knapp 92% auf den Daten vollständig unbekannter Testpersonen erreicht werden. Auf einem weiteren Beispieldatensatz konnte bei einer Suche nach bestimmten Signalverläufen, den sog. *Peaks*, sowohl hinsichtlich der korrekt erkannten Peaks als auch gemessen an den insgesamt korrekt als Peak bzw. als kein Peak erkannten Segmenten jeweils ein Anteil von über 99% erreicht werden. Die Ergebnisse eines bekannten Vergleichsverfahrens lagen hier, trotz einer mehr als zehnfachen Laufzeit, lediglich bei 83% bzw. 97%. Anhand der Erkennung von Anomalien in unbekannten Zeitreihen zeigt sich, dass mit den vorgestellten Ansätzen außerdem eine sehr effiziente Verarbeitung der Daten und gleichzeitig die Ermittlung aussagekräftiger Ergebnisse möglich ist. Am Beispiel einer EKG-Zeitreihe konnte die erfolgreiche Erkennung auffälliger und atypischer Signalverläufe mit einer über 150-fachen Geschwindigkeit gegenüber der tatsächlichen Dauer der Aufnahme durchgeführt werden.

4 Zusammenfassung und Ausblick

Ziel der Arbeit war die Entwicklung und Untersuchung neuartiger Verfahren zur Analyse von Zeitreihen unter Verwendung einer Online-Motivsuche. Alle vorgestellten Ansätze bauen auf einer Approximation der Zeitreihen mit orthogonalen Polynomen und einer Repräsentation mit Hilfe daraus gewonnener Informationen auf. Die wesentlichen innovativen Aspekte der entwickelten Verfahren können dabei wie folgt zusammengefasst werden:

- Eine effiziente Modellierung von Zeitreihen anhand normierter, trendbeschreibender Merkmale, die insbesondere in Kombination mit weiteren Attributen wie dem Approximationsfehler zur Definition eines komplexen Zeitreihenmodells mit einer probabilistischen Komponente und darauf basierenden neuen Abstandsmaßen eingesetzt werden kann.
- Ein generisches Online-Verfahren zur Zeitreihensegmentierung, welches durch die verwendeten Approximationsverfahren eine intuitive Formulierung komplexer Segmentierungskriterien und einen Einsatz unter Echtzeit- und Streaming-Bedingungen erlaubt.
- Die Darstellung einer Menge von Zeitreihenmodellen in Form eines Zeitreihenmotivs mit einer zeitabhängigen Unsicherheit bzw. in Form einer multivariaten Wahrscheinlichkeitsverteilung in Kombination mit zugehörigen Ähnlichkeitsmaßen zur Realisierung einer robusten und, sofern erwünscht, im Zeit- und Wertebereich translations- und skalierungsinvarianten Online-Motivsuche.

Insgesamt konnten aufbauend auf orthogonalen Polynomen und effizienten Update-Algorithmen schnelle und robuste Online-Ansätze zur Analyse von Zeitreihen entwickelt werden. Neben der Echtzeitfähigkeit konnte das Ziel interpretierbarer und damit einfach und flexibel anwendbarer Zwischenschritte erreicht werden. Ein wesentlicher Aspekt der vorgestellten Verfahren ist, dass keine oder nur sehr allgemeine Annahmen über die zu verarbeitenden Signale oder die zugrundeliegenden Prozesse gemacht werden. Neben dem Vorteil einer sehr vielseitigen Einsetzbarkeit ergibt sich daraus jedoch auch ein unmittelbarer Nachteil gegenüber anwendungs- oder problemspezifisch angepassten Ansätzen. So erleichtert die Nutzung von entsprechendem Nebenwissen nicht nur die gezielte Auswahl von Merkmalen, Abstandsmaßen, Verteilungsfunktionen oder Schwellwerten, sondern ermöglicht ein vollständig auf die jeweilige Anwendung oder Zielsetzung angepasstes und optimiertes Vorgehen, die Behandlung von Sonderfällen oder die Erkennung ungültiger Ergebnisse. Auch die reine Online-Eigenschaft der vorgestellten Verfahren kann in Situationen, in denen eine (zumindest teilweise) Offline-Verarbeitung von Zeitreihen oder Abschnitten möglich ist, zu einem entsprechenden Nachteil führen. Zwar besteht, etwa über die Wahl des Polynomgrades, an vielen Stellen die Möglichkeit, in gewissen Grenzen zwischen Genauigkeit und Geschwindigkeit zu wählen, ein global optimales Vorgehen ist aufgrund der bewusst gewählten und sehr beschränkten Sichtweise auf die Daten jedoch grundsätzlich ausgeschlossen.

Die sich unmittelbar ergebenden Möglichkeiten für eine Weiterentwicklung der vorgestellten Verfahren umfassen insbesondere die Integration anwendungs- und problemspezifischer

Komponenten, Merkmale oder Basisfunktionen sowie eine Kombination mit Verfahren, die entsprechend komplementäre Eigenschaften aufweisen. Dies führt auch zu etlichen Möglichkeiten zur Beschleunigung existierender Verfahren wie beispielsweise einer auf dynamischer Programmierung basierenden optimalen Segmentierung oder SWAB (Sliding Window And Bottom-up). Darüber hinaus bietet sich ein Einsatz der vorgestellten Techniken in weiteren Anwendungsgebieten wie Kontrolle und Prognose an, welche neben der Deskription und der Modellierung, die im Rahmen der Arbeit über eine Repräsentation unter Verwendung orthogonaler Polynome sowie die Formulierung entsprechender Zeitreihenmodelle adressiert wurden, zu den vier Hauptanwendungen der Zeitreihenanalyse zählen. Weitere naheliegende Anwendungsbereiche der vorgestellten Techniken sind beispielsweise die komprimierte Verarbeitung und Speicherung sowie eine Indexierung von Zeitreihen.

Literatur

[BSK+10] U. Blanke, B. Schiele, M. Kreil, P. Lukowicz, B. Sick und T. Gruber. All for one or one for all? – Combining Heterogeneous Features for Activity Spotting. In *Proc. of the 7th IEEE PerCom Workshop on Context Modeling and Reasoning*, Seiten 18–24, 2010.

[FGNS09] E. Fuchs, T. Gruber, J. Nitschke und B. Sick. On-line Motif Detection in Time Series with SwiftMotif. *Pattern Recognition*, 42(11):3015–3031, 2009.

[FGNS10] E. Fuchs, T. Gruber, J. Nitschke und B. Sick. Online Segmentation of Time Series Based on Polynomial Least-Squares Approximations. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(12):2232–2245, 2010.

[FGPS10] E. Fuchs, T. Gruber, H. Pree und B. Sick. Temporal Data Mining Using Shape Space Representations of Time Series. *Neurocomputing*, 74(1–3):379–393, 2010.

[FGS11] D. Fisch, T. Gruber und B. Sick. SwiftRule: Mining Comprehensible Classification Rules for Time Series Analysis. *IEEE Transactions on Knowledge and Data Engineering*, 23(5):774–787, 2011.

[Gru12] T. Gruber. *Analyse von Zeitreihen unter Verwendung orthogonaler Polynome am Beispiel der Online-Motivsuche und ihrer Anwendungen*. Dissertation, Fachbereich Elektrotechnik/Informatik, Universität Kassel, Kassel, Deutschland, 2012.

[LS06] S. Laxman und P. S. Sastry. A Survey of Temporal Data Mining. *Sadhana, Academy Proceedings in Engineering Sciences*, 31(2):173–198, 2006.

Thiemo Gruber studierte Informatik an der Universität Passau, wo er 2007 das Diplom erwarb. Anschließend war er als Doktorand und wissenschaftlicher Mitarbeiter am Lehrstuhl für Rechnerstrukturen der Universität Passau, der Fakultät für Maschinenbau und Mechatronik der Hochschule Deggendorf sowie am Fachgebiet für Intelligente Eingebettete Systeme der Universität Kassel beschäftigt, wo er 2012 promovierte. Gegenwärtig ist er als Post-Doktorand im DFG-geförderten Projekt „Methods for Activity Spotting With On-Body Sensors“ tätig. Seine Forschungsinteressen umfassen die effiziente Analyse von Zeitreihen sowie Methoden des Data Mining und maschinellen Lernens.

LiveShift: Ein Ansatz für zeitversetzte P2P Multimedia-Übertragungen *

Fabio V. Hecht

Universität Zürich, Institut für Informatik (IFI)
Binzmühlestrasse 14, 8046 Zürich, Schweiz
hecht@ifi.uzh.ch

Abstract: Der Peer-to-Peer (P2P) Ansatz verbessert die Skalierbarkeit und verringert die Infrastruktur- und Verwaltungskosten von Multimedia-Übertragungen, weil die Nutzer sich an der Bereitstellung des Dienstes beteiligen. Dieser Dissertationsabriss führt LiveShift ein, einen neuartigen Ansatz, der die nahtlose Kombination von P2P-Direktübertragungen und zeitversetzter Übertragungsfunktionalität in einem einzigen System ermöglicht und der die dafür notwendigen Protokolle und Regeln umsetzt. LiveShift erfüllt die Anforderungen der Netzwerk- und Dienstverwaltung, indem neue Dienste in voll dezentralisierter Art und Weise und mit minimaler Beeinflussung des Betreibers angeboten werden. Drei Kernaspekte, die sich aus dem Ermöglichen eines solchen neuartigen Anwendungsfalles ergeben, werden genauer betrachtet: (a) Ein voll verteiltes P2P-*Protokoll* für den Austausch von direkten wie von zeitverögerten Video-Übertragungen, (b) die Untersuchung von passenden *Regelsätzen zur Wiedergabesteuerung* in verschiedenen Szenarien und unter Berücksichtigung verschiedener Parameter, und (c) der Entwurf und die Auswertung eines neuartigen, *vollständig verteilten P2P-Trackers*, der gleichermassen Effizienz und Lastausgleich verbessert. Das Aufzeigen der Brauchbarkeit der erwähnten Mechanismen durch deren Integration in einer einzigen, offen und frei verfügbaren *Anwendung*.

1 Introduction

Der Peer-to-Peer (P2P) Ansatz verbessert nachweislich die Skalierbarkeit und verringert die Infrastruktur- und Verwaltungskosten von Multimedia-Übertragungen [HLL+07], da die Bereitstellung eines Dienstes teilweise an Benutzer delegiert werden kann. Dieser Dissertationsabriss führt LiveShift [Hec] ein, einen neuartigen Ansatz, der ein P2P-Overlay sowohl für die Übermittlung von Multimedia-Übertragungen als auch für die diesbezügliche Datenhaltung benutzt. Dies ermöglicht es Peers, Übertragungen zwecks zukünftiger Verbreitung zu speichern, so dass gleichermassen nahtlose Direktübertragungen, zeitversetzte Übertragungen und Video auf Abruf (Video-on-Demand, VoD) ermöglicht werden. Damit erhalten Benutzer die Freiheit, alle verfügbaren Programme ohne vorgängige Aufnahme von jeder beliebigen Position in der Übertragung aus zu starten und uninteressante Teile der Übertragung zu überspringen, bis die Direktübertragung eingeholt wurde.

*Englischer Titel der Dissertation: “LiveShift: A Time-Shifted P2P Multimedia Streaming Approach”

Das System kann beispielsweise auf einer mit einer Festplatte ausgestatteten Settop-Box oder als Anwendung auf einem Rechner installiert werden. Da das System P2P-basiert ist, sind keine wesentlichen Infrastruktur- oder Verwaltungsinvestitionen auf Anbieterseite notwendig. Die Benutzer können selbst in Übertragungs- und Speichergeräte investieren, so wie es auch der Fall ist bei digitalen Videorekordern (Digital Video Recorder, DVR). Zusätzlich haben Benutzer mit LiveShift die Möglichkeit, gespeicherte Übertragungen mit anderen zu teilen, was die Anzahl verfügbarer Programme massgeblich vergrössert.

Die Dissertation [Hec, liv] bearbeitet mehrere Aspekte, die diesen Anwendungsfall möglich machen. Die vier Hauptbeiträge der Dissertationen sind die folgenden: (a) Ein einziges, vollständig verteiltes P2P-Protokoll [HBC+11], das fähig ist, Direktübertragungen und zeitversetzte Übertragungen schnell und integriert zu lokalisieren und zu verteilen, wird detailliert beschrieben und ausgewertet; (b) Regelsätze für die Wiedergabe (sogenannte Playback-Policies), die bestimmen, ob das System die Wiedergabe anhält oder ob es Blöcke übespring, wenn Inhalte nicht verfügbar sind, werden untersucht, verglichen und bezüglich Benutzererlebnis klassifiziert [HBSS12]; (c) ein neuartiger, vollständig verteilter P2P-Tracker – B-Tracker [HBS11] genannt – wird eingeführt als ein Tracker, der Vorteile in Bezug auf Effizienz und Lastausgleich gegenüber existierender, verteilter P2P-Tracker aufweist; und (d) eine umfassende Implementation von LiveShift [HBM+08] wurde umgesetzt für die Durchführung von realistischen Experimenten und Vorführungen.

2 LiveShift-Protokoll und Policies

Die LiveShift-Architektur besteht aus einem flexiblen Protokoll und initialen Policies, die den Gebrauch des Protokolls definieren. Der geschilderte Anwendungsfall gibt Benutzern die Möglichkeit zum Kanalwechsel und dem zeitversetzten Sehen. LiveShift übernimmt den Mesh-Pull-Ansatz [HLL+07], weil er sich besser an dynamische Netzwerkbedingungen und an Dynamik im P2P-Overlay (Churn) anpasst als Baum-basierte Protokolle [MR07]. Mesh-pull teilt den Datenstrom in Stücke (Chunks) auf, die zwischen den Peers ohne fixe Struktur ausgetauscht werden. LiveShift benutzt zwei Stufen der Stückelung – ein *Segment* ist eine Adressierungseinheit, die sich aus mehreren, kleineren *Blöcken* zusammensetzt. Segmente und Blöcke werden rein zeitbasiert adressiert und identifiziert – sie sind von wohldefinierter und fixer Länge. Dies macht es trivial herauszufinden, aus welchem Block und Segment die zur Zeit abzuspielende Video-Übertragung besteht. Die Unterscheidung von Segmenten und Blöcken ist wichtig, um (mittels grösseren Segmenten) die Anzahl von Tracker-Operationen zu reduzieren, währenddem Peers Blöcke von unterschiedlichen Peers herunterladen können, so dass sich das System (wegen der kleineren Blöcke) im Fehlerfall schnell erholt. So wird im DT nur die Verfügbarkeit von Segmenten eingetragen; die Verfügbarkeit von Blöcken innerhalb eines Segments wird im direkten Austausch zwischen Peers bekannt gemacht.

Während die Kanalliste und die dazugehörigen Kanalinformationen in der DHT gespeichert werden, ist der DT für das Abbilden von Segmenten auf gewisse Anbieter – Peers die mindestens ein Segment eines Blocks haben – verantwortlich. Für die Funktion des DT wird B-Tracker, ein voll verteilter Tracker, welcher von allen Peers im Netzwerk aufrecht

erhalten wir. B-Tracker wird im detail im Unterkapitel 4 behandelt.

Ein Hauptunterschied zwischen LiveShift und anderen P2P Systemen resp. Protokollen besteht in der Behandlung der Asymmetrie von Interessen. Die Unterstützung von zeitversetztem Sehen, wie es in LiveShift vorgesehen ist, setzt voraus, dass Peers gespeicherte Blöcke liefern obwohl sie nicht zwingend an Inhalten, welche der herunterladende Peer anbietet, interessiert sind. Das verlangt nach einer Aufteilung zwischen Nachbarn und Abonnenten. Sobald ein Peer r dem System beitritt, ruft er die Kanalliste aus der DHT ab. Nachdem r eine $kanalId$ und eine $startZeit$, ausgewählt hat, konsultiert er den DT um einen Satz K_r Kandidaten, die einen Block im entsprechenden Segment angepriesen haben, zu erhalten. Alternativ können `PeerVorschlag`-Nachrichten, welche Vorschläge von Kandidaten enthalten, von anderen Peers empfangen werden. Darauf hin kontaktiert Peer r eine Zahl von Kandidaten $p \in K_r$ indem er ihnen eine `Abonnieren` Nachricht schickt, welche den $SegmentId$ und die deklarierte Upload-Kapazität enthält.

Erhält ein Peer $p \in C$ eine `Abbonieren`-Nachricht von einem Peer r, so versucht er r in seine Abonnentenliste A_p hinzuzufügen. Falls $|S_p| < \overline{S}_p$ ist, ist die Abonnentenliste noch nicht voll und eine `Abonniert`-Nachricht, welche eine Tabelle mit den Blöcken, die p gespeichert hat, und eine Abfallzeit Z_S enthält, wird an r geschickt. Peer r wird nun über Änderungen in der zugehörigen Blocktabelle mittels `Haben`-Nachrichten auf dem laufenden gehalten. Gilt $|S_p| = \overline{S}_p$, so überbrüft p ob ein anderer Peer $q \in S_p$ eine tiefere Priorität als r hat. Wenn dem so ist, wird p bevorzugt und q wird aus S_p entfernt. In jedem Fall erhält einer der beiden Peers, q oder r, eine `NichtAbonniert`-Nachricht. Die Grösse von $|S_p|$ zu limitieren ist notwendig, da wenn jeder Peer $|S|$ Abonnenten für ein Segment hat so ist die Anzahl an `Haben`-Nachrichten für einen neuen Block im gesamten P2P-System $|S|^2 - |S|$. Werden `Haben`-Nachrichten an Peers, die den betreffenden Block bereits haben, eingespart, so reduziert sich die Zahl der Nachrichten lediglich auf $(|S|^2 - |S|)/2$. Man beachte, dass sich der vorgeschlagene Algorithmus in zwei wichtigen Aspekten von bereits existierenden Mesh-Pull unterscheidet: Erstens, die Beziehung zwischen zwei Peers ist asymmetrisch und zweitens, das sofortige bevorzugen von Peers resultiert in einer schnelleren Reaktion des Systems als wenn die Peer auswahl in fixen Zeitintervallen vorgenommen wird, was die allgemeine Wiedergabeverzögerung reduziert.

Erhält Peer r eine `Abonniert`-Nachricht von p, so fügt er p zu seinen Nachbarn N_r hinzu. Jetzt muss r periodisch sein Interesse überprüfen indem er die Schnittmenge zwischen den Blöcken die zum herunterladen markiert sind und denen, welche p mit seiner Blocktabelle und seinen `Haben`-Nachrichten angepriesen hat. Ist die Schnittmenge nicht leer, so fügt r p zu I_r hinzu und sendet p eine `Interessiert`-Nachricht, was wiederrum p dazu veranlasst r in $W_p \subset S_p$, die Warteschlange für Peers die auf einen freien Upload-Platz warten, hinzuzufügen. Dann antwortet p mit einer `Eingereiht`-Nachricht, die eine Abfallzeit enthält. Im anderen Fall, in welchem p keine interessanten Blöcke mehr hat, sendet r eine `NichtInteressiert`-Nachricht um aus Q_p ausgetragen zu werden.

Peer p hat eine gewisse Anzahl an Upload-Plätzen $\overline{U}_p$, aus welchen jeweils einer einem interessierten Peer $r \in Q_p$ zur zugewiesen wird. Wird einem Peer r ein Upload-Platz zugewiesen, so erhält dieser ein `Zugewiesen`-Nachricht, welche eine Abfallzeit Z_I enthält. Bleibt der Upload-Platz in der Zeit Z_I ungenutzt, wird der Upload-Platz einem anderen Peer zugewiesen. Ähnlich zum Fall, in dem Peers in S_p sofort durch Peers mit höherer

Priorität ersetzt werden.

Erhält r einen Upload-Platz von p, ist es r erlaubt `BlockAnfrage`-Nachrichten an p zu senden und Videoblöcke mittels `BlockAntwort`-Nachrichten zu empfangen. Jeder Upload-Platz reiht maximal zwei `BlockAnfrage`-Nachrichten nacheinander in seine Warteschlange um die Verzögerung zwischen dem senden einer `BlockAntwort`-Nachricht und der nächsten `BlockAnfrage`-Nachricht zu minimieren. Das geht so weiter bis (a) r eine `NichtInteressiert`- oder eine `TrennenHoch`-nachricht sendet, (b) p eine `Eingereiht` (falls ein anderer Peer bevorzugt wird) oder eine `TrennenHerunter`-Nachricht sendet, oder (c) der Upload-Platz die Abfallzeit Z_I erreicht.

Die zwei unteschiedlichen trennen Nachrichten repräsentieren die Asymmetrie der Interessen. `TrennenHoch` wird von einem anfragenden Peer gesendet, welcher nicht mehr am herunterladen eines bestimmten Segmentes interessiert ist, i.e. beim Kanalwechsel. Ein Peer p der eine `TrennenHoch` empfängt unterlässt das Hochladen zu r und entfernt r aus S_p, Q_p und U_p. Im gegensatz werden `TrennenHerunter`-Nachrichten von einem anbietenden Peer p, welcher das System verlässt, versendet. Die Bedeutung ist ähnlich derer von `NichtAbonniert`, dahingehend, dass r aus S_p, Q_p und U_p entfernt und r seinerseits p aus K_r, N_r und I_r entfernen muss. Der unterschied liegt darin, dass r vor einem erneuten Versuch in betracht zieht, dass p das System verlassen hat.

LiveShift wurde mit dem Ziel evaluiert, die aus seinen Protokollen und Standard-Policies resultierende Leistung unter realen Bedingungen anhand der objektiven QoE Metriken Wiedergabeverzögering und Anteil der übesprungenen Blöcke zu messen. Die Evaluierung berücksichtigt, dass P2P Umgebungen heterogen bezüglich der Peer-Upload-Kapazitäten [HLR08] sind, dass Peers Kanäle mit hoher Frequenz wechseln [CRC+08], und dass Peers dem Netzwerk beitreten oder dieses verlassen (churn). Daher wurde das System vollständig implementiert. Vier Szenarien mit unterschiedlichen Peerkapazitäten wurden gewählt, um zu zeigen, dass das System eine Vielzahl von Peers mit einer Upload-Kapazität, die geringer ist als die Bitrate der Video-Übertragung, unterstützen kann. Während Szenario s1 nur 60% Last aufweist (Verhältnis zwischen der gesamten Upload- und benötigter Download-Kapazität), weist Szenario s3 85% Last auf.

Die Peers wurden konfiguriert sich wie echte Nutzer zu verhalten, indem sie Kanäle zeitversetzt ansahen und häufig wechselten. Die Kanalpopularität war annähernd exponentiell und die Verweildauer pro Kanal meist kurz (in 55.97% der Fälle betrug sie weniger als 10s) während Kanäle aber auch länger nicht gewechselt wurden (In 3.89% der Fälle wurde ein Kanal über eine Stunde nicht gewechselt). Die benutzten QoS Metriken waren die von Peers wahrgenommene und gemeldete Wiedergabeverzögerung ab dem Zeitpunkt an dem die $(channelId, startTime)$ gewählt wurde, sowie der Anteil der übersprungenen Blöcke.

Abbildungen 1 und 2 zeigen die von Nutzern wahrgenommene Wiedergabeverzögerung in ausgewählten Szenarien. Während Low-Upstream-Peers (LU) nur 50% der Stromrate heraufladne können, besitzen High-Upstream-Peers (HU) die fünffache Kapazität. Eine geringere Wiedergabeverzögerung bedeutet eine geringere Anlaufverzögering, weniger Anhalten der Wiedergabe und eine grössere Nähe zu dem, was der Nutzer initial sehen wollte. Die Ergebnisse gewähren die folgenden Einsichten, während weitere Ergebnisse

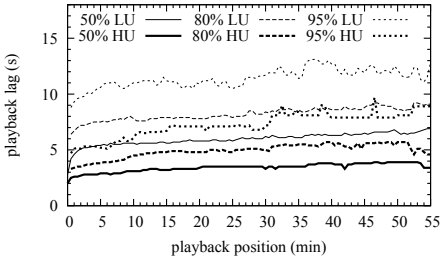


Abbildung 1: Wiedergabeverzögerung in s1

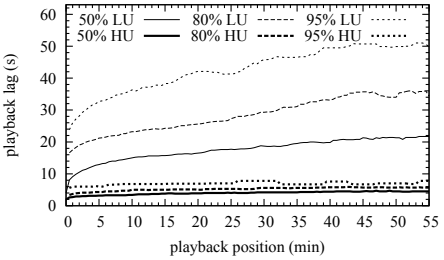


Abbildung 2: Wiedergabeverzögerung in s3

in der Dissertation zu finden sind: a) Die Wiedergabeverzögerung erhöht sich nur gering, wenn Nutzer einen Kanal länger schauen, was impliziert, dass Nutzer kein langes Anhalten der Wiedergabe wahrnehmen; b) sogar im ungünstigsten untersuchten Fall, nehmen 95% der HU Peers eine Wiedergabeverzögerung von weniger als 10s wahr, was eine akzeptable Performanz ist (viele live TV Übertragungen weisen eine ähnliche Verzögering auf); und c) LU Peers sind wesentlich anfälliger für hohe Wiedergabeverzögerungen, insbesondere in Szenarien mit Churn oder weniger verfügarer Bandbreite. Beispielsweise zeigt Abbildung 2, dass die schlechtesten 5% der LU Peers eine Wiedergabeverzögerungen von über 50 s haben, nachdem sie einen Kanal über 40 min geschaut haben.

3 Playback-Policies

Die Dissertation identifiziert zwei verwandte aber orthogonale Aspekte: die Definition von Protokollen und Poilicies zur direkten sowie zeitversetzten Multimedia-Übertragungen. Die *Playback-Policy* definiert ob ein Peer nicht-verfügbare Blöcke überspringt oder die Wiedergabe anhält, bis diese gefunden und heruntergeladen sind. Während einige Policies ausgiebig untersucht wurden, sind Playback-Policies nicht hinreichend untersucht. Dieser Abschnitt beschreibt und generalisiert vier Playback-Policies basierend auf verwandten Arbeiten und einer neuen Catchup Policy.

Skip/Stall Policy. Die Skip/Stall (`sk`) Policy wird durch $P_{sk} = (\ell, \alpha, \beta)$ definiert, wobei ℓ die Grösse des Wiedergabepuffers (in Blöcken) angibt und $\alpha \in (0, 1]$ den Füllstand des Puffers angibt, der erreicht sein muss, damit mit der Wiedergabe begonnen wird. Fehlende Blöcke werden unmittelbar übersprungen, allerdings wird bei leerem Puffer die Wiedergabe angehalten und wieder mit dem initialen Puffern begonnen. Wenn ein Block bei $b_e(t)$ fehlt und der Puffer nicht leer ist, hält die Wiedergabe an, bis ein Anteil von $\beta \in [0, 1]$ des Wiedergabepuffers gefüllt ist; erst dann werden fehlende Blöcke übersprungen.

Remaining Download Time Policy. Die Remaining Download Time Policy (`rd`) hält die Wiedergabe an bis die verbleibende Downloadzeit t_d kleiner ist als die verbleibende Wiedergabezeit t_p. Die Policy wird durch $P_{rd} = (\ell, \alpha, \beta, t_p)$ definiert, wobei der gleiche Algorithmus wie für die `sk` Policy verwendet wird. Im Gegensatz zur `sk` Policy wird allerdings eine variable Puffergrösse ℓ' verwendet, die basierend auf den Parametern t_p

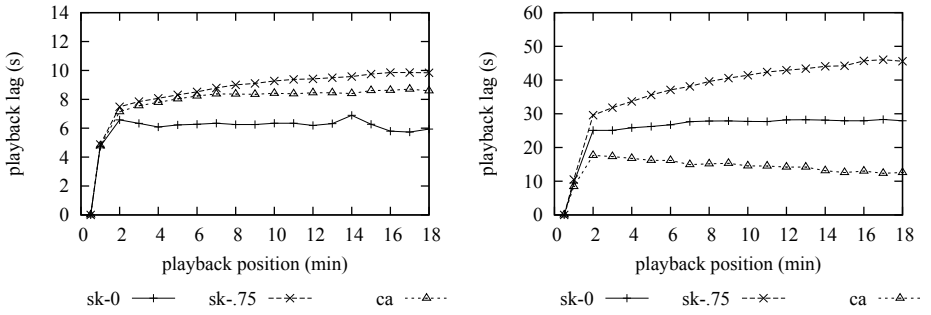


Abbildung 3: Playback-Policies, Wiedergabeverzögerung in s1 (links) und s4 (rechts)

und ℓ berechnet wird. Es sei i die Rate mit der Blöcke herunter geladen werden und L sei die Blocklänge, ausserdem sei r die relative Rate mit der Blöcke herunter geladen werden, also $r = i \cdot L$. Die variable Puffergrösse ℓ' ist daher durch $\ell' = \max\left(\frac{t_p}{L} \cdot \frac{(1-r)}{\alpha}, \ell\right)$ berechnet, wobei ℓ sowohl für das initiale Puffern als auch als eine allgemeine untere Schranke für die Puffergrösse (z.B. wenn $r \geq 1$) verwendet wird.

Retry Policy. Die Retry (`re`) Policy wird durch $P_{re} = (\ell, \alpha, T)$ definiert und hält nach dem initialen Puffern die Wiedergabe an, wenn ein Block an der Wiedergabeposition t nicht verfügbar ist. Es wird bis zu T mal versucht einen fehlenden Block abzuspielen. Sobald der Block verfügbar ist, wird er wiedergeben. Wird aber die Verzögerungsgrenze erreicht, wird er übersprungen.

Ratio Policy. Die Ratio (`ra`) Policy wird durch $P_{ra} = (\ell, \alpha, n)$ definiert, wobei die Bedeutung von ℓ und α unverändert bleibt. Nach dem initialen Puffern, wird ein verfügbarer Block an der Wiedergabeposition immer wiedergegeben. Es werden bis zu x aufeinanderfolgende fehlende Blöcke übersprungen, wenn direkt hinter diesen mindestens xn aufeinanderfolgende Blöcke verfügbar sind.

Catchup Policy. Die Policy wird durch $P_{ca} = (\ell, \alpha)$ definiert, wobei ℓ und α genau wie bei `sk` zum initialen Puffern verwendet werden. Nachdem die Wiedergabe begonnen hat, werden bei nicht-leerem Puffer alle fehlenden Blöcke übersprungen. Sollte der Puffer leer sein, wird die Wiedergabeposition zurückgesetzt, indem alle Blöcke, die für die Wiedergabeverzögerung verantwortlich sind, übesprungen werden, bis $b_e(t) = b_p(t)$.

Evaluation. Alle oben aufgeführten Playback-Policies wurden in LiveShift implementiert. Das Hauptziel war es zu vergleichen wie verschiedene Playback-Policies das Benutzererlebnis bei verschiedenen Leveln der Inhaltsverfügbarkeit beeinflussen. Bei den Experimenten wurde der gesamte LiveShift Code verwendet. Die Evaluationsparameter ähneln denen in Abschnitt 2. Jede Playback-Policy wurde mit vielen verschiedenen Werten für deren Hauptparameter untersucht. Aus Platzgründen werden in diesem Abschnitt nur Ergebnisse für die Skip/Stall mit Parametern $\beta = 0$ (`sk-0`) und $\beta = .75$ (`sk-.75`) und die Catchup Policy dargestellt. Alle Ergebnisse sind in [HBSS12] zu finden. Die Evaluationsmetriken umfassen Wiedergabeverzögering und übersprungene Blöcke.

Ausgewählte Resultate in den Abbildungen 3 zeigen, dass abhängig von der Playback-Policy (und deren Parameter), unterschiedliche Wiedergabeverzögerung resultieren. Während die Skip/Stall Policy durch den Parameter β sehr flexibel ist, resultiert die neue Catch-up Policy in einer tieferen Wiedergabeverzögerung verglichen mit anderen Policies in Szenario s4. Beobachtungen von LiveShift mit verschiedenen Playback-Policies, verschiedenen Parametern, in Szenarion mit Unter- und Überprovisionierten P2P Netzwerken, haben gezeigt dass Playback-Policies das Nutzererlebnis beinflussen. Nicht nur die ausgewählte Policy, aber auch ihre Parameter beinflussen wichtige Metriken, wie zum Beispiel die Wiedergabeverzögerung oder die Anzahl der übersprungenen Blöcke.

4 B-Tracker

Trackers werden verwendet um Peers zu finden die eine spezifische Ressource anbieten. In LiveShift sind das Peers, welche einen Block in einem spezifischen Segment anbieten. Eines der Ziele des LiveShift Entwurfs ist es von einer voll-verteilten Architektur zu profitieren, um die Skalierbarkeit und Robustheit zu verbessern; daher müssen Peers ihre Tracker-Dienst effizient anbieten und gleichmässig verteilen, so dass die Last vom Tracker Service gerecht verteilt wird. Allerdings sind heutige Tracker-Ansätze nicht geeignet, da populäre Inhalte nicht gleich verteilt wereden [HBS11].

Primäre Trackers. Zuerst setzt B-Tracker eine verteilte Hash-Tabelle (DHT) Struktur für die Tracker Entdeckung ein. Um die DHT als Tracker verwenden zu können, muss die *put(key, value)* Funktion modifiziert werden um mehrere Wertepaare abzuspeichern unter dem selben Schlüssel, und die *get(key)* Funktion muss ebenfalls modifiziert werden um eine zufällige Anzahl von Wertepaaren zurückzuliefern. Die Zahl dieser primären Peers ist durch den Replikationsfaktor von r_p gegeben. Da die primären Peers mit hoher Wahrscheinlichkeit nicht Anbieter von einer bestimmten Ressource sind, unter berücksichtigung einer zufälligen Verteilung, und um Peers zu motivieren weitere, sogenannte sekundäre Trackers zu verwendn, gibt es eine Limite von b_p Anbietern pro Ressource.

Sekundäre Trackers. Wenn ein Peer die Anbieterliste von einem primären Tracker bezogen hat, werden weitere Anfragen an sekundäre Trackers gestellt, da diese ebenfalls Anbieter dieser Ressource sind. Das führt dazu, dass die Last gleichmässig auf den sekundären Trackers verteilt wird. Der Parameter n_p legt die Anzhal der primären Trackers fest, welche zuerst konsultiert werden bevor man die sekundären Tracker anfragt.

Verbesserung der Effizienz. Anfragen an primäre und sekundäre Tracker beinhalten einen Bloom filter mit bereits bekannten Anbietern. Anbieter, welche in diesem Filter gespeichert sind werden ausgeschlossen.

Updating Mechanism. Der Replikationsfaktor r_p bestimmt wie viele Einträge für primäre Tracker gespeichert werden, und r_s bestimmt wie viele Einträge für sekundäre Tracker gespeichert werden.

Veraltete Informationen. Die Tracker-Informationen veralten mit der Zeit, da Peers das Netzwerk verlassen oder eine Ressource nicht mehr anbieten ohne den zuständigen Tracker zu informieren. B-Tracker verwendet eine Lebenszeit für jedes Wertepaar.

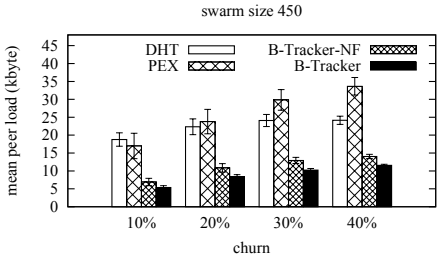


Abbildung 4: Effizienz

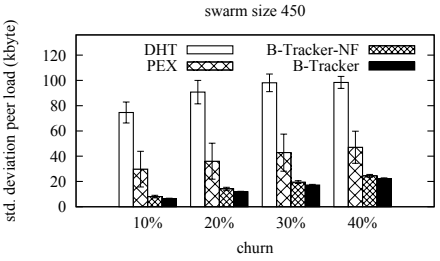


Abbildung 5: Lastausgleich

B-Tracker wurde in Java 1.6 implementiert und mit PEX und einem DHT-basierten Tracker Ansatz verglichen. Die Evaluation hat sich auf die Effizienz und den Lastausgleich fokussiert. Die Last berücksichtigt nur den Upload Traffic, da dies die knappste Ressource in eine P2P System ist. *Effizienz* ist definiert als das Mittel der Last pro Peer im Schwarm. Das heisst, je geringer die Last, desto besser die Effizienz. *Lastausgleich* ist definiert als die Standardabweichung der Last aller Peers im Schwarm. Das heisst je kleiner die Standardabweichung, desto besser der Ausgleich.

Ein P2P-System mit 1.000 Peers wurde wie folgt emuliert. Bei jedem Durchlauf wird ein Schwarm mit 50 oder 450 Peers erstellt. Jeder Peer im Schwarm erhält 35 Einträge aus der DHT. Die Messung beginnt erst, nachdem die ersten Einträge erhalten wurden, sodass ein Live-Schwarm emuliert werden kann. Um die Dynamik (churn) zu emulieren, werden Peers mit einer gewissen Wahrscheinlichkeit ausgeschaltet (10%, 20%, 30%, 40%). Die Peers, welche ausgeschalten werden, werden durch neue Peers ersetzt. Danach versuchen alle Peers 35 Einträge zu beziehen.

Effizienz. Die Abbildung 4 zeigt die durchschnittliche Belastung pro Peer für Schwarmgrössen 50 und 450. Ein DHT Ansatz ist wegen der vielen Routing-Nachrichten nicht effizient. PEX ist noch weniger effizient, weil Peers viele unnötige Meldungen versenden, um andere Peers über die Nachbaren zu informieren, ohne das dies nötig wäre. Der B-Tracker Ansatz zeigt eine bessere Effizienz als der B-Tracker-NF Ansatz wegen dem Einsatz von Bloom Filtern – obwohl diese Meldungen Grösser sind, da die Meldungen den Filter beinhalten, enthält die Liste meist keine unnnötigen Informationen.

Lastausgleich. Die Abbildung 5 zeigt den Lastenausgleich als Standardabweichung der Last von allen Peers im Schwarm. In allen untersuchten Szenarien wird die Last im B-Tracker-NF und B-Tracker Ansatz besser verteilt als mit dem DHT Ansatz. Im DHT Ansatz, werden Tracker stark ausgelastet sobald sich der Schwarm vergrössert. Der PEX Ansatz verbessert vor allem in einem grossen Schwarm den Lastausgleich. Der B-Tracker-NF Ansatz zeigt dass mit Hilfe von Bloom Filtern der Lastausgleich minimal verbessert wird. Der Lastausgleich verschlechtern sich sobald der Schwarm grösser wird. Dies kann dadurch erklärt werden, dass der DHT Ansatz verwendet wird, wenn PEX und sekundäre Tracker nicht die 35 Einträge bereitstellen können.

5 Zusammenfassung

Dieser Dissertationsabriss hat mehrere Schlüsselaspekte vorgeschlagen und untersucht, welche beim vollständig verteilten direkten und zeitversetzten P2P-Multimedia-Streaming involviert sind. Dieser Anwendungsfall war bisher grösstenteils unerforscht.

Der Fokus lag auf vier wichtigen Aspekten, namentlich (a) der Entwicklung und Evaluation eines vollständig verteilten Mesh-Pull-P2P-Protokolls, welches den Austausch sowohl von direkten als auch zeitversetzten Videostreams ermöglicht, (b) dem Untersuchen von Playback-Policies in verschiedenen Szenarien und unter Verwendung unterschiedlicher Parameter, (c) der Definition und Evaluation eines vollständig verteilten P2P Trackers, welcher sowohl die Effizienz als auch die Lastverteilung verbessert, und (d) der Demonstration der Praktikabilität obiger Mechanismen mittels Implementierung in einer OpenSource-Anwendung, welche in diesem Bericht nicht detailliert wurde.

Das LiveShift Protokoll wurde vollständig implementiert und unter höchst realistischen Bedingungen evaluiert, inklusive des schnellen Umschaltens zwischen zwischen Kanälen, einer grossen Zahl an Peers mit geringerer Upload-Kapazität als der Stream-Rate, sowie bei einer hohen Churn-Rate. Auswertungen basierend auf Traces zeigen, dass das System in der Lage ist, Inhalte und Upstream-Kapazität schnell genug zu finden, um eine geringe Wiedergabeverzögerung in Bezug zur Wiedergabeposition aufrechtzuerhalten.

Anschliessend wurde das Verhalten von LiveShift bei Anwendung verschiedener Playback-Policies mit unterschiedlichen Parametern untersucht. Es wurde offensichtlich, dass verschiedene Playback-Policies das Nutzererlebnis in einem P2P Video-Streaming-System beeinflussen, sowohl was die Wiedergabeverzögerung als auch den Anteil übersprungener Blöcke betrifft. Das Verständnis des Nutzerverhaltens ist die Grundvoraussetzung, um die am besten geeignete Policy für das gewünschte Ergebnis auszuwählen. Dabei kann entweder die Wiedergabeverzögerung so gering wie möglich gehalten, das überspringen von zahlreichen Blöcken vermieden, oder ein Kompromiss der beiden Varianten erreicht werden. Die endgültige Entscheidung kann dem Benutzer überlassen oder vom übermittelten Inhaltstyp abhängig gemacht werden.

Des Weiteren wurden der Entwurf, die Implementierung, und die Evaluation von B-Tracker beschrieben. Bei B-Tracker handelt es sich um einen neuartigen P2P-Tracker, welcher den neusten Stand der Technik weiter verbessert. Die wichtigste Innovation von B-Tracker ist, dass sämtliche Peers als Tracker für diejenigen Resourcen agieren, welche sie selbst zur Verfügung stellen. Dabei konnte bestätigt werden, dass B-Tracker im Vergleich zu verteilten P2P-Trackern, welche den reinen DHT- und PEX-Ansatz verwenden, sowohl die Effizienz als auch die Lastverteilung verbessert.

Danksagung

Der Autor dankt T. Bocek, D. Dönni, A. Lareida, P. Poullie, M. Waldburger und B. Stiller von der Communication Systems Group (CSG) der Universität Zürich sowohl für ihre wertvolle Unterstützung während der Ausarbeitung dieser Arbeit, als auch für deren

Übersetzung.

Literatur

[CRC+08] M. Cha, P. Rodriguez, J. Crowcroft, S. Moon und Xavier Amatriain. Watching Television over an IP Network. In *8th ACM SIGCOMM Conference on Internet Measurement (IMC '08)*, Seiten 71–84, New York, NY, USA, 2008.

[HBC+11] F. V. Hecht, T. Bocek, R. G. Clegg, R. Landa, D. Hausheer und B. Stiller. LiveShift: Mesh-Pull P2P Live and Time-Shifted Video Streaming. In *36th IEEE Conference on Local Computer Networks*, Seiten 319–327, Bonn, Germany, Oktober 2011.

[HBM+08] F. V. Hecht, T. Bocek, C. Morariu, D. Hausheer und B. Stiller. LiveShift: Peer-to-peer Live Streaming with Distributed Time-Shifting. In *8th International Conference on Peer-to-peer Computing (P2P'08)*, Aachen, Germany, September 2008.

[HBS11] F. V. Hecht, T. Bocek und B. Stiller. B-Tracker: Improving Load Balancing and Efficiency in Distributed P2P Trackers. In *11th IEEE International Conference on Peer-to-peer Computing (P2P'11)*, Seiten 310–313, Kyoto, Japan, September 2011.

[HBSS12] F. V. Hecht, T. Bocek, F. R. Santos und B. Stiller. Playback Policies for Live and On-Demand P2P Video Streaming. In *IFIP Networking*, Prague, Czech Republic, Mai 2012.

[Hec] F. V. Hecht. LiveShift: A Time-Shifted P2P Multimedia Streaming Approach. `http://www.csg.uzh.ch/staff/hecht/hecht-dissertation-notfinal.pdf`, last visited: November 2012.

[HLL+07] X. Hei, C. Liang, J. Liang, Y. Liu und K.W. Ross. A Measurement Study of a Large-Scale P2P IPTV System. *IEEE Transactions on Multimedia*, 9(8):1672–1687, December 2007.

[HLR08] X. Hei, Y. Liu und K. W. Ross. IPTV over P2P Streaming Networks: The Mesh-Pull Approach. *Communications Magazine, IEEE*, 46(2):86–92, March 2008.

[liv] LiveShift: P2P Live Video Streaming with Time Shifting Ability. `https://github.com/zegotinha/LiveShift/`, last visited: October 2012.

[MR07] N. Magharei und R. Rejaie. Mesh or Multiple-Tree: A Comparative Study of Live P2P Streaming Approaches. In *IEEE INFOCOM 2007*, Seiten 1424–1432, May 2007.



Fabio Victora Hecht has obtained a Doctoral degree at the Communication Systems Group at the Department of Informatics of the University of Zurich in December 2012 under supervision of Prof. Dr. Burkhard Stiller (University of Zurich, Switzerland) and Dr. Tobias Hoßfeld (Universität Würzburg, Germany). Formerly, he has obtained a five-year degree named "Bacharelado" – equivalent to a Swiss Diplom – in Computer Science from Universidade Federal do Rio Grande do Sul (UFRGS), Brazil.

Ein Einheitliches Rahmenwerk für Multi-Level Modellierung

Bastian Kennel
Lehrstuhl Software Engineering
Universität Mannheim
B6, 26, Gebäudeteil C
D-68131 Mannheim
bastian.kennel@gmail.com

Abstract: Multi-Level Modellierung hat sich in den vergangenen Jahren als mächtiges Werkzeug zur Abbildung der Klassifizierungsbeziehungen der realen Welt erwiesen. Die bisherigen Formalisierungen haben aber wesentliche Anwendungsfälle von Modellierungen ausgeblendet und dadurch die künstliche Barriere zwischen der Softwareentwicklung auf der einen Seite und der Wissensmodellierung (zB. im Umfeld der künstlichen Intelligenz, aber auch Ontologie Modellierung) auf der anderen Seite eher vergrößert als abgebaut. Diese Arbeit definiert eine Formalisierung für Multi-Level Modellierung, die beide Anwendungsfälle ermöglicht und dadurch nicht nur die Anwendungsbarriere zwischen beiden Domänen senkt, sondern durch die Kombination der Möglichkeiten neue Wege der Modellierung ermöglicht.

1 Motivation der Arbeit

Die Basis dieser Arbeit bildet der Multi-Level Modelierungsansatz nach Atkinson & Kühne [At97, AK01, AK03]. Die bestehenden Ansätze zur Implementierung dieses Ansatzes mit Hilfe der „potency“ Eigenschaft sind jedoch von der traditionellen Sichtweise der Software Entwicklung getrieben. Diese Sichtweise verhindert die Unterstützung von abweichenden Erstellungsformen und Benutzungsarten von Modellen. Diese Einschränkung reduziert nicht nur die Wirkweite des Multi-Level Modelling Ansatzes, sondern fördert auch die Spaltung der Modellierungsgruppen zwischen Software und Ontologie Entwicklung.

Die Motivation der Arbeit besteht darin, neben der Behebung einiger Schwächen des ursprünglichen „potency“ Ansatzes (u.A. [GKA08, AGK09, AKG11a]) die künstliche Kluft zwischen Softwareentwicklung und Ontologie Modellierung zu überbrücken. Die Lösung dieses Konfliktes besteht darin, eine formal definierte Basis auf Grundlage von Multi-Level Modeling[AKG12] zu erstellen und auf diesem Formalismus die Anwendungsfälle aus beiden Gebieten zu ermöglichen. Aus der Verbindung beider Ansätze und der Kombination der sich daraus ergebenden Möglichkeiten entstehen dann Möglichkeiten der Modellierung, die vorher keiner der beiden Anwendergruppen zur Verfügung standen.

2 Gegenstand und Beitrag der Arbeit

Um die formelle Basis für Multi-Level Modeling herzustellen, müssen die Bestandteile des Multi-Level Modeling Ansatzes formal erfasst und definiert werden. Die zentrale Beziehung in einem Multi-Level Model ist die Klassifizierungseigenschaft. Die Frage, ob bzw. wann ein Element eine Instanz eines anderen Elements ist wird in der Softwareentwicklung statisch beantwortet mit der Erstellungsschablone des Elements. Dies ist keine Überraschung, da in der klassischen Softwareentwicklung neue Objekte als Instanz eines Typs erzeugt werden. Die Frage der Validität dieser Beziehung stellt sich nicht, da sie per Definition wahr ist.

In einem Multi-Level Model kann man sich dieser Eigenschaft aber nicht mehr sicher sein. Da die Modellierung auch in der Meta Ebene erfolgen kann, müssen die Merkmale, die ein Element als den Typ bestimmen zu einem beliebigen Zeitpunkt nicht zwingend vorhanden sein. Startet die Modellierung gar mit einer Menge von Elementen (oder Individuen) ohne sichtbare Beziehungen (ein Standard Anwendungsfall in der Ontologie Modellierung) so ist die Bestimmung der Klassifizierungseigenschaften der Hauptzweck.

Eine Formalisierung, die sowohl den klassischen Konstruktionsansatz von neuen Elementen wie auch das Auffinden von Beziehungen zwischen Elementen unterstützen will, muss neben der entsprechenden Berücksichtigung im linguistischen Metamodel einen Mechanismus bereitstellen, um Klassifizierungsbeziehungen basierend auf den Domäneneigenschaften der Elemente zu erkennen und zu validieren. Die Definition dieses Mechanismus ist der zentrale Gegenstand dieser Arbeit.

2.1 Grundlagen der Multi-Level Klassifizierung

Die Grundlagen der Multi-Level Modellierung wurden durch Atkinson & Kühne in einer Reihe von Veröffentlichungen gelegt. Diese initiale Definition wurde aufgenommen und optimiert zu dem Zustand, der in Abbildung 1 zu sehen ist.

Beispielhaft für diese Optimierungen sei hier die Unterscheidung von Klassifizierungen in isonymische bzw. Hyponymische Klassifizierungen erwähnt. In der traditionellen, konstruktiven Sicht auf Klassifizierung ist es selbstverständlich, dass die Menge der Merkmale gleich mächtig ist [AKG11b]. Der Grund ist dass die Instanz als Objekt des Typs erstellt wurde, also genau die Merkmale besitzt, die der Typ auch besitzt. Diese Grundannahme ist aber in Multi-Level Umgebungen nicht allgemeingültig. Die isonym/Hyponym Unterscheidung adressiert dieses Problem. Eine Instanz eines Typs ist ein isonym des Typs, wenn sie alle vom Typ geforderten Merkmale besitzt, aber keines mehr. In anderen Worten, ein Isonym ist von einer Instanz, die von einem Typ erstellt wurde nicht zu unterscheiden. Im Gegensatz dazu enthält ein Hyponym alle Merkmale des Typs, aber noch mehr. Ein Hyponym kann nicht von diesem Typ erstellt worden sein, denn der Typ enthält nicht alle Merkmale, die nötig sind, um diese Instanz zu erzeugen.

Der zentrale Bestandteil des Metamodels ist Clabject. Dieses Element trägt bereits im Namen den zwei Facetten (Klasse und Object) von Multi-Level Entitäten Rechnung. Clab-

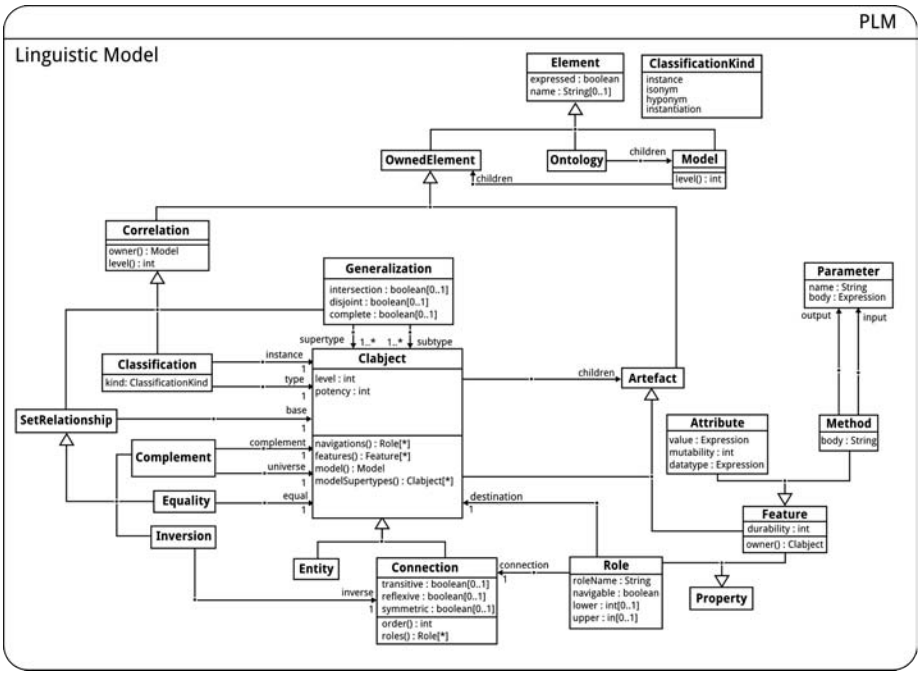


Abbildung 1: Das Panlevel Metamodel (PLM)

jects sind die einzigen Elemente, die Klassifizierungsbeziehungen eingehen können. Klassifizierungen werden durch die Korrelation Classification angezeigt. Diese Classification kann Informationen über die Art der Beziehung speichern:

instance zeigt eine Klassifizierung an, ohne weitere Informationen zu geben.

Isonym zeigt eine Klassifizierung an, bei der der Typ exakt die Informationen enthält, um die Instanz zu erzeugen.

hyponym zeigt eine Klassifizierung an, bei der die Instanz mehr Informationen enthält als der Typ.

instantiation zeigt eine Klassifizierung an, bei der die Instanz von der Vorlage des Typs erstellt wurde (ein Spezialfall von Isonym).

Die Domäneneigenschaften der Clabjects werden in Properties gespeichert. Eine Property kann entweder ein Feature oder eine Role sein. Eine Role speichert die Verbindung zu einem Anderen Clabject. Es ist zu erwähnen, dass die Verbindung selbst (repräsentiert durch ein Connection Element) ebenfalls ein Clabject ist. Dieses Konzept ist vergleichbar mit dem der Assoziationsklasse aus UML. Features speichern Datenattribute oder Verhalten eines Clabjects. Ein Datenattribut ist ein per Namen referenzierbarer Wert eines primitiven Datentyps. Ein Beispiel wäre das Alter einer Person als Zahl. Eine Methode enthält

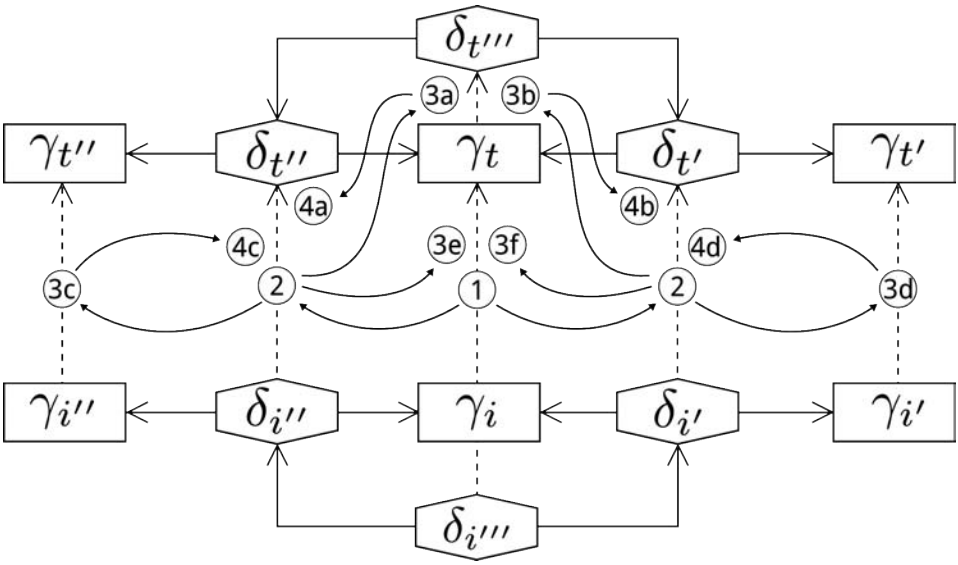


Abbildung 2: Rekursionsreihenfolge der Klassifizierungsprüfung $\gamma_i \rightarrow \gamma_t$

neben der Signatur (den Parametern) eine textuelle Repräsentation des Verhaltens. Dieser Text muss von der implementierenden Umgebung interpretierbar sein.

Vererbungen werden von Generalisierungen (Generalization) gespeichert. Die Anzahl der Sub- und Supertypen einer Generalisierung sind im Prinzip variabel, haben aber eine Auswirkung auf die Ausdruckskraft der Generaliserung. Generalisierungen können drei Merkmale besitzen:

intersection Nur möglich bei einem Subtyp mit mehreren Supertypen. Besagt, dass keine Instanz aller Supertypen existiert, die keine Instanz des Subtyps ist.

disjoint Nur möglich bei einem Supertyp mit mehreren Subtypen. Besagt, dass es keine Instanz des Supertyps gibt, die eine Instanz von mehr als einem Subtyp ist.

complete Nur möglich bei einem Supertyp mit mehreren Subtypen. Besagt, dass es keine Instanz des Supertyps gibt, die keine Instanz eines der Subtypen ist.

2.2 Formale Definition der Multi-Level Klassifizierung

Die Klassifizierungsbeziehung $\gamma_i \rightarrow \gamma_t$ ist eine paarweise Operation, doch für die Berechnung sind weitaus mehr Elemente außer den beiden Clabjects notwendig [AKG12]. Zum einen sind dort die in den Clabjects enthaltenen Properties, welche paarweise kompatibel sein müssen. Diese lokale Prüfung ist aber nicht ausreichend. Ist der Typ über eine

Connection mit einem anderen Clabject verbunden, so muss auch die Instanz eine solche Verbindung bereitstellen. Hierzu muss zum Einen das von der Instanz erreichbare Clabject eine Instanz des vom Typ erreichbaren Clabjects sein, zum Anderen aber muss die realisierende Connection ebenfalls eine Instanz sein. Der sich so aufspannende Abhängigkeitsgraph umfasst die komplette transitive Hülle der Erreichbarkeitsrelation und birgt ein rekursives Entscheidungsproblem in sich:

Damit i eine Instanz von t ist muss für jede Connection von c_t von t eine Connection c_i von i existieren, sodass $c_i \rightarrow c_t$. Die Klassifizierungsdefinition von Connections verlangt aber, dass die Teilnehmenden Clabjects in einer Klassifizierungsbeziehung stehen, welches die Frage sofort an $i \rightarrow t$ zurück gibt. Abbildung 2.2 zeigt das Rekursionsschema von $\gamma_i \rightarrow \gamma_t$.

Diese Rekursion wird durch eine lokal entscheidbare Abbruchbedingung aufgelöst. Die lokale Prüfung prüft alle Aspekte der Klassifizierung außer des rekursiven Aufrufs. Wird das selbe Paar ein zweites Mal geprüft und die lokale Prüfung war bereits erfolgreich, so wird die Rekursion positiv beendet. Letztlich kann die Rekursion nur die lokale Prüfung negativ beendet werden, denn jeder rekursive Schritt hat (außer weiteren Rekursionen) nur durch die lokale Prüfung zum Gegenstand. Wenn also das selbe Paar ein zweites Mal geprüft wird ist sichergestellt, dass alle lokalen Prüfungen bereits erfolgt sind und somit keine lokale Prüfung existiert, die die Rekursion negativ beenden könnte. Ergo kann die Rekursion positiv beendet werden.

Die Folge der rekursiven Abhängigkeit der transitiven Hülle der Erreichbarkeitsrelation ist, dass entweder alle entsprechenden Klassifizierungspaare in der Hülle valide sind, oder keines. In der Konsequenz kann eine valide Klassifizierungsrelation negiert werden durch eine Änderung des Models an einer Stelle außerhalb der beiden betroffenen Clabjects, solange sich die Änderung in der transitiven Hülle befindet.

2.3 Weiterführende Definitionen und Ergebnisse

Mit dem Werkzeug der paarweisen Klassifizierung lassen sich nun weitere Operationen definieren. Diese weiteren Operationen unterscheiden sich dahingehend, ob sie den Zustand der bearbeiteten Ontologie verändern (Evolution Services) oder nicht (Query Services).

Query Services beantworten im weitesten Sinne Fragen über die Ontologie. Diese Fragen sind häufig boolsche Prüfungen der Ontologie auf eine bestimmte Eigenschaft, welche durch Prüfung der Domänendaten beantwortet werden kann. Allgemein kann aber jeder Ausdruck auf einer Ontologie evaluiert werden.

Evolution Services führen auf dem momentanen Datenbestand der Ontologie eine Operation aus mit dem Ziel, aus den vorhanden Informationen der Ontologie neue (im Sinne von „bisher nicht explizit in der Ontologie enthalten“) Informationen zu erstellen.

Es folgen je ein Beispiel für Query Services (Ontologie Korrektheit) und Evolution Services (Subsumption).

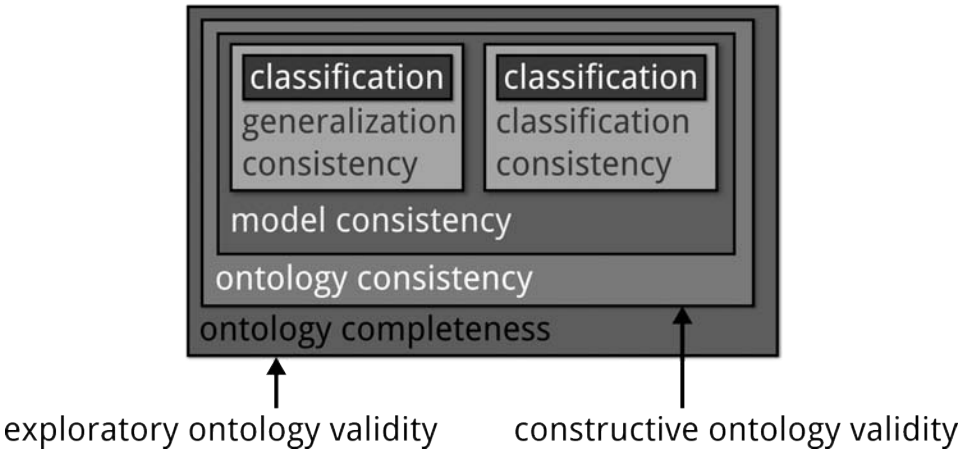


Abbildung 3: Die rekursive Konstruktion der exploratory und constructive ontology Validierung

2.3.1 Ontologie Korrektheit

Ontologie Korrektheit ist eine boolsche Auswertung auf einer Ontologie. Semantisch besagt sie, ob die Ontologie „richtig“ ist in dem Sinne, dass sie keine falschen oder widersprüchlichen Informationen enthält. Die Definition einer korrekten Ontologie variiert mit dem Modus, in dem die Ontologie betrachtet wird:

Im traditionellen konstruktiven Modus ist eine Ontologie korrekt, wenn die Informationen die sie enthält durch keine andere enthaltene Information negiert wird. Die tatsächliche Korrektheit aller Information lässt sich im konstruktiven Modus nicht erwarten, da sich die Ontologie ja noch in der Konstruktion, also in der Entwicklung befindet. Da die Ontologie noch nicht fertig ist, kann es kein Fehler sein, dass bestimmte Informationsartefakte nicht enthalten sind. Sie können der Ontologie noch hinzugefügt werden. Die bereits enthaltenen Informationen dürfen aber nicht widersprüchlich sein. Dies ist ein Fehler der nicht durch Hinzufügen weiterer Informationen behoben werden kann. Widersprüchliche Informationen die zu einer konstruktiv inkorrekten Ontologie führen sind:

- Klassifizierungen, die kein Typ-Instanz Paar verbinden
- Generalisierungen, deren Instanzraum ihren Merkmalen nicht genügt, z.B. bei einer „complete“ Generalisierung gibt es eine Instanz des Supertypes, die nicht Instanz des Subtyps ist.
- Inkonsistenzen im Stapel der Abstraktionslevel, also die Ausdehnung der Konsistenz der Klassifizierungen und Generalisierungen durch die ganze Ontologie

Im explorativen Modus reicht die konstruktive Korrektheit nicht aus. Vielmehr, dadurch dass die Grundprämisse explorativ ist kann davon ausgegangen werden, dass die Ontologie fertig ist in dem Sinne, dass die in ihr enthaltene Information komplett ist.

Konkret bedeutet dies, dass jede Behauptung eines Elements auch zutreffen muss. Eine Generalisierung behauptet eine Mengenbeziehung der Instanzen. Voraussetzung ist, dass die Generalisierung nicht auf dem untersten Level (also ohne mögliche Instanzen) existiert. Auf diesem Level dürfen keine Generalisierungen existieren und das Argument, dieses Level könne zu einem späteren Zeitpunkt hinzugefügt werden ist im explorativen Modus nicht valide.

Formell wird diese Eigenschaft durch die „potency" der Clabjects erfasst. Hat ein Clabject eine potency größer als null, so bedeutet dies, dass ein Isonym des Clabjects existiert. Hat ein Clabject eine potency von zwei so bedeutet dies, dass ein Isonym welches eine potency von eins hat, existiert. Im konstruktiven Modus ist es ausreichend, dass diejenigen Isonyme die existieren korrekt definiert sind, im explorativen Modus müssen alls Isonyme, die durch eine potency impliziert sind auch tatsächlich existieren.

Abbildung 3 zeigt schematisch die Definition der Korrektheit einer Ontologie.

2.3.2 Subsumption

Im Kontext von Multi-Level Modeling bezeichnet Subsumption das Auffinden von neuen Generalisierungen. Semantisch bedeutet dies, dass neue Typen für das Instanzlevel gefunden werden. Die Stärke der formalen Definition der Klassifizierung kommt zum Tragen, da gleich die Attribute des neuen Typs mit berechnet werden können. Der Algorithmus für Supsumption ist in Algorithmus 1 angegeben.

Algorithmus 1 Σ_i.`subsumption`()

for $\gamma_s \in \Sigma_i$.`clabjects`() **do**
  $subtypes \leftarrow \emptyset$
  for $\gamma \in \Sigma_i$.`clabjects`() $\setminus \{\gamma_s\}$ **do**
    if γ.`subsume`(γ_s) **then**
      $subtypes \leftarrow subtypes \cup \{\gamma\}$
  if $|subtypes| > 0$ **then**
    $\xi \leftarrow$ `Generalization`()
    ξ.supertype $\leftarrow \{\gamma_s\}$
    ξ.subtype $\leftarrow subtypes$
    $disjoint \leftarrow$ **true**
    $complete \leftarrow$ **true**
    for $\gamma_i \in \Sigma_{i+1}$.`clabjects`() : γ_i.`isIsonym`(γ_s) **do**
      if $\nexists \gamma_{s'} \in \xi$.subtype : γ_i.`isIsonym`($\gamma_{s'}$ **then**
        $complete \leftarrow$ **false**
      if $\exists \gamma_{s'}, \gamma_{s''} \subset \xi$.subtype : $\gamma_{s'} \neq \gamma_{s''} \wedge \gamma_i$.`isIsonym`($\gamma_{s'}$) $\wedge$ γ_i.`isIsonym`($\gamma_{s''}$) **then**
        $disjoint \leftarrow$ **false**
    ξ.disjoint $\leftarrow disjoint$
    ξ.complete $\leftarrow complete$

Zentraler Bestandteil ist die `subsume` Operation zwischen zwei Clabjects, die prüft ob das

eine ein Subtyp des anderen ist. Die Definition von Subtyp kann hier über den Umweg der Instanzen gewählt werden:

Ein Clabject c1 ist ein Subtyp eines Clabjects c2, wenn jede Instanz von c1 auch eine Instanz von c2 ist.

Diese Definition hat aber das Problem, dass die Existenz der Instanzen zur Berechnung notwendig ist. Da die Instanzmenge eines Typs aber bereits durch die Merkmale des Typs definiert ist, lässt sich die Definition eines Subtyps relativ einfach hierdurch ausdrücken.

Der Algorithmus prüft paarweise alle Clabjects und erstellt für jede nichtleere Menge von Subtypen eine Generalisierung. Anschließend werden die *disjoint* und *complete* Attribute berechnet. Ein Isonym des Supertyps welches keine Instanz eines der Subtypen ist, negiert die *complete*; ein Isonym des Supertyps, welches ein Isonym mehr als eines Subtyps ist, negiert *disjoint*.

Nach Ausführung des Algorithmus sind alle Generalisierungen mit der semantischen Priorität der Anzahl der Subtypen erstellt und deren Attribute basierend auf dem vorhanden Instanzlevel berechnet.

3 Beitrag der Arbeit zur weiterführenden Forschung

Die Trennung der Welten der Software Entwicklung und der Wissensmodellierung der Ontologien war über viele Jahre von konzeptionellen Problemen geprägt wie etwa der Unterscheidung der Open World und Closed World Assumption (OWA/CWA), die Formalisierung der instance-of Relation oder in der Summe die unterschiedlichen Anwendungsfälle und daraus resultierenden Funktionen. Mit den Ergebnissen dieser Arbeit ist die Grundlage für die Harmonisierung dieser beiden Welten gegeben.

Es werden aber auch gänzlich neue Ansätze geboten:

- Die Unterscheidung der Klassifizierung von Isonym und Hyponym löst nicht nur bestehende gedankliche Probleme. Bisher konnte nur von „Typ“ oder „Instanz“ gesprochen werden. Diese Unterscheidung bietet nun die Möglichkeit, präziser zu beschreiben welche Beziehung gemeint ist.
- Die Gleichbehandlung aller Abstraktionsebenen ermöglicht echte Multi-Level Modellierung mit beliebig vielen Abstraktionsebenen in jede Dimension.
- Die Implementierung als modelgetriebener grafischer Editor (Melanie,[GK11]) auf der Eclipse Platform unter Zuhilfenahme der Eclipse Projekte EMF und GMF bietet große Erweiterungsmöglichkeiten nicht nur im formellen Bereich: die Kopplung von grafischer und textueller Repräsentation und die Verbindung von domänenspezifischer und allgemeiner Darstellung von Modellen [AGK12a] sind zwei Felder, die innerhalb der Gruppe gerade untersucht werden. Die Integration von OCL in EMF Modelle macht Auswertungen von beliebigen Ausdrücken auf der Datenbasis der Ontologie möglich.[AGK12b]

- Die Unterscheidung in konstruktive und explorative Modellierung löst nicht nur seit langem bestehende Widerstände auf, sondern gibt Raum für weiterführende Fragestellungen: Was bedeutet es semantisch, wenn man die Modellierungsart wechselt und aus welchen Gründen sollte man das tun? Muss man eventuell die instance-of Relation abhängig von diesem Modus implementieren?
- Die Ontologien in Melanie werden nie in Code übersetzt und können trotzdem ausgeführt und formell behandelt werden, da die Entwicklung vollkommen modelgetrieben ist. Es ist also jederzeit eine vollständige Kette von Model (Anforderung) zu laufendem Code gegeben.

Zusammenfassend haben die Ergebnisse dieser Arbeit das Potenzial viele Felder der Softwareentwicklung zu berühren (Requirements Engineering, Knowledge Engineering bis hin zu Domain Specific Languages), obwohl der ursprüngliche Fokus der Arbeit auf einem sehr speziellen Feld, nämlich Multi-Level Modellierung lag.

Literatur

[At97] Atkinson, C.: Meta-Modelling for distributed Object Environments. Enterprise Distributed Object Computing Workshop. EDOC‘97. 1997.

[AK01] Atkinson, C.; Kühne, T.: The Essence of multilevel metamodeling. Proceedings of the 4th International Conference on The Unified Modeling Language, Modeling Languages, Concepts, and Tools . Springer. 2001.

[AK03] Atkinson, C.; Kühne, T.: Model-driven development: a metamodeling foundation. IEEE Software 20(5). IEEE. 2003.

[GKA08] Gutheil, M.; Kennel, B.; Atkinson, C.: A Systematic Approach to Connectors in a Multilevel Modeling Environment. ACM/IEEE 11th International Conference on Model Driven Engineering Languages and Systems, MODELS 2008. Springer. 2008.

[AGK09] Atkinson, C.; Gutheil, M.; Kennel, B.: A Flexible Infrastructure for Multilevel Language Engineering. IEEE Transactions on Software Engineering, 35(6). IEEE Computer Society. 2009. S. 742-755.

[AKG11a] Atkinson, C.; Kennel, B.; Goß, B.:The Level-Agnostic Modeling Language. Proceedings of the 3rd Internation Conference on Software Language Engineering, SLE 2010. Springer. 2011.

[AKG12] Atkinson, C. et. al.: Classification in Potency-based multi-level Modeling, IEEE Transactions on Software Engineering *(in review)*. 2012.

[AKG11b] Atkinson, C.; Kennel, B.; & Goß, B.: Supporting Constructive and Exploratory Modes of Modeling in Multi-Level Ontologies. 7th International Workshop on Semantic Web Enabled Software Engineering, SWESE 2011. Springer. 2011.

[GK11] Gerbig, R.; Kennel, B.: Multi-Level Modeling and Ontologie Engineering Environment (Melanie). http://code.google.com/a/eclipselabs.org/p/melanie/. 2011.

[AGK12a] Atkinson, C.; Gerbig, R.; Kennel, B.: Symbiotic General-Purpose and Domain-Specific Languages. Proceedings of the 34rd International Conference on Software Engineering, ICSE 2012. ACM. 2012.

[AGK12b] Atkinson, C.; Gerbig, R.; Kennel, B.: On-the-Fly Emendation of Multi-Level Models. Modelling Foundations and Applications, 8th European Conference, ECMFA 2012. Springer. 2012.

[Ke12] Kennel, B.: A Unified Framework for Multi-Level Modeling. Dissertation, Universität Mannheim. 2012. https://ub-madoc.bib.uni-mannheim.de/31906



Bastian Kennel wurde am 5. August 1981 in Mannheim geboren. Nach dem Abitur im Jahr 2001 am Werner-Heisenberg-Gymnasium in Bad Dürkheim und dem Zivildienst sowie einem Sommer als Bademeister folgte 2002 das Diplom Studium des Integrierten Studiengangs Mathematik-Informatik an der Universität Mannheim. Nach dem Grundstudium war er als Tutor für diverse Grundstudiumsvorlesungen tätig und wählte als Vertiefung *Softwaretechnik* am Lehrstuhl von Prof. Colin Atkinson. Dieses Studium schloss er Anfang 2008 mit einer Diplomarbeit im Bereich Modellsemantik ab. Unmittelbar im Anschluss folgte die Arbeit als wissenschaftlicher Assistent am Lehrstuhl Atkinson welche in die vorliegende Doktorarbeit mündete. Seit 2009 arbeitet er bei der BASF IT Services GmbH in Ludigshafen, neben der Promotion in Teilzeit, seit 2012 in Vollzeit.

Approximationsalgorithmen für Spektrumsallokation und Power Control in Funknetzwerken*

Thomas Kesselheim

Department of Computer Science
Cornell University
kesselheim@cs.cornell.edu

Abstract: In einem Funknetzwerk können gleichzeitige Transmissionen aufgrund von Interferenzeffekten kollidieren. Um trotzdem eine zuverlässige Funktionsweise garantieren zu können, sind Algorithmen erforderlich, die die Zugriffe auf das Funkspektrum verwalten. In dieser Arbeit entwerfen und analysieren wir derartige Algorithmen aus der Perspektive der Theoretischen Informatik. Da sich die behandelten Probleme unter den üblichen Annahmen der Komplexitätstheorie nicht effizient exakt lösen lassen, betrachten wir Approximationsalgorithmen. Hierbei verfolgen wir das Ziel, beweisbare Garantien über die Qualität der berechneten Lösung herzuleiten. Im Gegensatz zu den meisten früheren Arbeiten in der Algorithmik modellieren wir die Interferenzbedingungen mit Hilfe des Signal-zu-Interferenz-plus-Rausch-Verhältnisses (signal-to-interference-plus-noise ratio, SINR). Auf diese Weise erlaubt uns das Interferenzmodell, variable Sendeleistungen zu berücksichtigen.

1 Einleitung

Funknetzwerke spielen eine enorme Rolle in unserer heutigen Gesellschaft. Beispielweise ist drahtloser Internetzugang mittels Mobilfunknetzen und WLANs heutzutage allgegenwärtig. Eine weitere, vielversprechende Anwendung sind Sensornetze. Diese bestehen aus kleinen Geräten, die sich selbstständig koordinieren, um Messungen in der Industrie oder der Umwelt vorzunehmen.

Eine wichtige Gemeinsamkeit all dieser Funknetzwerke besteht darin, dass gleichzeitige Transmissionen aufgrund von Interferenzeffekten kollidieren können. Beim Bau von Sensornetzen muss der Umgang mit Interferenz selbstverständlich berücksichtigt werden. In Netzen mit fester Infrastruktur hingegen konnte in der Vergangenheit Interferenz bereits bei der Konzeption der Netze grundsätzlich ausgeschlossen werden, indem für unterschiedliche Dienste bzw. Funkzellen verschiedene Frequenzen verwendet wurden. Dieser Ansatz ist aber leider an seine Grenzen gestoßen: Durch den sehr großzügigen Umgang mit Spektrum sind Frequenzen ein knappes Gut geworden, das es mit Bedacht zu verwal-

*Englischer Titel der Dissertation: "Approximation Algorithms for Spectrum Allocation and Power Control in Wireless Networks" [Kes10]. Diese Arbeit wurde unterstützt durch das UMIC Research Centre, RWTH Aachen University.

ten gilt.

Zum Betrieb jeglicher Funknetzwerke werden daher intelligente Algorithmen benötigt, die Spektrumszugriffe kontrollieren und koordinieren. Bei deren Entwicklung legen praktisch motivierte Arbeiten ihren Schwerpunkt häufig auf gewisse technologische oder regulatorische Aspekte. Sie evaluieren ihre Ergebnisse anschließend in Simulationen oder Experimenten. Dieser Ansatz hat jedoch den Nachteil, dass er im Wesentlichen heuristisch arbeitet: Allgemeine Eigenschaften können auf diese Weise nur schwer nachgewiesen werden.

Im Gegensatz hierzu liefert die theoretische Analyse von Algorithmen beweisbare Garantien. Bedauerlicherweise greifen jedoch die meisten Arbeiten, die Algorithmen in drahtlosen Netzwerken analysieren, auf unrealistische Annahmen zurück. Üblicherweise werden die Interferenzbedingungen durch einen Graphen modelliert, dessen Kanten angeben, ob eine Transmission mit einer anderen kollidieren würde. Dies ist jedoch in mehrerer Hinsicht zweifelhaft, weil physikalische Bedingungen nur ungenügend abgebildet werden: Um eine Transmission erfolgreich zu übermitteln, darf die Gesamtheit der Interferenz nicht zu groß sein. Ein solches Modell hingegen betrachtet Interferenzen einzelner Sender lediglich separat. Darüber hinaus ist es auf diese Weise auch nicht möglich, verschiedene Sendeleistungen zu modellieren.

In dieser Arbeit versuchen wir, die beiden genannten Ansätze anzunähern und wünschenswerte Eigenschaften zu kombinieren. Wir nutzen hierzu etablierte Modelle aus der Elektrotechnik, um die Interferenzbedingungen zu modellieren. Diese erlauben uns, die genannten Effekte durch Aggregation von Interferenz und unterschiedliche Sendeleistungen zu berücksichtigen. Die behandelten Algorithmen analysieren wir formal und beweisen Garantien über die Güte ihrer Lösungen. Aus diesem Grund sind unsere Untersuchungen von sehr grundsätzlicher Natur. Wir abstrahieren von den verschiedenen Anwendungsgebieten und Technologien und konzentrieren uns auf die gemeinsamen zugrunde liegenden kombinatorischen Optimierungsprobleme.

1.1 Interferenzmodell

Wir benutzen ein Standardmodell aus der Elektrotechnik (siehe z. B. [Rap01]), das erstmalig von Moscibroda und Wattenhofer [MW06] in einer Fragestellung der Algorithmik betrachtet wurde. Es basiert auf dem Signal-zu-Interferenz-plus-Rausch-Verhältnis (signal-to-interference-plus-noise ratio, SINR). Bei der SINR handelt es sich um das übliche Maß, um die Qualität eines empfangenen Signals zu quantifizieren. Sie ist definiert als das Verhältnis zwischen Stärke des gewünschten Signals und der Summe aller anderen Signalstärken plus Rauschen. Je größer dieses Verhältnis ist, desto besser können verschiedene Symbole in einer Transmission unterschieden werden und desto besser ist folglich die Signalqualität.

Für eine formale Definition müssen wir zunächst die Signalausbreitung modellieren. Für die Abnahme der Signalstärke bei der Ausbreitung einer elektromagnetischen Welle sind verschiedene Effekte verantwortlich. Diese werden typischerweise in einem einfachen Pfadverlust-Modell zusammengefasst. Wir nehmen an, dass sich die Knoten des Funknetz-

werkes in einem metrischen Raum (V, d) befinden. Wenn ein Knoten s mit Leistung p sendet, empfängt ein Knoten r in Entfernung $d(s, r)$ dieses Signal mit einer Stärke proportional zu $p/d(s, r)^\alpha$. Die Konstante α wird als Pfadverlust-Exponent (*path-loss exponent*) bezeichnet. Häufig wird angenommen, dass dieser einen Wert zwischen 2 und 6 annimmt; Werte kleiner als 2 können jedoch auch auftreten. Für die meisten unserer Ergebnisse reicht die Annahme $\alpha > 0$ aus.

Gegeben sei nun eine Menge $\mathcal{L} \subseteq V \times V$ von Paaren von Sendern und Empfängern (*links*), die gleichzeitig auf derselben Frequenz senden, sowie eine Zuweisung von Sendeleistungen (*power assignment*) $p\colon \mathcal{L} \to \mathbb{R}_{>0}$. Die SINR von Transmission $\ell = (s, r)$ ist nun definiert als

$$\gamma_\ell(\mathcal{L}, p) = \frac{\frac{p(\ell)}{d(s,r)^\alpha}}{\sum_{\ell'=(s',r')\in\mathcal{L},\ell'\neq\ell} \frac{p(\ell')}{d(s',r)^\alpha} + \nu} \ .$$

Die Konstante $\nu > 0$ dient zur Modellierung von Hintergrundrauschen, das für alle Transmissionen identisch angenommen wird.

Bei den meisten Problemstellungen nehmen wir feste Datenraten an. In unserem Modell bedeutet dies, dass die SINR einen gewissen Schwellenwert für eine erfolgreiche Transmission überschreiten muss.

2 Capacity-Maximization Problem

Das *Capacity-Maximization Problem* ist die wahrscheinlich grundlegendste Fragestellung der kombinatorischen Optimierung im Zusammenhang mit dem oben dargestellten Interferenzmodell: Gegeben ist eine Menge von n Kommunikationsanfragen, von denen eine möglichst große Anzahl ausgewählt werden soll, die gleichzeitig bedient werden kann. Man unterscheidet dabei zwischen der Variante, in der die Sendeleistungen im Voraus festgelegt sind, und der Variante, in der der Algorithmus diese festlegen darf bzw. muss. Zunächst soll hier auf die zweitgenannte Variante eingegangen werden, wobei wir zusätzlich annehmen, dass für alle Anfragen derselben Schwellenwert β gilt, den die SINR jeweils erreichen muss.

Formal stellt sich diese Problemstellung wie folgt dar: Gegeben ist eine Menge $\mathcal{R} \subseteq V \times V$ von Kommunikationsanfragen. Es müssen nun eine Teilmenge $\mathcal{L} \subseteq \mathcal{R}$ und ein Power Assignment $p\colon \mathcal{L} \to \mathbb{R}_{>0}$ ausgewählt werden, so dass für alle gewählten $\ell \in \mathcal{L}$ gilt: $\gamma_\ell(\mathcal{L}, p) \geq \beta$. Das Ziel ist es, $|\mathcal{L}|$, die Größe der Menge $\mathcal{L}$, zu maximieren. Andrews und Dinitz [AD09] zeigten, dass dieses Problem NP-vollständig ist. Deshalb konzentrieren wir uns hier auf Approximationsalgorithmen.

Die wesentliche Schwierigkeit beim Entwurf eines Algorithmus für dieses Problem ist der Umgang mit der Auswahl der Sendeleistungen. Ein sehr einfacher Ansatz ist es, die Möglichkeit der Wahl der Sendeleistungen zu ignorieren und alle Sendeleistungen auf denselben, festen Wert zu setzen (*uniform power assignment*). Interessanterweise erreicht man auf diese Weise bereits Approximationsfaktoren von $O(\log \Delta)$, wie beispielsweise von Andrews und Dinitz [AD09] gezeigt. Hierbei ist $\Delta = \frac{\max_{(s,r)\in\mathcal{R}} d(s,r)}{\min_{(s,r)\in\mathcal{R}} d(s,r)}$, das heißt das

Verhältnis von größtem zu kleinsten Abstand, den ein Sender zu seinem Empfänger hat.

Bessere Ergebnisse können erreicht werden, indem man die Sendeleistung für einen Link $\ell = (s, r)$ abhängig vom Abstand von s und r setzt, nämlich proportional zu $\sqrt{d(s,r)^\alpha}$. Diese *Square-Root Power Assignments* wurden erstmalig in [FKRV09] untersucht. In mehreren, teilweise aufeinander aufbauenden Arbeiten von Halldórsson und anderen [Hal09, HM11, HHMW13] konnte gezeigt werden, dass auf diese Weise Approximationsfaktoren von $O(\log\log\Delta)$ möglich sind.

Jedoch hat auch diese Wahl einen deutlichen Nachteil: Sowohl für Uniform Power Assignments als auch für Square-Root Power Assignments gibt es Familien von Netzwerken (mit $\Delta = 2^n$ bzw. $\Delta = 2^{2^n}$), in denen nur Approximationsfaktoren der Größenordnung $\Omega(n)$ erreicht werden. Damit sind die erreichten Ergebnisse nicht entscheidend besser als die von trivialen Algorithmen: Bereits ein Algorithmus, der nur einen einzigen beliebigen Link auswählt, hat einen Approximationsfaktor von n.

Tatsächlich ist dies aber eine Schwäche des gesamten Ansatzes, Sendeleistungen nur abhängig vom Abstand zwischen Sender und Empfänger zu wählen. Fanghänel et al. [FKRV09] konnten zeigen, dass für alle Funktionen $f\colon \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ eine Familie von Instanzen existiert, so dass mit dem Power Assignment $p(\ell) = f(d(\ell))$ nur Approximationsfaktoren in $\Omega(n)$ erreicht werden können. Dies führte zu der Frage, ob es Algorithmen gibt, die auf allen Instanzen eine nicht-triviale Approximationsgarantie erreichen.

In dieser Arbeit stellen wir den ersten Algorithmus mit konstantem Approximationsfaktor vor. Dies bedeutet, dass auf Instanzen beliebiger Größe – also unabhängig von n – die berechnete Lösung höchstens einen konstanten Faktor schlechter sein kann als die optimale Lösung. Diese Konstante hängt vom Pfadverlust-Exponenten α ab. Sie wurde nicht weiter optimiert, um die Analysen so einfach wie möglich zu halten und da besonders das asymptotische Verhalten von Bedeutung ist.

Der Algorithmus ist strukturell erstaunlich einfach. Im Gegensatz zu früheren Algorithmen wird zunächst die Link-Menge $\mathcal{L}$ ausgewählt und erst im Anschluss die Sendeleistung zugewiesen. Die Auswahl geschieht durch einen Greedy-Algorithmus. Er betrachtet die Links der Menge $\mathcal{R}$ nach steigendem Abstand zwischen Sender und jeweiligem Empfänger. Ein Link $\ell' = (s', r')$ wird hinzugefügt, wenn bezüglich der bislang ausgewählten Links gilt

$$\sum_{\substack{(s,r)\in\mathcal{L}\\ d(s,r)<d(s',r')}} \frac{d(s,r)^\alpha}{d(s,r')^\alpha} + \frac{d(s,r)^\alpha}{d(s',r)^\alpha} \leq \tau := \frac{1}{2\cdot 3^\alpha\cdot(4\beta+2)} \quad .$$

Das bedeutet, dass die Abstände zwischen den Sendern und Empfängern des aktuell betrachteten Links und denen der zuvor ausgewählten groß genug sein müssen. Zur anschließenden Auswahl der Sendeleistungen würde es eigentlich ausreichen, ein lineares Gleichungssystem zu lösen. Wir nutzen jedoch einen anderen Algorithmus. Es ist nämlich noch erforderlich, zu zeigen, dass es überhaupt Sendeleistungen gibt, die alle ausgewählten Transmissionen gleichzeitig erfolgreich machen. Dieser Algorithmus durchläuft die ausgewählten Links, nun aber nach fallendem Abstand zwischen Sender und Empfänger.

Die Sendeleistung für Link ℓ' wird dabei festgelegt auf

$$p(\ell') = 4\beta \sum_{\substack{(s,r)\in\mathcal{L} \\ d(s,r)>d(s',r')}} \frac{p(\ell)}{d(s,r')^\alpha} d(s',r')^\alpha \quad .$$

Das bedeutet: Es wird eine Sendeleistung proportional zur minimalen Sendeleistung ausgewählt, die erforderlich wäre, um nur gegen die Interferenz der längeren Links anzukommen.

Aus Platzgründen kann hier leider nicht die Analyse vorgestellt werden. Sie besteht aus zwei größeren Teilen: Einerseits muss gezeigt werden, dass überhaupt eine gültige Lösung berechnet wird. Es ist nicht offensichtlich, dass im Endeffekt tatsächlich alle SINR-Bedingungen erfüllt sind. Andererseits ist natürlich auch noch die Approximationsgarantie zu zeigen; das heißt, dass der Approximationsfaktor durch eine Konstante beschränkt ist.

2.1 Erweiterungen

Der obige Algorithmus lässt sich in mehrfacher Hinsicht erweitern. Beispielsweise ist bislang nur vorgesehen, dass alle SINR-Schwellenwerte identisch sind. Mit einigen leichten Änderungen ist es auch möglich, individuelle Schwellenwerte zu berücksichtigen.

Dies ist insbesondere von Belang, um einen Algorithmus für flexible Datenraten zu entwerfen. Hier wird nicht mehr nur angenommen, dass eine Transmission entweder erfolgreich ist oder nicht. Vielmehr läuft die Übertragung – abhängig von der Signalqualität – mit einer unterschiedlichen Datenrate. Zur Modellierung wird kein Schwellenwert mehr auf die SINR angenommen, sondern allgemeiner eine Utility-Funktion u_ℓ, welche SINR-Werte auf die jeweilige Datenrate abbildet. Das Ziel ist nun, die Funktion $\sum_{\ell\in\mathcal{L}} u_\ell(\gamma_\ell(\mathcal{L}, p))$ zu maximieren. Dieses Problem kann mit Hilfe eines Algorithmus für das Problem mit Schwellenwerten gelöst werden. Hierbei wird in der Approximationsgarantie ein zusätzlicher Faktor $O(\log n)$ verloren.

Darüber hinaus können alle beschriebenen Techniken auch für vorgegebene Sendeleistungen angewendet werden. In der Arbeit wird gezeigt, wie ein von Halldórsson und Mitra [HM11] vorgestellter Algorithmus in analoger Weise analysiert und auf individuelle Schwellenwerte erweitert werden kann.

2.2 Simulationsergebnisse

Alle bislang vorgestellten Ergebnisse entstammen Worst-Case-Analysen. Diese könnten jedoch durch künstliche, pathologische Instanzen verfälscht werden. Um dies auszuschließen, führten wir einige Simulationen durch. Insbesondere interessierte uns hierbei, ob der Einfluss von unterschiedlichen Sendeleistungen tatsächlich derart bedeutsam ist, wie unsere Worst-Case-Analysen ergaben. Mittels nicht-konvexer Optimierung lösten wir deshalb zufällig erzeugte Instanzen des Capacity-Maximization Problem optimal. Interessanter-

weise stellte sich heraus, dass auch in diesem Fall Square-Root Power Assignments besser abschneiden als Uniform Power Assignments. Eine Optimierung der Sendeleistung führt jedoch zu noch deutlich besseren Ergebnissen. Insofern liefern die theoretischen Analysen Erkenntnisse, die auch in zufällig erzeugten Instanzen Bestand haben.

Weitere Simulationen zeigen, dass die von uns entwickelten Algorithmen zwei wünschenswerte Eigenschaften vereinen: In Bezug auf zufällig erzeugte Instanzen zeigen sie vergleichbare Ergebnisse wie frühere Algorithmen. Im Gegenzug ist jedoch bei unseren Algorithmen die Qualität der Lösung garantiert. Insbesondere ist sichergestellt, dass in keinem Netzwerk nur triviale Lösungen berechnet werden.

Wie eingangs erwähnt, war es das Ziel dieser Simulationen, zu evaluieren, ob Worst-Case-Analysen auch für andere Instanzen hilfreiche Erkenntnisse liefern können. Das benutzte Interferenz-Modell wurde hierbei nicht hinterfragt. Für zukünftige Untersuchungen könnte es interessant sein, die Algorithmen in realistischeren Modellen zu simulieren oder gar in realen Netzen zu testen. Das geht jedoch weit über diese Arbeit hinaus, deren Gegenstand die theoretische Analyse von Algorithmen ist.

3 Latency-Minimization Problem

Ein weiteres, sehr grundlegendes Problem ist das *Latency-Minimization Problem*. Hier müssen alle Anfragen in möglichst wenigen Zeitschritten bedient werden. Auch für diese Problemstellung untersuchen wir sowohl die Variante, in der die Sendeleistungen im Voraus gegeben sind, als auch diejenige, in der der Algorithmus die Sendeleistungen auswählt.

Aus den entsprechenden Capacity-Maximization-Algorithmen lassen sich für diese Probleme unmittelbar Algorithmen erstellen, indem jeweils iterativ die Ausnutzung des ersten Zeitschritts maximiert wird. Auf diese Weise erreichen wir für beide Varianten $O(\log n)$-Approximationen.

Weiterhin analysieren wir einen verteilten Algorithmus für *Latency Minimization* mit festen Sendeleistungen. Dieser lässt alle Sender mit einer festen Wahrscheinlichkeit senden, bis diese zum ersten Mal erfolgreich sind. Wir zeigen, dass auf diese Weise eine $O(\log^2 n)$-Approximation erreicht werden kann. Wir erweitern den Algorithmus, so dass die einzelnen Sender nur sehr wenige Informationen brauchen: Zunächst zeigen wir, wie die optimale Sendewahrscheinlichkeit gefunden werden kann. Darüber hinaus zeigen wir, dass es mit nur konstanten Kosten möglich ist, Acknowledgement-Transmissionen zu implementieren. Durch die Asymmetrie des Modells ist nämlich nicht sichergestellt, dass auch eine bestätigende Transmission vom Empfänger zum Sender erfolgreich wäre.

Darüber hinaus können vorhandene Ansätze mit unseren Algorithmen kombiniert werden, um Multi-Hop-Scheduling-Probleme zu lösen. Für diese erreichen wir ebenfalls Approximationsfaktoren, die poly-logarithmisch in n beschränkt ist.

4 Rayleigh-Fading

Das beschriebene einfache Pfadverlust-Ausbreitungsmodell lässt viele Faktoren außer Acht. So interferiert eine elektromagnetische Welle beispielsweise auch mit ihren eigenen Reflexionen. Diese Interferenz kann konstruktiv oder destruktiv sein – die Signalstärke kann hierdurch also verstärkt oder geschwächt werden. Dies hängt davon ab, wie sich die Laufwege der einzelnen Kopien der elektromagnetischen Welle unterscheiden. Als Folge treten in manchen Umgebungen starke Schwankungen der Signalstärke auf verhältnismäßig kleinen Abständen auf.

Um diese Effekte zu modellieren, wird häufig Rayleigh-Fading eingesetzt. Die Signalstärken werden hierbei als stochastisch angesehen. Eine Transmission ist auch hier erfolgreich, wenn die SINR hoch genug ist – diese ist jetzt allerdings eine Zufallsvariable.

Wir betrachten ein solches stochastisches Interferenzmodell erstmalig aus algorithmischer Perspektive. Interessanterweise sind wir durch eine *Black-Box-Transformation* in der Lage, alle Ergebnisse aus dem Modell ohne Fading zu übertragen. Hierbei verlieren wir nur einen Faktor von $O(\log^* n)$ im Approximationsfaktor. Das heißt, wir erreichen die ersten $O(\log^* n)$-Approximationen für *Capacity Maximization* und $O(\log n \cdot \log^* n)$-Approximationen für *Latency Minimization* im Rayleigh-Fading-Modell.

5 Sekundäre Spektrumsmärkte

Sekundäre Spektrumsmärkte sind ein möglicher Regulierungsmechanismus, um der Knappheit im Frequenzspektrum zu begegnen. In diesen Märkten werden Lizenzen für die Sekundärnutzung von aktuell ungenutzten Teilen des Spektrums verkauft. Diese Lizenzen gelten nur kurzzeitig und lokal; sie müssen deshalb regelmäßig automatisiert neu vergeben werden. Dabei ist Interferenz zwischen unterschiedlichen Sekundärnutzern zu berücksichtigen. Eine gängige Methode, um diese Märkte zu organisieren, sind Auktionen: Die möglichen Sekundärnutzer bieten auf Lizenzen für einzelne Teile des zur Verfügung gestellten Spektrums. Anschließend muss ein Mechanismus eine Zuordnung festlegen, so dass das Gemeinwohl (*social welfare*) maximiert wird.

Für unsere Betrachtungen dieses algorithmischen Problems nutzen wir eine Verallgemeinerung der bisherigen Interferenzmodelle. Wir nehmen an, dass die Interferenz über einen kantengewichteten Konfliktgraphen modelliert ist, dessen Knoten den Sekundärnutzern entsprechen. Eine Menge von Sekundärnutzern kann sich einen Kanal teilen, wenn sich für jeden Knoten das eingehende Kantengewicht der übrigen ausgewählten Knoten zu weniger als 1 aufsummiert.

Durch diese Modellierung als verallgemeinertes Independent-Set-Problem können die verschiedenen Varianten des oben beschriebenen SINR-Modells, aber auch eine Vielzahl weiterer Modelle dargestellt werden. Interessanterweise haben die dabei entstehenden Konfliktgraphen eine wichtige Gemeinsamkeit: Die *Inductive Independence Number* ρ [YB09] ist beschränkt durch eine Konstante oder eine schwach wachsende Funktion wie $O(\log n)$. Dies ermöglicht uns, die Nichtapproximierbarkeitsschranke von $\Omega(n^{1-\varepsilon})$ des Maximum-

Independent-Set-Problems auf allgemeinen Graphen [Hås99] zu umgehen.

Durch Randomisiertes Runden von LP-Lösungen erhalten wir eine $O(\rho \cdot \log n)$-Approximation für Maximum-Weight Independent Set auf kantengewichteten Konfliktgraphen. Dieser Algorithmus lässt sich auch auf das Szenario erweitern, in dem mehrere Kanäle zur Verfügung stehen. Wir erhalten unterschiedliche Approximationsfaktoren je nach Annahme, welche Struktur die Bewertungen der Nutzer haben, wenn diese mehrere Kanäle erhalten. Für k Kanäle insgesamt und keine weiteren Annahmen erhalten wir $O(\sqrt{k} \cdot \rho \cdot \log n)$ als Approximationsgarantie. Unter Bewertungsfunktionen, die allen Kanälen denselben Wert zurechnen, lässt sich dies auf $O(\rho \cdot (\log n + \log k))$ verbessern. Nimmt man stattdessen Submodularität an, erhält man für die wichtige Klasse der MRS-Bewertungen den Approximationsfaktor $O(\rho \cdot \log n)$.

Da es sich um eine Auktion handelt, ist davon auszugehen, dass sich die Nutzer als eigensinnige Bieter verhalten. Glücklicherweise können unsere Approximationsalgorithmen eingesetzt werden, um *Truthful-in-Expectation-Mechanismen* zu konstruieren. Diese stellen sicher, dass im Erwartungswert kein Bieter davon profitieren kann, eine unwahre Bewertung mitzuteilen. Hierzu setzen wir unter anderem das Framework von Lavi und Swamy [LS11] ein.

6 Dynamisches Scheduling

Als ein weiteres, komplexeres Problemszenario betrachten wir die Paketzustellung innerhalb eines Netzwerks. Wir nehmen an, dass über die Zeit verteilt Kommunikationsanfragen auftreten, die ausnahmslos zu erfüllen sind – mit möglichst geringen Wartezeiten. Für dieses Szenario verwenden wir eine andere Abstraktion als die oben genannten Konfliktgraphen, die uns nun erlaubt, verteilte Protokolle zu entwickeln. Wir führen ein stochastisches Modell und ein Worst-Case-Modell ein, um die Menge der auftretenden Anfragen zu quantifizieren und somit zu beschränken.

Ausgehend von Algorithmen für das entsprechende statische Scheduling-Problem konstruieren wir verteilte stabile Protokolle. Stabilität bedeutet in diesem Zusammenhang, dass die erwartete Zeit für ein Paket zwischen Ankunft und Auslieferung beschränkt ist. Die Transformation hin zu dynamischen Protokollen ist komplizierter als bei vergleichbaren früheren Ansätzen [SV00, RT96], da die statischen Algorithmen, die wir als Ausgangspunkt nutzen, nicht zwangsläufig linear skalieren, wenn man die Eingabeinstanz skaliert. Trotzdem sind wir in der Lage, einen Durchsatz zu garantieren, der so groß ist wie der des statischen Algorithmus.

Im SINR-Modell mit festen Sendeleistungen arbeitet unser Ansatz perfekt mit dem oben genannten verteilten Algorithmus für Latency Minimization zusammen. Für den Fall, dass der Algorithmus die Sendeleistungen wählen muss, kann prinzipiell auch der oben genannte, zentralisierte Algorithmus verwendet werden. Es fehlt einzig ein verteilter Algorithmus für das statische Problem, um auch hier ein verteiltes, stabiles Protokoll zu konstruieren. In allen genannten Fällen weicht der Durchsatz in Netzwerken der Größe m vom bestmöglichen Durchsatz um Faktoren der Größenordnung $O(1)$ bis $O(\log^2 m)$ ab.

7 Fazit und Ausblick

In dieser Arbeit haben wir einige Algorithmen für die fundamentalen Optimierungsprobleme im Zusammenhang mit SINR-Modellen vorgestellt. Bei vielen dieser Algorithmen handelt es sich um die ersten, die nicht-triviale Approximationen auf allen Instanzen garantieren können. Trotz dieses eigentlich theoretischen Ursprungs erweisen sich die Algorithmen auch in Simulationen als konkurrenzfähig.

Auf einer grundsätzlicheren Ebene haben wir das Verständnis für die Modelle verbessert und neue Techniken für den Umgang mit ihnen eingeführt. Wir haben dies an zwei komplexeren Problemszenarien verdeutlicht, in denen das tatsächliche Interferenzmodell nicht mehr von derart großer Bedeutung war und sich die Analysen stattdessen auf eine abstraktere algorithmische Fragestellung konzentrieren konnten.

Nichtsdestoweniger gibt es weiterhin viel Raum für Verbesserungen. Zum Beispiel könnte man nach Algorithmen mit besseren Approximationsfaktoren suchen. Alternativ könnte man zeigen, dass dies nicht bzw. nicht beliebig möglich ist. Bis jetzt gibt es kaum komplexitätstheoretische Ergebnisse zur Approximierbarkeit dieser Probleme.

Ein weiteres wichtiges Themengebiet ist Dezentralisierung. Für die meisten unserer Algorithmen nehmen wir an, die Positionen der Sender und die Interferenzbedingungen perfekt zu kennen. Plant man etwas Toleranz ein, reichen teilweise auch weniger präzise Daten. Trotzdem bleibt es eine offene Frage, wie viele Informationen in welcher Genauigkeit eigentlich erforderlich sind, um die Probleme zu lösen.

Die betrachteten SINR-Modelle sind deutlich realistischer als frühere Modelle. Dennoch berücksichtigen sie bei weitem noch nicht alle Aspekte, die für Funkübertragungen von Bedeutung sind. So ist es bislang nicht möglich, Hindernisse bei der Ausbreitung zu berücksichtigen. Dies scheitert bereits an der Tatsache, dass schon leichte Relaxierungen des Ausbreitungsmodells zu Nichtapproximierbarkeiten führen (siehe z. B. [Gou09]). Vergleichbares gilt auch für weitere unbeachtete Aspekte: In den meisten Fällen gibt es kein akzeptiertes Modell, das es erlaubt, die Effekte zu berücksichtigen, und gleichzeitig nichttriviale Approximationen zulässt.

Schließlich könnte es interessant sein, andere Zielfunktionen zu betrachten. In dieser Arbeit war immer das Ziel, den Gesamtdurchsatz des Netzwerks zu optimieren. Andere bedeutsame Aspekte wie Fairness oder Energieverbrauch wurden außer Acht gelassen. Es ist jedoch zu hoffen, dass mit den entwickelten Techniken auch derartige Problemstellungen zu lösen sind.

Literatur

[AD09] Matthew Andrews und Michael Dinitz. Maximizing capacity in arbitrary wireless networks in the SINR model: Complexity and game theory. In *Proceedings of the 28th Conference of the IEEE Communications Society (INFOCOM)*, Seiten 1332–1340, 2009.

[FKRV09] Alexander Fanghänel, Thomas Kesselheim, Harald Räcke und Berthold Vöcking. Ob-

livious interference scheduling. In *Proceedings of the 28th ACM Symposium on Principles of Distributed Computing (PODC)*, Seiten 220–229, 2009.

[Gou09] Olga Goussevskaia. *Computational Complexity and Scheduling Algorithms for Wireless Networks*. Dissertation, ETH Zurich, 2009.

[Hal09] Magnús M. Halldórsson. Wireless Scheduling with Power Control. In *Proceedings of the 17th annual European Symposium on Algorithms (ESA)*, Seiten 361–372, 2009.

[Hås99] Johan Håstad. Clique is hard to approximate within $n^{1-\varepsilon}$. *Acta Mathematica*, 182(1):105–142, 1999.

[HHMW13] Magnús M. Halldórsson, Stephan Holzer, Pradipta Mitra und Roger Wattenhofer. The Power of Non-Uniform Wireless Power. In *Proceedings of the 24th ACM-SIAM Symposium on Discrete Algorithms (SODA)*, Seiten 1595–1606, 2013.

[HM11] Magnús M. Halldórsson und Pradipta Mitra. Wireless Capacity with Oblivious Power in General Metrics. In *Proceedings of the 22nd ACM-SIAM Symposium on Discrete Algorithms (SODA)*, Seiten 1538–1548, 2011.

[Kes12] Thomas Kesselheim. *Approximation Algorithms for Spectrum Allocation and Power Control in Wireless Networks*. Dissertation, RWTH Aachen University, 2012.

[LS11] Ron Lavi und Chaitanya Swamy. Truthful and Near-Optimal Mechanism Design via Linear Programming. *Journal of the ACM*, 58(6):25:1–25:24, Dezember 2011.

[MW06] Thomas Moscibroda und Roger Wattenhofer. The Complexity of Connectivity in Wireless Networks. In *Proceedings of the 25th Conference of the IEEE Communications Society (INFOCOM)*, Seiten 1–13, 2006.

[Rap01] Theodore Rappaport. *Wireless Communications: Principles and Practice*. Prentice Hall PTR, 2nd. Auflage, 2001.

[RT96] Yuval Rabani und Éva Tardos. Distributed packet switching in arbitrary networks. In *Proceedings of the 28th annual ACM symposium on Theory of computing (STOC)*, Seiten 366–375, 1996.

[SV00] Christian Scheideler und Berthold Vöcking. From static to dynamic routing: Efficient transformations of store-and-forward protocols. *SIAM Journal on Computing*, 30(4):1126–1155, 2000.

[YB09] Yuli Ye und Allan Borodin. Elimination Graphs. In *Proceedings of the 36th International EATCS Colloquium on Automata, Languages and Programming (ICALP)*, Seiten 774–785, 2009.



Thomas Kesselheim wurde am 29. November 1984 in Würselen geboren. Er wuchs in Geilenkirchen auf. Nach dem Abitur begann er sein Studium der Informatik an der RWTH Aachen, das er 2009 mit dem Diplom abschloss. Im Anschluss war er Doktorand unter Prof. Dr. Berthold Vöcking am Lehrstuhl für Informatik 1 der RWTH im Exzellenzcluster *UMIC*. Im Jahr 2012 promovierte er zu dem Thema *Approximation Algorithms for Spectrum Allocation and Power Control in Wireless Networks*. Seit 1. Februar 2013 ist er DAAD-Postdoc-Stipendiat an der Cornell University, Ithaca, NY, USA.

Formale Verifikation von exogenen Koodinationsmodellen*

Sascha Klüppelholz

Institut für Theoretische Informatik
Technische Universität Dresden
sascha.klueppelholz@tu-dresden.de

Abstract: In dieser Arbeit wird ein ganzheitlicher Ansatz zur Modellierung, Analyse und Synthese paralleler Systeme vorgestellt, welcher auf ausgewählten, aus der Literatur bekannten Formalismen aufbaut. Ziel ist die systematische und stringente Einbettung von Koordinationsaspekten. Der hier beschriebene Ansatz erlaubt es, das operationelle Systemverhalten auf beliebiger Ebene des Hardware-/Softwarestacks sowie die Interaktion und das komplexe Zusammenspiel unterschiedlicher Teilsysteme verschiedener Ebenen zu beschreiben und mithilfe formaler Methoden zu analysieren. Aufgrund der Komplexität moderner Hardware- und Softwaresysteme wurde ein hierarchischer Ansatz gewählt, welcher es erlaubt die Beschreibung komplexen Systemverhaltens auf mehrere Teilsysteme geringerer Komplexität zu verteilen. Die Interaktion und Kommunikation zwischen den Komponenten basiert hierbei auf der exogenen und kanalbasierten Koordinationssprache Reo. Diese unterstützt eine klare Trennung der Berechnung, welche durch die Komponenten durchgeführt wird, und der Koordination, welche durch ein Netzwerk aus synchronen und asynchronen Kanälen sichergestellt wird.

1 Einleitung

Moderne Informations- und Kommunikationssysteme gewinnen in unserem täglichen Leben immer mehr an Bedeutung. Durch ihre zunehmende Präsenz, sowohl in der Arbeitswelt als auch im Privatleben, beeinflussen, verändern und prägen sie mehr und mehr Bereiche des gesellschaftlichen Zusammenlebens. Private Kommunikation, Geschäftsprozesse und menschliche Interaktion allgemein basieren verstärkt auf den Möglichkeiten, die die neuen Technologien bieten. Gleichzeitig erhöht sich unsere Abhängigkeit von Technologie insgesamt und damit unser Risiko für den Fall, dass Systeme nicht wie erwartet funktionieren. Gleichsam können wir beobachten, dass die Komplexität und damit die Fehleranfälligkeit der genutzten Technologie durch ihre Mobilität, Heterogenität und Vernetzung stetig zunimmt. Diese Beobachtungen unterstreichen die Forderung nach einer stärkeren Integration und dem systematischen Einsatz von formalen Verifikationsmethoden, welche bereits in der Entwicklungsphase eingesetzt werden können.

Im Bereich der formalen Verifikation existieren zahlreiche Modellierungsformalismen basierend auf Varianten von u.a. Petrinetzen [Pet77], Transitionssystemen [Kel76], Prozess-

*Englischer Titel der Dissertation: "Verification of Branching-Time and Alternating-Time Properties for Exogenous Coordination Models"

algebren [Hoa78, Mil89, MPW92], etc. sowie zahlreiche Verifikationsmethoden und Softwarewerkzeuge wie bspw. NuSMV [CCGR00], oder SPIN [Hol97]. Allerdings stellen viele Model Checking Tools nur recht einfache Eingabesprachen zur Verfügung, deren Ausdrucksstärke bzgl. der vorhandenen Koordinationmechanismen und Adaptivität recht eingeschränkt sind. In der vorliegenden Arbeit stehen diese Koordinationsmechanismen im Vordergrund, da ausdrucksstarke Koordinationssprachen einen kompositionellen und hierarchischen Systementwurf potenziell befördern. Zudem stellen wir fest, dass die Sichtweise bekannter Model Checking Werkzeuge oft eher zustandsbasiert als aktionsbasiert ist. Sie eignen sich daher nur bedingt zur expliziten Modellierung und Analyse von Koordinationsmechanismen. In der vorliegenden Arbeit wollen wir daher einen Ansatz vorstellen, welcher diesen Aspekt stärkt und dabei die zustandsbasierte und aktionsbasierte Sicht kombiniert. Hierbei adaptieren und erweitern wir aus der Literatur wohlbekannte Formalismen. Der Fokus liegt dabei auf Modellierungssprachen und auf auf alternierenden Logiken (bspw. [AHK02]) basierenden Verifikationsmethoden, die auf die Spezifikation und Analyse komponentenbasierter Systeme mit exogener Koordination zugeschnitten sind und so die Wiederverwendbarkeit und Austauschbarkeit von Subsystemen begünstigen. Unser Ansatz eignet sich daher besonders zur Integration in den kontinuierlichen Entwicklungs- und Wartungsprozess moderner Kommunikationssysteme. Der vorgestellte Ansatz, welcher die Modellierung, Analyse und Synthese paralleler Systeme umfasst, ist aufgrund des gewählten Abstraktionsniveaus potenziell geeignet Systemverhalten auf beliebiger Ebene des Hardware-/Softwarestacks sowie das ebenenübergreifende Zusammenspiel von (heterogenen) Teilsystemen zu beschreiben und zu analysieren. Hierbei besteht eine Herausforderung darin, einen möglichst eleganten, intuitiven, einfach zu erlernenden und möglichst ausdrucksstarken Formalismus zur Modellierung mit klar formal definierter Semantik bereitzustellen, welcher es aber gleichzeitig erlaubt formale Methoden zur Verifikation der Korrektheit einzusetzen. In Abschnitt 2 dieser Arbeit wird ein hybrider, auf zwei Eingabesprachen beruhender Modellierungsansatz vorgestellt, der auf die Spezifikation komponentenbasierter Systeme mit exogener Koordination zugeschnitten ist und dessen kompositionelle Semantik auf endlichen Automaten beruht. Die Sprachen ermöglichen so das hierarchische Modellieren komplexen Systemverhaltens durch schrittweises Verfeinern mittels Dekomposition (Top-down Entwurf) bzw. durch sukzessives Vereinigen von Teilsystemen mittels Aggregation (Bottom-up Entwurf). Eine weitere Herausforderung besteht darin, dass auch die zur Analyse eingesetzten formalen Methoden möglichst mächtig sein sollten, sodass sie den Nachweis aller relevanten Systemeigenschaften erlauben, während die (praktische) Komplexität der dazugehörigen algorithmischen Probleme in akzeptablen Schranken bleibt. Ein weiterer Beitrag dieser Arbeit sind daher die in Abschnitt 3 vorgestellten alternierenden Logiken und dazugehörigen Model Checking Algorithmen, welche speziell auf den gewählten Ansatz zugeschnitten sind und es erlauben die Korrektheit des Gesamtsystems, von Teilsystemen, sowie der verwendeten Koordinations- und Kommunikationsmechanismen nachzuweisen. Die beschriebenen Model Checking Algorithmen wurden im Rahmen der Doktorarbeit [Klü12] in unser Verifikationswerkzeug Vereofy [BKK12] integriert und in umfangreichen Fallstudien evaluiert. Vereofy verwendet die in dieser Arbeit vorgestellten Modellierungssprachen und wird in Abschnitt 4 näher beschrieben.

Gewählter Modellierungsansatz. Als Ausgangspunkt dieser Arbeit dient uns der komponentenbasierte Systementwurf, in dem komplexes Systemverhalten auf mehrere logische Einheiten aufgeteilt wird aus deren Zusammenspiel sich das Gesamtverhalten ergibt. Die logischen Einheiten nennen wir fortan Komponenten. Komponenten haben ein klar definiertes Interface, bestehend aus Ein-/Ausgabeports (I/O-Ports). Das in dieser Arbeit adressierte Abstraktionsniveau beschreibt das Verhalten der Komponenten in Bezug auf das nach außen sichtbare Ein-/Ausgabeverhalten an ihren I/O-Ports und ist daher prinzipiell geeignet, Einheiten auf beliebiger Ebene des Hardware-/Softwarestacks sowie deren Zusammenspiel zu beschreiben. Eine Komponente kann so auf Hardwareebene bspw. das I/O-Verhalten einer CPU oder eines Speichers beschreiben. Auf Softwareebene kann so mittels Komponenten z.B. das I/O-Verhalten eines bestimmten Objekts in Bezug auf Methodenaufrufe abgebildet werden. Der komponentenbasierte Systementwurf begünstigt insbesondere das hierarchische Systemdesign mittels Dekomposition bzw. Aggregation. Hierbei ist vor allem entscheidend auf welche Art Komponenten miteinander interagieren und kommunizieren. In der vorliegenden Arbeit verfolgen wir einen Ansatz welcher auf exogenen Koordinationssprachen beruht. Exogene Koordinationssprachen (bspw. Linda [GCCC85] oder PICCOLA [ALSN01]) erlauben eine klare Trennung von Berechnungsaspekten, die typischerweise innerhalb der Komponenten gelagert sind, und Koordinationsaspekten, die außerhalb der Komponenten in der Form von "glue code" gegeben sind. Diese klare Trennung der Koordinationsaspekte von den Berechnungsaspekten unterstützt die Wiederverwendbarkeit und Austauschbarkeit von Komponenten und Kommunikationsstrukturen sowie den hierarchischen Systementwurf insgesamt.

Zur Beschreibung des I/O-Verhaltens von Komponenten stützen wir uns in dieser Arbeit auf Constraint Automata (CA) [BSAR06]. CA sind eine Variante von Transitionssystemen, in denen die Zustandsübergänge mit Bedingungen, so genannten "constraints", beschriftet sind, die zum einen die Menge der aktiven I/O-Ports und zum anderen den beobachtbaren Datenfluss an den I/O-Ports beschränken. Zur Beschreibung der Koordinationsmechanismen verwenden wir die kanalbasierte, exogene Koordinationsprache Reo [Arb04], deren Praktikabilität bereits in einem breiten Spektrum von Anwendungen nachgewiesen wurde (vgl. bspw. [KA09, MA10]). Die operationelle formale Semantik von Reo kann selbst wieder in CA-Semantik angegeben werden. Daraus ergibt sich die Kompositionalität unseres gesamten gewählten Ansatzes. Reo Kanäle, Netzwerke und die Komponenten selbst werden als CA beschrieben, die mittels Produktbildung auf Automatenebene miteinander komponiert werden. Unabhängig davon ob er für das Verhalten eines einzelnen Reo Kanals, eines Netzwerks, einer Komponente oder des Gesamtsystems steht, dient der CA als Ausgangspunkt für die formale Verifikation. Im nächsten Abschnitt stellen wir Modellierungssprachen vor, deren Semantik auf endlichen, um Polarität und Datentypen erweiterten CA definiert ist und die zur Modellierung komponentenbasierter mit exogener Koordination verwendet werden können.

2 Modellierungssprachen

Zur Modellierung komponentenbasierter Systeme mit exogener Koordination stellen wir in diesem Abschnitt einen hybriden Modellierungsansatz vor, welcher auf den Sprachen CARML und RSL basiert, deren formale operationelle Semantik über CA definiert ist. Die Kombination beider Sprachen ermöglicht den kompositionellen und hierarchischen

Systementwurf und begünstigt so die Wiederverwendbarkeit und Austauschbarkeit sowohl einzelner Komponenten als auch der verwendeten Kommunikationsmechanismen. Die erste Modellierungssprache CARML (Constraint Automata Reactive Modules Modeling Language) ist eine guarded-command Sprache [Dij76], welche durch reactive modules [AH99] inspiriert ist und hauptsächlich dazu dient das Interface, sprich die vorhandenen I/O-Ports, sowie das nach außen sichtbare, schrittweise Ein-/Ausgabeverhalten einzelner, atomarer Komponenten und Kanäle zu beschreiben. Die zweite Modellierungsspache RSL (Reo Scripting Language) ist eine durch die Koordinationssprache Reo inspirierte Skriptsprache mit deren Hilfe sich die (ggf. dynamisch veränderliche) Struktur eines zu analysierenden Systems beschreiben lässt. Die wichtigsten Operatoren dienen daher dem Erzeugen und Komponieren neuer Instanzen von Reo Kanälen und Komponenten, sowie der Beschreibung dynamischer Netzwerkstukturen, die sich je nach Konfiguration des Netzwerks verändern können. In den nachfolgenden Abschnitten beschreiben wir das Grundkonzept beider Sprachen.

Syntax von CARML/RSL. Ein CARML Modul beschreibt das Verhalten einer einzelnen Komponente und besteht aus drei Teilen, in denen das Interface, die lokalen Variablen sowie das operationelle Verhalten der Komponente angeben sind. CARML Module (sowie RSL Skripte) können parametrisiert deklariert sein. Hierbei dienen Parameter Θ, Ω, Π und Υ als Platzhalter für Datentypen, Funktionen, Prädikate und Variablen innerhalb der Modul- bzw. Netzwerkdefinition. Zum Zeitpunkt der Instantiierung müssen die uninterpretierten Symbole für benutzerdefinierte Datentypen, Funktionen, Prädikate und Variablen übergeben und damit aufgelöst werden. Im oberen Teil eines CARML Moduls werden zunächst die I/O-Ports mit assoziiertem Datentyp angegeben, welche das Interface der beschriebenen Komponente (bzw. Kanals) definieren. Jedes CARML Modul kann eine Menge von lokalen Variablen unterschiedlichen Datentyps enthalten, welche den Zustandsraum des zugrundeliegenden CA ausmachen. Die angegebenen Initialwerte lokaler Variablen deklarieren die Startzustände des CA. Das eigentliche operationelle Verhalten wird in Form von dreiteiligen guarded commands, bestehend aus einem *state_guard*, einem *I/O_guard* und einem *state_assignment*, angegeben. Ein *state_guard* ist eine Konjunktion von Bedingungen über Belegungen der lokalen Variablen, ein *I/O-guard* eine Konjunktion von Bedienungen an den am Interface observierbaren Datenfluss und ein *state_assignment* beschreibt den Effekt auf die lokalen Variablen nachdem eine entsprechende Transition gefeuert hat. Die im Mittelteil angegeben atomaren Präpositionen dienen der vereinfachten Darstellung von Transitionsdefinitionen sowie von Formeln.

Ein RSL Skript erlaubt innerhalb von Statements die Verwendung der durch Reo inspirierten Basisoperatoren zur Instantiierung (*new*) und Komposition (*join*) zum Erzeugen bzw. Verbinden zuvor von in CARML bzw. RSL beschriebenen Komponenten und Kanälen. Diese können kombiniert werden mit Skriptelementen wie bedingten Anweisungen, Schleifen, etc.. Durch das Ausführen eines RSL Skripts entsteht sukzessive das beschriebene Gesamtsystem. Zunächst wird im oberen Abschnitt eines RSL Skripts der statische Teil des Netzwerks sowie dessen Interface angegeben. Darüber hinaus kann eine endliche Anzahl von Topologien definiert werden, zwischen denen das Netzwerk potenziell dynamisch wechseln kann. Der Übergang zwischen Topologien wird hierbei zunächst als vollständig nicht-deterministisch angenommen, kann aber von außen durch das Verbinden einer neuen in CARML oder RSL beschriebenen Controller-Komponente eingeschränkt bzw. terminiert werden.

Semantik von CARML/RSL. Die operationelle Semantik von CARML und RSL basiert auf um Datentypen und Polarität der I/O-Ports erweiterte CA mit zugehörigem Produktoperator, sowie eines Operators (*hide*) zum Abstrahieren interner Berechnungsschritte innerhalb von Teilsystemen. Während die formale, operationelle Semantik eines CARML Moduls unmittelbar durch Angabe eines Automaten definiert ist, ergibt sich das operationelle Verhalten eines in RSL beschriebenen Systems aus der sukzessiven Produktbildung der Automaten aller Kanäle eines Netzwerks sowie der ggf. verbundenen Komponenten. Die gemeinsame unterliegende Semantik von CARML und RSL erlaubt es nun komplexe, mit RSL komponierte Teilsysteme als Bausteine zu verwenden und auf einer höheren Beschreibungsebene ggf. mehrfach neu zu instantiieren und komponieren.

3 Die temporalen Logiken ASL und BTSL

In diesem Abschnitt stellen wir temporale Logiken mit dazugehörigen Model Checking Verfahren vor, mit deren Hilfe sich das gewünschte Verhalten einzelner Komponenten, Koordinationsstrukturen sowie des Gesamtsystems spezifizieren und verifizieren lässt. Die Logiken sind auf den komponentenbasierten Systementwurf mit Reo und CA zugeschnitten und erlauben es, sowohl auf den internen Zustand von Teilsystemen und Netzwerkstrukuren, als auch auf den observierbaren Datenfluss an den Interfaceports Bezug zu nehmen. So kombiniert und erweitert die Logik BTSL die aus CTL [CE81, CGP99] bekannten branching-time Operatoren zur Qualifizierung über Pfade mit aus anderen Logiken, wie PDL [FL79] und TDSL (*timed data stream logic*) [ABdBR04, CCA04] bekannten Operatoren zur Quantifizierung über I/O-Präfixe. Letztere werden durch Angabe eines endlichen Automaten $\mathcal{Z}$ beschrieben und charakterisieren so den an den Interfaceports beobachtbaren Datenfluss. Die zweite temporale Logik ASL ist eine durch ATL [AHK02] inspirierte alternating-time Logik. Sie beruht auf einer Interpretation von komponentenbasierten Systemen als Zweiparteienspiel. Hierbei können Komponenten Koalitionen bilden um gewisse temporale Pfadeigenschaften zu erzwingen. ASL umfasst hierbei die aus BTSL bekannten Modalitäten zur Quantifizierung über I/O-Präfixe. Die Logik BTSL ist insbesondere eine Teillogik von ASL und bezieht ebenfalls die Betrachtung endlichen Systemverhaltens mit ein.

ASL Syntax und Semantik. Die nachfolgende Grammatik beschreibt die Syntax von ASL Zustandsformeln (bezeichnet mit Φ) sowie ASL Pfadformeln (bezeichnet mit φ):

$$\begin{aligned} \Phi &::= \quad \mathsf{true} \mid a \mid \Phi_1 \wedge \Phi_2 \mid \neg\Phi \mid \mathbb{E}_N\varphi \mid \mathbb{A}_N\varphi \\ \varphi &::= \quad \langle\mathcal{Z}\rangle\Phi \mid [\![\mathcal{Z}]\!]\Phi \mid \Phi_1 \,\mathrm{U}\, \Phi_2 \mid \Phi_1 \,\mathrm{R}\, \Phi_2 \end{aligned}$$

Hier ist $N \subseteq \mathcal{N}$ eine Menge der von einer Koalition kontrollierbaren I/O-Ports, $a \in AP$ eine atomare Präposition und $\mathcal{Z} = \langle Z, \Sigma, \longrightarrow_{\mathcal{Z}}, Z_0, Z_F\rangle$ ein (nicht-deterministischer) endlicher Automat (NEA) mit Akzeptanzmenge $Z_F \subseteq Z$.

Die Interpretation der Modalität $\mathbb{E}_N\varphi$ ist, dass es eine N-Strategie gibt, welche ausschließlich das Verhalten an den I/O-Ports in N beeinflussen kann, sodass, wenn die Strategie angewendet wird, ausschließlich Pfade erhalten bleiben, welche die Pfadformel φ erfüllen. Formal ist eine N-Strategie eine Funktion die jedem endlichen Lauf in einem CA eine Menge von I/O-Operationen inkl. eines speziellen Symbols $\surd$ zuordnet, welches signali-

siert, dass das Stoppen eine mögliche Wahl der Strategie ist. Eine Nebenbedingung ist, dass die N-Strategie jedes Verhalten erhalten muss, welches als nicht-kontrollierbar angesehen wird. Der Operator $\mathbb{E}_N$ steht somit für die Existenzquantifizierung über N-Strategien, während der duale Operator $\mathbb{A}_N\varphi$ für die Allquantifizierung steht.

Ein Pfad π im CA erfüllt $\langle\!\langle\mathcal{Z}\rangle\!\rangle\Phi$, falls es ein Präfix η des Pfades gibt, sodass der beobachtbare Datenfluss in der durch $\mathcal{Z}$ charakterisierten Sprache liegt und η in einem Zustand endet der Φ erfüllt. Damit dient die Pfadmodalität $\langle\!\langle\mathcal{Z}\rangle\!\rangle\Phi$ der Existenzquantifizierung über I/O-Präfixe, während der duale Operator $[\![\mathcal{Z}]\!]\Phi$ die Allquantifizierung über I/O-Präfixe erlaubt. Ein Pfad π in $\mathcal{A}$ erfüllt $[\![\mathcal{Z}]\!]\Phi$, falls jedes Präfix η dessen beobachtbarer Datenfluss in der durch $\mathcal{Z}$ charakterisierten Sprache liegt in einem Zustand endet der Φ erfüllt. Die Standard Modalitäten für die Quantifizierung über Pfade und damit die Teillogik BTSL, wie sie in [KB09] beschrieben wurde, erhält man mithilfe der Modalitäten $\mathbb{E}_N$ und $\mathbb{A}_N$ mit $N = \emptyset$, also unter der Annahme, dass $\emptyset$-Strategien kein Verhalten entfernen können: $\forall\varphi \stackrel{\text{def}}{=} \mathbb{E}_\emptyset\varphi$ sowie $\exists\varphi \stackrel{\text{def}}{=} \mathbb{A}_\emptyset\varphi$. Die verbleibenden Modalitäten haben die erwartete Standardsemantik.

ASL und BTSL Model Checking. Die Model Checking Algorithmen mit deren Hilfe sich entscheiden lässt, ob ein als CA gegebenes System $\mathcal{A}$ eine ASL Formel erfüllt, basieren im wesentlichen auf Fixpunktberechnungen innerhalb von $\mathcal{A}$ bzw. innerhalb eines Produktautomaten, welcher aus der Parallelschaltung von $\mathcal{A}$ und $\mathcal{Z}$ entsteht. Die Basisoperationen der Fixpunktberechnungen sind spezielle Operatoren zum Berechnen von Mengen von Vorgängerzuständen im CA bzw. im Produktsystem. Abbildung 1 zeigt die Behandlung von ASL Zustandsformeln der Form $\mathbb{E}_N\langle\!\langle\mathcal{Z}\rangle\!\rangle\Phi$. Gesucht ist hier eine erweiterte $N\cup\{A_\surd\}$-Strategie, bestehend aus "erzwingbaren Schritten" im Produktsystem, welche sicherstellt einen Zustand zu erreichen, der zum einen Φ erfüllt und gleichzeitig akzeptierend in $\mathcal{Z}$ ist. Der zusätzliche Port $A_\surd$ wird als kontrollierbar angenommen und dient dazu die Option des Anhaltens explizit zu machen. Die rechte Seite von Abbildung 1 zeigt analog die Behandlung von ASL Formeln der Form $\mathbb{E}_N[\![\mathcal{Z}]\!]\Phi$. Zur algorithmischen Behandlung nehmen wir an, dass $\mathcal{Z}$ als deterministischer endlicher Automat (DEA) gegeben ist bzw. zunächst vorab determinisiert wurde.

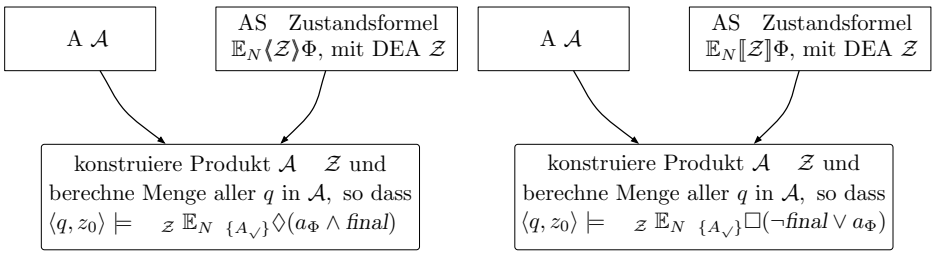


Abbildung 1: Schema für die Behandlung von $\mathbb{E}_N\langle\!\langle\mathcal{Z}\rangle\!\rangle\Phi$ und $\mathbb{E}_N[\![\mathcal{Z}]\!]\Phi$

Komplexitätsbetrachtung. Die Zeitkomplexität der im vorherigen Absatz vorgestellten Algorithmen ist polynomiell in der Größe von $\mathcal{A}$ und exponentiell in der Größe des NEA $\mathcal{Z}$, wobei sich die Größe auf die Anzahl der Knoten und Kanten in $\mathcal{A}$ bzw. $\mathcal{Z}$ bezieht. Damit liegen die dazugehörigen Model Checking Probleme in der Komplexitätsklasse

EXPTIME. Tatsächlich sind sowohl das ASL als auch BTSL Model Checking Problem PSPACE-vollständig [Klü12].

4 Vereofy

Vereofy ist ein Softwarewerkzeug zur formalen Verifikation von komponentenbasierten Systemen, welches an unserem Lehrstuhl an der Technischen Universität Dresden entwickelt wurde. In Vereofy nutzen wir die in Abschnitt 2 vorgestellten Modellierungssprachen CARML und RSL zur Beschreibung des Systemverhaltens. Um dem Problem der Zustandsraumexplosion entgegen zu wirken verwendet Vereofy eine auf Schaltfunktionen und Binären Entscheidungsgraphen (BDDs) [Bry86] basierende, symbolische Darstellung zur effizienten Repräsentation der zu analysierenden CA. Die Implementierung beruht daher ebenfalls auf symbolischen Varianten der im vorherigen Abschnitt vorgestellten Model Checking Algorithmen. Vereofy selbst ist in C++ programmiert und lässt sich sowohl unter Mac OS X, Linux als auch Windows kompilieren und ausführen. Darüber hinaus existiert ein Ecplise Plugin für die am Centrum Wiskunde & Informatica (CWI) in Amsterdam entwickelten *Extensible Coordination Tools* (ECT) (vgl. bspw. [Kra11]), einer graphischen Benutzerschnittstelle zum Erstellen komponentenbasierter Systeme mit Anbindung an zahlreiche Analyse- und Synthesewerkzeuge.

Hauptmerkmale von Vereofy. Zur Modellierung werden die Sprachen CARML und RSL verwendet. Um das Modellieren zu erleichtern existieren zahlreiche zusätzliche Sprachkonzepte und Erweiterungen der zuvor vorgestellten Basissprachen, wie z.B. Funktionen, Enumeratoren, bedingte Codeabschnitte, Transitionslabels, u.v.m.. Eine vollständige Übersicht und Dokumentation aller Sprachkonzepte CARML und RSL befindet sich im Benutzerhandbuch [BKK12] von Vereofy.[1] In der vorinstallierten Bibliothek gibt es bereits zahlreiche nützliche CARML Module und RSL Skripte für Kanäle, Koordinationsnetzwerke sowie Komponenten aus denen sich sehr einfach und schnell komplexe Systeme erstellen lassen. Eigene Bausteine können nutzerseitig zu neuen Bibliotheken zusammengefasst werden, welche fortan ebenfalls zur Instantiierung und Komposition bereitstehen. Zum detaillierten Verständnis der erstellten Systemmodelle können Automaten und Netzwerkstrukturen exportiert werden. Hierfür existiert neben einer Exportfunktion in das GraphViz Format[2] auch die Möglichkeit CARML und RSL Programme automatisch in das XML Format für ECT zu konvertieren. Umgekehrt können ECT Spezifikationen in CARML und RSL Programme konvertiert werden. Intern werden CA mithilfe von Entscheidungsgraphen repräsentiert. Hierfür verwendet Vereofy die BDD-Bibliothek JINC [Oss10]. Vereofy unterstützt auf unsere Anwendung zugeschnittene dynamische Umordnungsverfahren und Heuristiken zum Erzeugen geeigneter BDD-Variablenordnungen sowie Techniken zum Speichern und Laden von Variablenordnungen. Zur Analyse stehen in Vereofy neben Simulation mittels Erzeugen zufälliger Pfade und den in Abschnitt 3 vorgestellten Model Checking Verfahren auch ein linear-time Model Checker sowie ein Bisimulation Checker zur Verfügung [BBKK09, BKK11]. Die Model Checker geben wann immer möglich einen Hinweis in Form eines Gegenbeispiels bzw. eines Zeugen aus welchem Grund eine Formel (nicht) erfüllt ist. Im Fall von ASL Zustandsformeln der Form

[1] Die Veröffentlichung einer neuen Version von Vereofy ist für die zweite Jahreshälfte 2013 vorgesehen.
[2] `http://www.graphviz.org/`

$\exists\varphi$ bzw. $\forall\varphi$ sind dies Pfade und im Fall von ASL Zustandsformeln der Form $\mathbb{E}_N\varphi$ bzw. $\mathbb{A}_N\varphi$ Strategien in Form von Automaten. Pfade können in der Konsole ausgegeben werden oder in ECT dargestellt und animiert werden. Strategien können angewendet und das Systemverhalten unter Anwendung der automatisch erzeugten Strategie verifiziert werden.

Zur praktischen Evaluation der in Vereofy implementierten Model Checking Verfahren wurden diese in zahlreichen Fallbeispielen systematisch untersucht. Die Klasse der untersuchten Systemmodelle reicht von einfachen Spielzeugbeispielen, Kommunikationsprotokollen, Spielen bis hin zu kleineren industriellen Fallstudien, wie bspw. die Untersuchung eines Routingprotokolls [BBK+10] im Kontext von Sensornetzwerken und die Analyse einer Kommunikationsplattform [KKSB11]. Insgesamt zeigen die Ergebnisse [Klü12] die generelle Praktikabilität des vorgestellten Ansatzes zur Modellierung, Analyse und Synthese moderner Kommunikationssysteme. Allgemeine Voraussagen bzgl. der Anwendbarkeit und Effizienz sind gerade aufgrund der symbolischen Repräsentation der CA schwer möglich. Es lässt sich aber feststellen, dass sich für regulär strukturierte, statische Systeme, wie etwa ein Protokoll für speisende Philosophen, Zustandsräume mit mehr als 10^{300} erreichbaren Zuständen aufbauen und analysieren lassen. Im Fall von weniger regulär strukturierten Systemen mit komplexeren Daten und dynamischen Verhaltensanpassungen sind es immerhin noch Zustandsräume mit 10^{30} und mehr Zuständen. Mit wachsender Komplexität der zu analysierenden Systeme wächst gleichsam der Bedarf an fortgeschrittenen (automatischen) Abstraktionstechniken, Heuristiken, und kompositionellen Verifikationsmethoden, die diese Grenzen weiter verschieben. Darüber hinaus werden auch quantitative Erweiterung des beschriebenen Ansatzes, wie z.B. Erweiterungen um Echtzeit und Probabilismus, Gegenstand zukünftiger Arbeit sein.

5 Zusammenfassung

In der vorliegenden Arbeit wurde ein ganzheitlicher Ansatz zur Modellierung, Analyse und Synthese komponentenbasierter Systeme vorgestellt. Dieser besteht zum einen aus den beiden Modellierungssprachen CARML und RSL, deren formale operationelle Semantik auf CA beruht. Das gewählte Abstraktionsniveau erlaubt es, das Interfaceverhalten beliebiger Einheiten des Hardware-/ Softwarestacks sowie deren ebenenübergreifendes Zusammenspiel hierarchisch zu modellieren. Neben den Modellierungssprachen wurden die temporalen Logiken BTSL und ASL vorgestellt, die auf den gewählten Ansatz mit Reo und CA zugeschnitten sind und es erlauben branching-time sowie alternating-time Eigenschaften zu spezifizieren, welche sowohl auf den internen Zustand von Komponenten als auch auf den Datenfluss und die Koordinationsmechanismen zwischen Komponenten Bezug nehmen können. Beide Logiken beziehen die Betrachtung endlichen Systemverhaltens mit ein. In der Komplexitätsbetrachtung wurde die PSPACE-Vollständigkeit des Model Checking Problems sowohl für ASL als auch für BTSL nachgewiesen. Zur praktischen Evaluation der vorgeschlagenen Modellierungssprachen und der Model Checking Algorithmen wurden diese in Vereofy integriert und in zahlreichen Fallbeispielen systematisch untersucht. Das Softwarewerkzeug Vereofy selbst wird aktuell in verschiedene Lehrveranstaltungen unserer Arbeitsgruppe eingesetzt und weiterentwickelt. Darüber hinaus ist die Weiterentwicklung von Vereofy im Rahmen von verschiedenen Forschungsprojekten vorgesehen.

Literatur

[ABdBR04] F. Arbab, C. Baier, F. S. de Boer und J.J.M.M. Rutten. Models and Temporal Logics for Timed Component Connectors. *Proc. SEFM'04*, 0:198–207, 2004.

[AH99] R. Alur und T.A. Henzinger. Reactive Modules. *Formal Methods in System Design*, 15(1):7–48, 1999.

[AHK02] R. Alur, T.A. Henzinger und O. Kupferman. Alternating-time temporal logic. *Journal of the ACM*, 49(5):672–713, 2002.

[ALSN01] F. Achermann, M. Lumpe, J.-G. Schneider und O. Nierstrasz. *PICCOLA—a small composition language, Formal methods for distributed processing*, Seiten 403–426. Cambridge University Press, New York, NY, USA, 2001.

[Arb04] F. Arbab. Reo: A Channel-Based Coordination Model for Component Composition. *MSCS*, 14(3):329–366, 2004.

[BBK+10] C. Baier, T. Blechmann, J. Klein, S. Klüppelholz und W. Leister. Design and Verification of Systems with Exogenous Coordination using Vereofy. In *Proc. ISoLA'10*, Jgg. 6416 of *LNCS*, Seiten 97–111. Springer, 2010.

[BBKK09] C. Baier, T. Blechmann, J. Klein und S. Klüppelholz. Formal Verification for Components and Connectors. In *Proc. FMCO'08*, Jgg. 5751 of *LNCS*, Seiten 82–101. Springer, 2009.

[BKK11] C. Baier, J. Klein und S. Klüppelholz. Modeling and Verification of Components and Connectors. In *Proc. SFM'11*, Jgg. 6659 of *LNCS*, Seiten 114–147. Springer, 2011.

[BKK12] T. Blechmann, J. Klein und S. Klüppelholz. *Vereofy User Manual*. TU Dresden, Germany, 2008–2012. http://www.vereofy.de.

[Bry86] R.E. Bryant. Graph-Based Algorithms for Boolean Function Manipulation. *IEEE Transactions on Computers*, 35:677–691, 1986.

[BSAR06] C. Baier, M. Sirjani, F. Arbab und J.J.M.M. Rutten. Modeling Component Connectors in Reo by Constraint Automata. *SCP*, 61(2):75–113, 2006.

[CCA04] D. Clarke, D. Costa und F. Arbab. Modelling Coordination in Biological Systems. In *Proc. ISoLA'04*, Jgg. 4313 of *LNCS*, Seiten 9–25. Springer, 2004.

[CCGR00] A. Cimatti, E.M. Clarke, F. Giunchiglia und M. Roveri. NuSMV: a new symbolic model checker. *International Journal on Software Tools for Technology Transfer*, 2(4):410–425, 2000.

[CE81] E.M. Clarke und E.A. Emerson. Design and Synthesis of Synchronization Skeletons Using Branching-Time Temporal Logic. In *Proc. Workshop on Logic of Programs'81*, Jgg. 131 of *LNCS*, Seiten 52–71. Springer, 1981.

[CGP99] E.M. Clarke, O. Grumberg und D. Peled. *Model Checking*. MIT Press, 1999.

[Dij76] E.W. Dijkstra. *A Discipline of Programming*. Prentice-Hall, 1976.

[FL79] M.J. Fischer und R.J. Ladner. Propositional dynamic logic of regular programs. *Journal of Computer and System Science*, 8:194–211, 1979.

[GCCC85] D. Gelernter, N. Carriero, S. Chandran und S. Chang. Parallel Programming in Linda. In *Proceedings of the International Conference on Parallel Processing (ICPP'85)*, Seiten 255–263, 1985.

[Hoa78] C.A.R. Hoare. Communicating sequential processes. *Communications of the ACM*, 21(8):666–677, 1978.

[Hol97] G.J. Holzmann. The model checker SPIN. *IEEE Transactions on Software Engineering*, 23(5):279–295, 1997.

[KA09] N. Kokash und F. Arbab. Applying Reo to service coordination in long-running business transactions. In *Proc. SAC'09*, Seiten 1381–1382. ACM, 2009.

[KB09] S. Klüppelholz und C. Baier. Symbolic model checking for channel-based component connectors. *SCP*, 74(9):688–701, 2009.

[Kel76] R.M. Keller. Formal verification of parallel programs. *Communications of the ACM*, 19(7):371–384, 1976.

[KKSB11] J. Klein, S. Klüppelholz, A. Stam und C. Baier. Hierarchical modeling and formal verification. An industrial case study using Reo and Vereofy. In *Proc. FMICS'11*, Jgg. 6959 of *LNCS*, Seiten 228–243. Springer, 2011.

[Klü12] S. Klüppelholz. *Verification of Branching-Time and Alternating-Time Properties for Exogenous Coordination Models*. Dissertation, TU Dresden, Germany, 2012.

[Kra11] C. Krause. *Reconfigurable Component Connectors*. Dissertation, Leiden University, The Netherlands, 2011.

[MA10] S. Meng und F. Arbab. A Model for Web Service Coordination in Long-Running Transactions. In *Proc. SOSE'10*, Seiten 121–128, 2010.

[Mil89] R. Milner. *Communication and Concurrency*. Prentice-Hall, 1989.

[MPW92] R. Milner, J. Parrow und D. Walker. A calculus of mobile processes. *Information and Computation*, 100:1–40, 1992.

[Oss10] J. Ossowski. *JINC - A Multi-Threaded Library for Higher-Order Weighted Decision Diagram Manipulation*. Dissertation, Universität Bonn, 2010.

[Pet77] C.A. Petri. Non-sequential processes. GMD-ISF Report ISF-77-05, GMD, Sankt Augustin, 1977.



Foto: get-shot.de

Sascha Klüppelholz wurde am 21. Oktober 1976 in Haan (Rheinland) geboren. Er studierte Informatik an der Rheinischen Friedrich-Wilhelms-Universität Bonn und schloss das Studium 2005 als Diplom Informatiker ab. Im März 2012 verteidigte er seine Promotion in Theoretischer Informatik an der Technischen Universität Dresden mit Auszeichnung "summa cum laude". Er war während seiner Promotion zeitweise Stipendiat in der Promotionsförderung des Begabtenförderungswerks Villigst e.V. und arbeitet aktuell als wissenschaftlicher Mitarbeiter am Lehrstuhl für Algebraische und Logische Grundlagen der Informatik an der TU Dresden. Dort ist er u.a. eingebunden in Arbeiten im SFB 912 HAEC und des Exzellenzclusters cfAED. Darüber hinaus ist er assoziiertes Mitglied des Graduiertenkollegs RoSI zu rollenbasierten Software-Infrastrukturen und einer der Hauptentwickler von Vereofy.

Lernen Motorischer Fähigkeiten: Von Algorithmen zu Roboter-Experimenten *

Jens Kober

CoR-Lab - Universität Bielefeld
Honda Research Institute Europe
jkober@cor-lab.uni-bielefeld.de

Abstract: In dieser Doktorarbeit werden Ansätze diskutiert, die es Robotern ermöglichen, motorische Fähigkeiten zu erlernen. Motorische Fähigkeiten können oft durch Motor-Primitive, die elementare Bewegungen kodieren, dargestellt werden. Es gab schon eine Reihe von erfolgreichen Anwendungen des Erlernens von Motor-Primitiven durch überwachtes Lernen. Allerdings sind viele interessante motorische Lernprobleme hochdimensionale Reinforcement-Learning-Probleme (bestärkendes Lernen), die oft außerhalb der Anwendbarkeit der aktuellen Reinforcement-Learning-Methoden liegen. Diese Doktorarbeit leistet einen Beitrag zum Stand der Technik in Reinforcement-Learning, angewandt auf die Robotik, sowohl durch neuartige Algorithmen als auch durch neuartige Anwendungen. Gezeigt wird, wie motorische Fähigkeiten auf drei verschiedenen Ebenen gelernt werden können. Alle vorgeschlagenen Ansätze wurden ausgiebig mit Aufgaben wie u. a. einem Becherspiel, Darts, Tischtennis oder einem Wurfspiel in der Simulation und auf realen Robotern validiert.

1 Einführung

Seit Issac Asimov in den 1940er Jahren begann Kurzgeschichten über Roboter zu schreiben, werden Roboter von der Öffentlichkeit als potentielle Haushaltshilfen, Begleiter und Soldaten angesehen. Science-Fiction-Filme zeigen Roboter sowohl als Freunde als auch als Feinde der Menschheit, aber in beiden Fällen liegen deren Fähigkeiten weit über den Fähigkeiten der aktuellen realen Roboter. Simon [Sim65], einer der Pioniere der künstlichen Intelligenz (KI), behauptete, dass „Maschinen innerhalb von zwanzig Jahren in der Lage sein werden, jegliche Arbeit, die ein Mensch verrichten kann, zu erledigen." Solche über-optimistischen Versprechen führten dazu, dass heutige Prognosen eher konservativ ausfallen. Im Moment werden Roboter langsam Teil unseres täglichen Lebens in Form von Spielzeugen und Haushaltshilfen, wie autonome Staubsauger, Rasenmäher und Fensterputzer. Die meisten anderen Roboter sind noch auf Forschungslabore und industrielle Umgebungen beschränkt. Viele Aufgaben des täglichen Lebens können nur sehr langsam von einem Roboter verrichtet werden und die Fähigkeit zur Verallgemeinerung ist oft sehr begrenzt. Daher sind alle diese Systeme noch weit von den Erwartungen, die von Literatur

*Englischer Titel der Dissertation: "Learning Motor Skills: From Algorithms to Robot Experiments" [Kob12]



Abbildung 1: Diese Abbildung illustriert die Verallgemeinerung eines Rückhand-Motor-Primitives. Der Roboter verwendet jeweils dasselbe Motor-Primitiv, um auf Bälle an unterschiedlichen Positionen mit unterschiedlichen Geschwindigkeiten zu reagieren. Hierfür werden nur die Meta-Parameter des Motor-Primitives angepasst.

und Filmen geweckt werden, als auch von den Träumen der KI-Forscher entfernt.

Insbesondere in Japan wurde die Notwendigkeit von Haushalts-Robotern aufgrund der Alterung der Bevölkerung erkannt. Eine der wichtigsten Herausforderungen ist, mit sich ändernden Situationen in einer von Menschen und Robotern geteilten Umgebung umzugehen (z. B. umgestellte Möbel, wechselnde Lichtverhältnisse, kooperative Aufgaben) und die Notwendigkeit, sich den individuellen Anforderungen und Erwartungen der menschlichen Besitzer anzupassen. Die meisten aktuell käuflich erwerblichen Produkte verfolgen entweder einen Universal-Ansatz, der oft nicht optimal ist (z. B. Staubsauger-Roboter, die ihre Umgebung nicht wahrnehmen, sondern einen Algorithmus verwenden, der auf Hindernisse reagiert und der eine Abdeckung des gesamten Bodens garantiert [Bot12]) oder einen Ansatz, der einen Setup-Schritt entweder in Software (z. B. Eingabe eines Raumplans) oder in Hardware (z. B. Anbringen von Markern) erfordert. Als Alternative könnte man sich ein selbst-lernendes System vorstellen.

Diese Doktorarbeit behandelt keine Navigations-Probleme, sondern konzentriert sich auf das Erlernen von motorischen Fähigkeiten [Wul07]. In erster Linie werden Aufgaben betrachtet, bei denen das dynamische Verhalten des Roboters und seiner Umgebung berücksichtigt werden muss und wo ein kinematischer Bewegungsplan nicht ausreichend ist. Motorische Fähigkeiten können oft durch Motor-Primitive dargestellt werden. Solche Motor-Primitive kodieren elementare Bewegungen, die verallgemeinert, aneinandergereiht und kombiniert werden können, um komplexere Aufgaben zu erfüllen. Zum Beispiel könnte man ein Vorhand- und Rückhand-Spiel als zwei verschiedene Motor-Primitive für Tischtennis ansehen, welche je nach Ballposition verallgemeinert werden (siehe Abbildung 1). Die Arbeit fokussiert auf das Lernen der optimalen Ausführung von Motor-Primitiven und wie man solche auf neue Situationen verallgemeinern kann. Die vorgestellten Anwendungen kommen aus dem Sport- und Spiel-Bereich, aber die vorgestellten Techniken können auch bei alltäglichen Aufgaben im Haushalt Anwendung finden.

2 Motivation

Die Forschung an Ansätzen des maschinellen Lernens hat zu einer Vielzahl von Algorithmen geführt. Leider sind die meisten Standard-Ansätze nicht direkt auf die Robotik anwendbar, vor allem aufgrund der inhärenten hohen Dimensionalität. Daher besteht ein Bedarf an

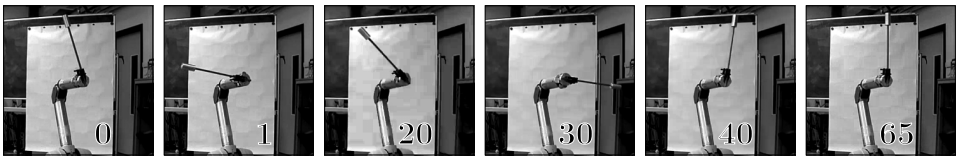


Abbildung 2: Diese Abbildung illustriert den Lernprozess des „Underactuated Swing-Up“. Ziel dieser Aufgabe ist es, das schwere Pendel von einer hängenden Position nach oben zu schwingen und dort zu balancieren. Das Drehmoment der Motoren ist limitiert, damit das Pendel nicht direkt nach oben bewegt werden kann, sondern vorher Schwung geholt werden muss. Die Bilder zeigen jeweils die Position am Ende einer Iteration. Der Lernprozess wurde mit einer Policy (Strategie), die durch Imitations-Lernen erlangt wurde, initialisiert (Bild 0). Bild 1 zeigt dieselbe Policy mit aktivierter Drehmoment-Limitierung.

Methoden, die spezifisch auf die Bedürfnisse des Roboter-Lernens zugeschnitten sind. Diese Doktorarbeit fokussiert auf das Reinforcement-Learning (bestärkende Lernen) für Motor-Primitive.

Die Reinforcement-Learning-Forschung begann in den 1950er Jahren (z. B. [Min54, FC54, Bel57]), betrachtete aber vor allem theoretische Probleme. Algorithmen wurden häufig auf synthetischen Benchmark-Problemen mit diskreten Zuständen und Aktionen evaluiert. Die wohl bekanntesten realen Anwendungen des Reinforcement-Learning sind Spiele wie Backgammon [Tes94] oder Go [CKL96], aber auch Roboter-Anwendungen können schon in den 1990er Jahren gefunden werden (z. B. [MC92, GFB94]). Im Gegensatz zu vielen Problemen in der Reinforcement-Learning-Literatur haben Roboter-Probleme inhärent kontinuierliche Zustände und Aktionen. Darüber hinaus benötigen Experimente in der Robotik oft teure und potenziell empfindliche Hardware und erfordern auch oft menschliche Überwachung und menschliches Eingreifen. Diese Unterschiede erfordern die Anpassung bestehender Reinforcement-Learning-Ansätze oder die Entwicklung von maßgeschneiderten Ansätzen.

Policy-Search (Strategie-Suche) hat sich als eine Alternative zum wertefunktion-basierten Reinforcement-Learning [SM01, KHS01, Pes01, BKNS04, EFCR06, TWS07] etabliert. Speziell für das Lernen von motorischen Fähigkeiten in der Robotik ist die direkte Suche nach einer Policy vielversprechend, statt zunächst das duale Problem (d. h. die Bestimmung der Werte-Funktion) zu lösen. Darüber hinaus können die Integration von Vorwissen in Form der Policy-Struktur, einer anfänglichen Policy oder eines Modells des Systems die benötigte Lernzeit drastisch reduzieren. Diese Doktorarbeit behandelt Policy-Search-Methoden, die eine vorstrukturierte Policy und eine anfängliche Policy nutzen können.

3 Beiträge

Diese Doktorarbeit leistet einen Beitrag zum Stand der Technik in Reinforcement-Learning, angewandt auf die Robotik, sowohl durch neuartige Algorithmen (Abschnitt 3.1) als auch durch neuartige Anwendungen (Abschnitt 3.2).

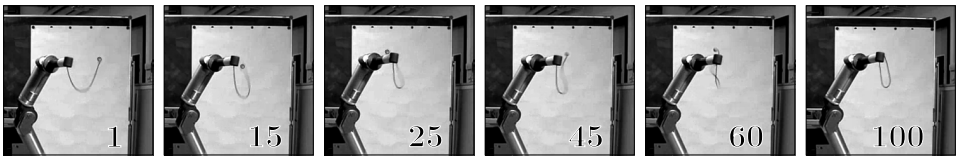


Abbildung 3: Diese Abbildung illustriert den Lernprozess der Becherspiel-Aufgabe. Das Ziel dieser Aufgabe ist es, den Ball in dem Becher zu fangen. Die Bilder zeigen jeweils die Position des Balls, die dem Becher pro Iteration am nächsten kam. Der Lernprozess wurde mit einer Policy, die durch Imitationslernen erlangt wurde, initialisiert. Dieses Nachmachen alleine genügt nicht, um die Aufgabe erfolgreich zu lösen (ganz links). Nach etwa 100 Versuchen hat der Roboter gelernt, den Ball zuverlässig zu fangen (ganz rechts).

3.1 Algorithmen

Reinforcement-Learning, angewandt auf die Robotik, muss mit einer Reihe von Herausforderungen umgehen, wie im zweiten Kapitel der Arbeit anhand einer Literatur-Übersicht diskutiert wird. Diese Studie liefert einen Überblick über die verschiedenen Techniken und möglichen Anwendungen. Der Fokus liegt auf den spezifischen Herausforderungen und Ansätzen, die das Lern-Problem trotzdem lösbar machen. Die Dimensionalität ist systembedingt hoch und kontinuierlich. Iterationen in der realen Welt sind teuer, da sie Zeit und menschliche Betreuung benötigen und potenziell teure und empfindliche Hardware voraussetzen. Der Einsatz von Modellen kann diese Probleme reduzieren, erzeugt jedoch andere Herausforderungen. Jeder Lernalgorithmus ist durch die Qualität der Kosten-Funktion beschränkt. Das Aufstellen einer Kosten- oder einer Belohnungs-Funktion ist oft nicht einfach. Selbst die Kostenfunktion einer einfachen menschlichen Greifbewegung ist nicht vollständig geklärt [BW07]. Inverses Reinforcement-Learning ist eine vielversprechende Alternative zur manuellen Spezifizierung der Belohnungs-Funktion und wurde für die Becherspiel-Aufgabe untersucht [BKP11].

Idealerweise sollte ein Algorithmus, der auf einen Roboter angewandt wird, sicher sein, d. h. eine Beschädigung des Roboters muss vermieden werden und der Algorithmus sollte schnell sein, sowohl im Hinblick auf die Konvergenz als auch auf die Rechenzeit. Wichtige Punkte für schnelle Konvergenz eines Algorithmus sind, dass er Versuche effizient nutzt, nur sehr wenige offene Parameter hat und Vorwissen nutzen kann. In dieser Doktorarbeit werden innerhalb eines Frameworks der erfolgsgewichteten Nachahmung Algorithmen vorgestellt, die diesen Anforderungen entsprechen.

Das Übersichts-Kapitel „Reinforcement Learning in Robotics: A Survey“ basiert auf [KBP13] und einer vorhergehenden Version [KP12b].

3.1.1 Policy learning by Weighting Exploration with the Returns (PoWER)

Im Kapitel „Policy Search for Motor Primitives in Robotics“ der Arbeit wird der „Policy learning by Weighting Exploration with the Returns“-Algorithmus (PoWER) vorgestellt. PoWER ist eine erwartungswert-maximisierungs-inspirierte Policy-Search-



Abbildung 4: Diese Abbildung illustriert einen Dart-Wurf mit dem Humanoiden JST-ICORP/SARCOS CBi. Der Roboter hat die Aufgabe, einen gelernten, erfolgreichen Wurf so zu verallgemeinern, dass alle Felder auf der Dartscheibe zuverlässig getroffen werden können.

Methode, die auf der strukturierten Exploration im Parameter-Raum beruht. In diesem Kapitel wird ein Framework erfolgsgewichteter Nachahmung eingeführt. Basierend auf [DH97], wird der Return (Gewinn) einer Episode als eine nicht-normalisierte Wahrscheinlichkeitsverteilung betrachtet. Somit kann eine untere Schranke des Logarithmus des erwarteten Returns gefunden und maximiert werden. Je nach Optimierungs-Strategie dieser unteren Schranke und der Explorations-Strategie entspricht das Framework mehreren bekannten Policy-Search-Methoden: dem episodischen REINFORCE [Wil92], dem „Policy Gradient Theorem“ [SMSM99], dem epsiodischen „Natural Actor Critic“ [PS08b], sowie einer Verallgemeinerung der „Reward-Weighted Regression“ [PS08a]. Der neuartige Algorithmus, PoWER, basiert auf einer erwartungswert-maximisierungs-inspirierten Optimierung und einer strukturierten, zustands-abhängigen Explorations-Strategie. Dieser Ansatz hat bereits in anderen Publikationen Anwendungen gefunden, z. B. [KCC10, KUC$^+$11, NFV$^+$12, dSKB12, VOG$^+$13]. Algorithmen, die quasi identisch zu PoWER sind, können auch über Ansätze wie „Path Integrals“ [TBS10], „Relative Entropy Policy Search“ [PMA10] und „Monte-Carlo EM“-Algorithmen [VTKP09] hergeleitet werden.

Die zugehörigen Experimente sind im Abschnitt 3.2.2 beschrieben. Dieses Kapitel basiert auf [KP11b] und den vorläufigen Versionen [KMP08, KP08, KP09, KP10].

3.1.2 Cost-regularized Kernel Regression (CrKR)

Im Kapitel „Reinforcement Learning to Adjust Parametrized Motor Primitives to New Situations“ der Arbeit wird der Algorithmus „Cost-regularized Kernel Regression“ (CrKR) vorgestellt. CrKR ist eine nicht-parametrische Policy-Search-Methode, die sich besonders für das Lernen von Meta-Parametern, d. h. einer kleinen Anzahl von Parametern, die die Bewegung global beeinflussen, eignet. In diesem Szenario kann es schwierig sein, eine gute Parametrisierung für die Policy zu finden; hier bietet eine nicht-parametrische Policy mehr Flexibilität. CrKR wird basierend auf der „Reward-Weighted Regression“ [PS08a] hergeleitet. Der resultierende Algorithmus ist mit der Gaussian-Process-Regression (Gauß-Prozess-Regression) verwandt und ähnlich zu dieser hat er auch eine prädiktive Unsicherheit, die dazu eingesetzt wird, die Exploration des Reinforcement-Learnings zu leiten. Dieser Ansatz wird verwendet, um eine Funktion zu lernen, die die Meta-Parameter abhängig von der momentanen Situation ergibt. Die Parameter der Motor-Primitive, die die Feinheiten der Bewegung bestimmen, können vorher durch andere Verfahren gelernt werden.

Die zugehörigen Experimente sind im Abschnitt 3.2.3 beschrieben. Dieses Kapitel basiert auf [KWOP12] und den vorläufigen Versionen [KOP10, KOP11, KP11a].



Abbildung 5: Diese Abbildung illustriert das Setup für das Wurf-Spiel. Der Roboter lernt gleichzeitig, die Ziele zu treffen und ein Spiel zu spielen, das von Black Jack inspiriert wurde.

3.2 Anwendungen

Diese Doktorarbeit zeigt eine große Anzahl von Benchmark-Aufgaben und untersucht die vorgestellten Ansätze mit Roboter-Aufgaben, sowohl mit simulierten als auch mit realen Robotern. Die eingesetzten Roboter sind ein Barrett WAM, ein BioRob, der Humanoide JST-ICORP/SARCOS CBi und ein Kuka KR 6. Diese Dissertation untersucht, wie einzelne motorische Fähigkeiten gelernt werden können und wie man diese verallgemeinern kann, um sie in neuen Situationen anzuwenden. Die vorliegende Arbeit hat zum Stand des Reinforcement-Learnings, angewandt auf die Robotik, durch die Erforschung hochdynamischer Bewegungen und die Vorstellung sehr effizienter Lernprozesse beigetragen.

3.2.1 Darstellung Motorischer Fähigkeiten

Das Kapitel „Movement Templates for Learning of Hitting and Batting“ der Doktorarbeit beschreibt, wie die „Dynamical Systems Motor Primitives“-Darstellung [INS02] für motorische Fähigkeiten verallgemeinert werden kann, um Schlag-Bewegungen, wie sie z. B. bei Tischtennis benötigt werden (Abbildung 1), zu repräsentieren. Dieses Kapitel basiert auf [KMK+10].

3.2.2 Einzelne Motorische Fähigkeiten

Aufgrund der hohen Dimensionalität können motorische Fähigkeiten nicht von Null an gelernt werden. Stattdessen wird imitiert wie Kinder lernen, und der Lernprozess durch Imitations-Lernen initialisiert. Beispielsweise kann der Roboter durch die Bewegung geführt werden, um eine anfängliche Policy zu erhalten. Anschließend lernt der Reinforcement-Learning-Algorithmus, diese Fähigkeit zuverlässiger auszuführen. Nach einer realistischen Anzahl von Iterationen (siehe Abbildungen 2 und 3) kann die Aufgabe regelmäßig erfüllt werden und der Roboter zeigt eine hervorragende durchschnittliche Leistung. Dieser Ansatz wird mit einer Reihe von verschiedenen Policy-Parametrisierungen, u. a. mit den „Dynamical Systems Motor Primitives“ [INS02] und anderen parametrischen Darstellungen, untersucht. PoWER wird mit einer Vielzahl von Policy-Search-Ansätzen verglichen, sowohl mit einfachen Beispielen als auch mit Roboter-Aufgaben. Der „Underactuated Swing-Up“ (Abbildung 2) und eine komplexe Becherspiel-Aufgabe (Abbildung 3) werden auf einem echten Barrett WAM effizient gelernt.



Abbildung 6: Diese Abbildung illustriert die gelernte Tischtennisball-Jonglier-Fähigkeit. Die Aufgabe ist es, den Ball auf dem Schläger hüpfen zu lassen. Hierzu musste der Lernalgorithmus bestimmen, welche Motor-Primitive Vorrang haben, z. B. ob es wichtiger ist, den Ball genau mit der Mitte des Schlägers zu treffen oder mit der richtigen Orientierung.

3.2.3 Verallgemeinerte Motorische Fähigkeiten

Um die Effizienz eines Lernprozesses zu erhöhen, ist es häufig vorteilhaft, eine motorische Fähigkeit an neue Situationen anzupassen, statt sie komplett neu zu lernen. Diese Art des Lernens erfordert oft eine nicht-intuitive Zuordnung von Situation zu Aktionen. Um den vorgeschlagenen Ansatz in einem komplexen Szenario zu demonstrieren, wurden das „Around the Clock"-Dart-Spiel (Abbildung 4), Tischtennis (Abbildung 1) und ein Wurf-Spiel (Abbildung 5) gewählt und diese sowohl auf simulierten als auch auf realen Robotern implementiert. In diesen Szenarien wird gezeigt, dass der Ansatz mit einer Vielzahl von Situationen zurecht kommt, d. h. unterschiedlichen Kosten-Funktionen (mit und ohne sekundären Zielen) und ganz unterschiedlichen Policys mit ihren zugehörigen Meta-Parametern. Die Experimente wurden auf vier verschiedenen realen Robotern durchgeführt (einem Barrett WAM, einem BioRob, dem Humanoiden JST-ICORP/SARCOS CBi und einem Kuka KR 6). Das Wurf-Spiel zeigt erste Schritte in Richtung eines hierarchischen Reinforcement-Learning-Systems.

Viele Roboter-Aufgaben können in Teilaufgaben zerlegt werden. Doch oft sind diese Teilaufgaben nicht gleichzeitig erfüllbar und die Prioritäts-Struktur muss bestimmt werden. Erste Schritte in Richtung eines Regler-Gesetzes, das auf einer Anzahl von priorisierten Motor-Primitiven beruht, werden mit einer Tischtennisball-Jonglier-Aufgabe (siehe Abbildung 6) auf einem Barrett WAM untersucht. Das Kapitel „Learning Prioritized Control of Motor Primitives" basiert auf [KP12a].

4 Fazit

Diese Doktorarbeit erweitert den Stand der Forschung in Reinforcement-Learning, angewandt auf die Robotik, sowohl durch neuartige Algorithmen als auch durch neuartige Anwendungen. Die vorgestellten Algorithmen, die aus dem neuen Framework erfolgsgewichteter Nachahmung entstammen, entsprechen den speziellen Anforderungen des Lernens auf realen Robotern, die in Abschnitt 3.1 erwähnt wurden. Alle vorgeschlagenen Ansätze wurden ausführlich mit bestehenden Ansätzen verglichen und mit herausfordernden Roboter-Aufgaben validiert. Diese sind unter anderem die komplexe Becherspiel-Aufgabe,

das Verallgemeinern von Dart-Würfen und Tischtennis-Schlägen, ein Zielwurf-Spiel und eine Tischtennisball-Jonglier-Aufgabe. Die Ansätze wurden mit verschiedenen realen Robotern realisiert: mit einem Barrett WAM, dem Humanoiden JST-ICORP/SARCOS CBi, einem KUKA KR 6 Roboter und einem BioRob.

Literatur

[Bel57] R. E. Bellman. *Dynamic Programming*. Princeton University Press, Princeton, NJ, 1957.

[BKNS04] J. A. Bagnell, S. Kadade, A. Ng und J. C. Schneider. Policy Search by Dynamic Programming. In *Advances in Neural Information Processing Systems (NIPS)*, 2004.

[BKP11] A. Boularias, J. Kober und J. Peters. Relative Entropy Inverse Reinforcement Learning. *Journal of Machine Learning Research - Proceedings Track*, 15:182–189, 2011.

[Bot12] BotJunkie. BotJunkie Interview: Nancy Dussault Smith On iRobot's Roomba, Februar 2012.

[BW07] P. M. Bays und D. M. Wolpert. Computational Principles of Sensorimotor Control that Minimise Uncertainty and Variability. *Journal of Physiology*, 578:387–396, 2007.

[CKL96] H. W. Chan, I. King und J. C. S. Lui. Performance Analysis of a New Updating Rule for TD(λ) Learning in Feedforward Networks for Position Evaluation in Go Game. In *IEEE Int. Conf. on Neural Networks*, 1996.

[DH97] P. Dayan und G. E. Hinton. Using Expectation-Maximization for Reinforcement Learning. *Neural Computation*, 9(2):271–278, 1997.

[dSKB12] B. C. da Silva, G. D. Konidaris und A. G. Barto. Learning Parameterized Skills. In *Int. Conf. on Machine Learning*, 2012.

[EFCR06] A. El-Fakdi, M. Carreras und P. Ridao. Towards Direct Policy Search Reinforcement Learning for Robot Control. In *IEEE/RSJ Int. Conf. on Intelligent Robots and Systems (IROS)*, 2006.

[FC54] B. G. Farley und W. A. Clark. Simulation of Self-organizing Systems by Digital Computer. *IRE Transactions on Information Theory*, 4:76–84, 1954.

[GFB94] V. Gullapalli, J. Franklin und H. Benbrahim. Aquiring Robot Skills via Reinforcement Learning. *IEEE Control Systems Journal, Special Issue on Robotics: Capturing Natural Motion*, 4(1):13–24, 1994.

[INS02] A. J. Ijspeert, J. Nakanishi und S. Schaal. Learning Attractor Landscapes for Learning Motor Primitives. In *Advances in Neural Information Processing Systems (NIPS)*, 2002.

[KBP13] J. Kober, J. A. Bagnell und J. Peters. Reinforcement Learning in Robotics: A Survey. *Int. Journal of Robotics Research*, 2013.

[KCC10] P. Kormushev, S. Calinon und D. G. Caldwell. Robot Motor Skill Coordination with EM-based Reinforcement Learning. In *IEEE/RSJ Int. Conf. on Intelligent Robots and Systems (IROS)*, 2010.

[KHS01] I. Kwee, M. Hutter und J. Schmidhuber. Gradient-based Reinforcement Planning in Policy-Search Methods. In *Europ. Workshop on Reinforcement Learning (EWRL)*, 2001.

[KMK+10] J. Kober, K. Mülling, O. Krömer, C. H. Lampert, B. Schölkopf und J. Peters. Movement Templates for Learning of Hitting and Batting. In *IEEE Int. Conf. on Robotics and Automation (ICRA)*, 2010.

[KMP08] J. Kober, B. Mohler und J. Peters. Learning Perceptual Coupling for Motor Primitives. In *IEEE/RSJ Int. Conf. on Intelligent Robots and Systems (IROS)*, 2008.

[Kob12] J. Kober. *Learning Motor Skills: From Algorithms to Robot Experiments*. Dissertation, TU Darmstadt, April 2012.

[KOP10] J. Kober, E. Oztop und J. Peters. Reinforcement Learning to Adjust Robot Movements to New Situations. In *Robotics: Science and Systems Conf. (R:SS)*, 2010.

[KOP11] J. Kober, E. Oztop und J. Peters. Reinforcement Learning to Adjust Robot Movements to New Situations. In *Int. Joint Conf. on Artificial Intelligence (IJCAI), Best Paper Track*, 2011.

[KP08] J. Kober und J. Peters. Policy Search for Motor Primitives in Robotics. In *Advances in Neural Information Processing Systems (NIPS)*, 2008.

[KP09] J. Kober und J. Peters. Learning Motor Primitives for Robotics. In *IEEE Int. Conf. on Robotics and Automation (ICRA)*, 2009.

[KP10] J. Kober und J. Peters. Imitation and Reinforcement Learning - Practical Algorithms for Motor Primitive Learning in Robotics. *IEEE Robotics and Automation Magazine*, 17(2):55–62, 2010.

[KP11a] J. Kober und J. Peters. Learning Elementary Movements Jointly with a Higher Level Task. In *IEEE/RSJ Int. Conf. on Intelligent Robots and Systems (IROS)*, 2011.

[KP11b] J. Kober und J. Peters. Policy Search for Motor Primitives in Robotics. *Machine Learning*, 84(1-2):171–203, 2011.

[KP12a] J. Kober und J. Peters. Learning Prioritized Control of Motor Primitives. 2012. `arXiv:1209.0488 [cs.RO]`.

[KP12b] J. Kober und J. Peters. *Reinforcement Learning: State-of-the-Art*, Kapitel Reinforcement Learning in Robotics: A Survey, Seiten 579–610. Springer Berlin / Heidelberg, 2012.

[KUC+11] P. Kormushev, B. Ugurlu, S. Calinon, N. Tsagarakis und D. G. Caldwell. Bipedal Walking Energy Minimization by Reinforcement Learning with Evolving Policy Parameterization. In *IEEE/RSJ Int. Conf. on Intelligent Robots and Systems (IROS)*, 2011.

[KWOP12] J. Kober, A. Wilhelm, E. Oztop und J. Peters. Reinforcement Learning to Adjust Parametrized Motor Primitives to New Situations. *Autonomous Robots*, 33(4):361–379, 2012.

[MC92] S. Mahadevan und J. Connell. Automatic Programming of Behavior-based Robots using Reinforcement Learning. *Artificial Intelligence*, 55(2-3):311–365, 1992.

[Min54] M. L. Minsky. *Theory of Neural-Analog Reinforcement Systems and its Application to the Brain-Model Problem*. Dissertation, Princeton University, 1954.

[NFV+12] B. Nemec, D. Forte, R. Vuga, M. Tamosiunaite, F. Wörgötter und A. Ude. Applying Statistical Generalization to Determine Search Direction for Reinforcement Learning of Movement Primitives. In *IEEE/RAS Int. Conf. on Humanoid Robots (Humanoids)*, 2012.

[Pes01] L. Peshkin. *Reinforcement Learning by Policy Search*. Dissertation, Brown University, Providence, RI, 2001.

[PMA10] J. Peters, K. Mülling und Y. Altun. Relative Entropy Policy Search. In *National Conf. on Artificial Intelligence (AAAI)*, 2010.

[PS08a] J. Peters und S. Schaal. Learning to Control in Operational Space. *Int. Journal of Robotics Research*, 27(2):197–212, 2008.

[PS08b] J. Peters und S. Schaal. Natural Actor-Critic. *Neurocomputing*, 71(7-9):1180–1190, 2008.

[Sim65] H. A. Simon. *The Shape of Automation for Men and Management*. New York: Harper & Row, 1965.

[SM01] M. Strens und A. Moore. Direct Policy Search using Paired Statistical Tests. In *Int. Conf. on Machine Learning (ICML)*, 2001.

[SMSM99] R. S. Sutton, D. McAllester, S. Singh und Y. Mansour. Policy Gradient Methods for Reinforcement Learning with Function Approximation. In *Advances in Neural Information Processing Systems (NIPS)*, 1999.

[TBS10] E. A. Theodorou, J. Buchli und S. Schaal. Reinforcement Learning of Motor Skills in High Dimensions: A Path Integral Approach. In *IEEE Int. Conf. on Robotics and Automation (ICRA)*, 2010.

[Tes94] G. Tesauro. TD-Gammon, a Self-Teaching Backgammon Program, Achieves Master-Level Play. *Neural Computation*, 6(2):215–219, 1994.

[TWS07] M. E. Taylor, S. Whiteson und P. Stone. Transfer via Inter-Task Mappings in Policy Search Reinforcement Learning. In *Int. Joint Conf. on Autonomous Agents and Multiagent Systems (AAMAS)*, 2007.

[VOG+13] R. Vuga, M. Ogrinc, A. Gams, T. Petrič, N. Sugimoto, A. Ude und J. Morimoto. Motion Capture and Reinforcement Learning of Dynamically Stable Humanoid Movement Primitives. In *IEEE Int. Conf. on Robotics and Automation (ICRA)*, 2013.

[VTKP09] N. Vlassis, M. Toussaint, G. Kontes und S. Piperidis. Learning Model-free Robot Control by a Monte Carlo EM Algorithm. *Autonomous Robots*, 27(2):123–130, 2009.

[Wil92] R. J. Williams. Simple Statistical Gradient-following Algorithms for Connectionist Reinforcement Learning. *Machine Learning*, 8:229–256, 1992.

[Wul07] G. Wulf. *Attention and motor skill learning*. Human Kinetics, Champaign, IL, 2007.



Jens Kober wurde am 6. Mai 1982 in Künzelsau geboren. In 2008 absolvierte er sein Ingenieurstudium an der Universität Stuttgart (Diplom-Ingenieur Technische Kybernetik) und zeitgleich ein französisches Ingenieurstudium (Ecole Centrale Paris). Die Doktorarbeit von Jens Kober wurde im gemeinsamen Roboter-Lern-Labor des Fachgebietes Intelligente Autonome Systeme, TU Darmstadt, und des Max Planck Instituts für Intelligente Systeme, Tübingen, angefertigt. Betreut wurde die Promotion von Professor Dr. Jan Peters. Während seiner Doktorarbeit nutzte Jens Kober die Möglichkeit als Gastwissenschaftler am Advanded Telecommunication Research (ATR) Center in Japan und als Praktikant bei Disney Research Pittsburgh, USA, zu forschen. Seit kurzem arbeitet er am Offenbacher Honda Research Institute Europe und zugleich am CoR-Lab der Universität Bielefeld.

Modellierung korrelierter Eingabedaten für Simulationen*

Jan Kriege
Fakultät für Informatik, TU Dortmund
jan.kriege@tu-dortmund.de

Abstract: Ein wichtiger Schritt bei der Erstellung von Simulationsmodellen ist die geeignete Repräsentation von korrelierten Eingabedaten. Für unabhängig und identisch verteilte Daten existieren zahlreiche Ansätze, während sich die Modellierung von Korrelation noch schwierig gestaltet. In diesem Beitrag wird ein Ansatz vorgestellt der Phasenverteilungen und ARMA-Prozesse kombiniert um korrelierte Daten abzubilden. Für diesen Ansatz wird ein Verfahren zur Parameteranpassung vorgestellt und anhand von echten Verkehrsdaten wird gezeigt, dass der Ansatz eine gute Darstellung von Verteilung und Korrelation ermöglicht.

1 Einleitung

Die Leistungsbewertung von Computer- und Kommunikationssystemen spielt eine wichtige Rolle beim Entwurf neuer Systeme oder bei Änderungen an vorhandenen Systemen. Aufgrund der zunehmenden Komplexität dieser Systeme ist es oftmals nicht mehr möglich, Experimente mit dem realen System durchzuführen und der Einsatz stochastischer Modelle ist zur Ermittlung von Leistungsmaßen erforderlich. Für eingeschränkte Modellklassen bieten sich numerische Techniken [Ste94] zur Ermittlung dieser Maße an. Aufgrund der zuvor erwähnten Komplexität bleibt aber oft nur eine simulative Untersuchung [LK00], für die keine Einschränkungen des Modells erforderlich sind. Eine geeignete Darstellung der Eingabedaten (wie z.B. Ankunftszeiten oder Bedienzeiten) ist unerlässlich, um valide Simulationsmodelle und somit brauchbare Simulationsergebnisse zu erhalten. Oftmals liegen Beobachtungen aus einem realen System vor und es wird versucht, wesentliche Charakteristika dieser Beobachtungen durch Verteilungen oder stochastische Prozesse abzubilden. Für den Fall, dass diese Daten unabhängig und identisch verteilt sind, sich also durch eine Verteilung geeignet abbilden lassen, existiert eine umfangreiche Theorie [LK00]. Methoden zur Parameteranpassung von Verteilungen werden von Standardwerkzeugen [LM03] zur Verfügung gestellt und gängige Simulationssoftware unterstützt üblicherweise den Einsatz einer umfangreichen Auswahl von Verteilungen. Anders stellt sich die Lage dar, wenn die Beobachtungen aus dem realen System Abhängigkeiten und Korrelationen enthalten, wie es in vielen Anwendungsbereichen der Fall ist. Als Beispiel seien hier Rechner- und Kommunikationsnetzwerke [CB96, PF95] genannt. Es ist bekannt, dass die Vernachlässigung dieser Korrelationen zu einer Unterschätzung des Ressourcenbedarfs führt und Verteilungen zur Modellierung der Eingabedaten hier nicht mehr

*Englischer Titel der Dissertation: “Fitting Simulation Input Models for Correlated Traffic Data”

ausreichen [LMT93]. In der Vergangenheit wurden daher unterschiedliche Typen von stochastischen Prozessen vorgestellt, um sowohl die empirische Verteilung als auch die auftretenden Abhängigkeiten modellieren zu können, z.B. Autoregressive-Moving-Average (ARMA) Prozesse [BJ70], ARTA Prozesse [CN96] und Markovsche Ankunftsprozesse (MAPs) [Neu81].

Beim Einsatz dieser Prozesse in Simulationsmodellen ergeben sich aber noch zahlreiche Probleme: So gestaltet sich die Parameteranpassung für Prozesse deutlich schwieriger als für Verteilungen und ist meist nur prototypisch implementiert. Fehlende Unterstützung in den gängigen Simulationstools erschwert den Einsatz der Prozesse zusätzlich. Außerdem unterstützen viele Prozesstypen nur eine eingeschränkte Klasse von Verteilungen, die nicht ausreicht, um z.B. Zwischenankunftszeiten in Rechnernetzen adäquat zu modellieren.

Ziel dieser Arbeit ist es daher, die zuvor angesprochenen Probleme beim Einsatz stochastischer Prozesse in der Simulation zu mildern. In Abschnitt 2 werden wir zunächst einen kurzen Überblick über existierende Ansätze zur Modellierung von korrelierten Daten geben und einige Vor- und Nachteile herausarbeiten. In Abschnitt 3 wird schließlich eine neue Klasse von stochastischen Prozessen vorgestellt, die Phasenverteilungen zur Modellierung der empirischen Verteilung mit ARMA Prozessen zur Modellierung der Autokorrelation kombiniert. Die Umsetzung dieser theoretischen Verfahren in Werkzeuge zur Parameteranpassung und Simulation wird in Abschnitt 4 beschrieben. In Abschnitt 5 präsentieren wir einige experimentelle Ergebnisse, die zeigen dass die neue Klasse von stochastischen Prozessen geeignet ist, sowohl Verteilung als auch Korrelation von realen Netzwerkdaten geeignet abbilden zu können.

2 Grundlagen

Wir betrachten die Modellierung von stochastischen Prozessen Y_t anhand von Beobachtungen aus einem realen System, die üblicherweise in Form eines Traces $T = (t_1, t_2, \ldots, t_l)$ vorliegen. Sofern die Beobachtungen unabhängig und identisch verteilt sind, ist es ausreichend die Parameter einer geeigneten Verteilungsfunktion anzupassen, wozu eine umfangreiche Theorie existiert [LK00]. Die Qualität der Parameteranpassung wird häufig mit Hilfe der Likelihood-Funktion $L(T, X) = \prod_{i=1}^{l} f_X(t_i)$ für einen Trace T und eine angepasste Verteilung mit Dichtefunktion $f_X(x)$ bestimmt. Aus numerischen Gründen nutzt man oft die log-Likelihood $l(T) = \log L(T, X)$. Im Gegensatz zur Parameteranpassung von Verteilungen existieren für die Anpassung von stochastischen Prozessen, die sowohl die Verteilung als auch die Korrelation eines Traces abbilden deutlich weniger Ergebnisse. Wir werden im Folgenden einige Ansätze mit ihren Stärken und Schwächen vorstellen.

2.1 Phasenverteilungen und Markovsche Ankunftsprozesse

Phasenverteilungen (PH-Verteilungen) lassen sich mittels einer $n \times n$ Matrix D_0 mit Transitionsraten und einem Vektor π mit initialen Wahrscheinlichkeiten definieren und be-

schreiben unabhängig und identisch verteilte Zufallsvariablen als Zeit bis zur Absorption in einer Markov-Kette [Neu81]. Die Momente und die Dichtefunktion einer PH-Verteilung ergeben sich wie folgt:

$$\mu_i = E(X^i) = i!\pi M^i e^T \text{ und } f_X(t) = \pi e^{D_0 t} e^T \tag{1}$$

mit $M = -(D_0)^{-1}$ und dem Vektor $e = (1, \cdots, 1)$ der Länge n. Phasenverteilungen sind eine sehr flexible Familie von Verteilungen, die jede Verteilung mit positiver Dichtefunktion in $(0, \infty)$ beliebig genau approximieren können [AO97]. Da die Darstellung von Phasenverteilungen redundant ist, gestaltet sich die Parameteranpassung im Allgemeinen schwierig. Die meisten Verfahren schränken daher die Klasse der unterstützten Verteilungen ein. Für azyklische PH-Verteilungen, bei denen sich D_0 als obere Dreiecksmatrix darstellen lässt, existieren Ansätze, die die Parameter anhand der empirischen Momente [BK09] oder durch Maximierung der Likelihood [TBT06] anpassen.

Sofern auch Korrelation berücksichtigt werden soll, können PH-Verteilungen zu Markovschen Ankunftsprozessen (MAPs) erweitert werden. Insbesondere bei einer größeren Anzahl von Korrelationskoeffizienten ist die Parameteranpassung von MAPs allerdings schwierig, auch wenn neuere Ansätze gute Resultate erzielen [CZS10].

2.2 ARMA Prozesse

Autoregressive Moving Average (ARMA) Prozesse [BJ70] dienen zur Modellierung von Zeitreihen. Ein $ARMA(p, q)$ Prozess ist definiert als

$$Z_t = \alpha_1 Z_{t-1} + \alpha_2 Z_{t-2} + ... + \alpha_p Z_{t-p} + \beta_1 \epsilon_{t-1} + \beta_2 \epsilon_{t-2} + ... + \beta_q \epsilon_{t-q} + \epsilon_t \tag{2}$$

wobei die Rauschterme ϵ_t normalverteilt mit Mittelwert 0 und Varianz σ_ϵ^2 sind. Für $q = 0$ ergibt sich ein sogenannter $AR(p)$ Prozess der durch $Z_t = \alpha_1 Z_{t-1} + \alpha_2 Z_{t-2} + ... + \alpha_p Z_{t-p} + \epsilon_t$ beschrieben ist. ARMA Modelle sind sehr flexibel bei der Modellierung der Autokorrelation und Methoden zur Parameteranpassung werden durch Standardsoftware für Statistik zur Verfügung gestellt [BJ70]. Die Verteilung der Modelle ist allerdings die gewichtete Summe von $N(0, \sigma_\epsilon^2)$ verteilten Zufallsvariablen, was bedeutet, dass nur Verteilungen modelliert werden können, die sich durch einfache Transformationen aus der Normalverteilung ergeben.

2.3 ARTA Prozesse

ARTA-Prozesse [BN05, CN96] kombinieren einen $AR(p)$ Prozess $\{Z_t; t = 1, 2, ...\}$ mit einer Verteilung F_Y und versuchen so die genannten Schwächen des $AR(p)$ Prozesses bei der Modellierung der Verteilung zu beseitigen. Sie beschreiben eine Sequenz $Y_t = F_Y^{-1}[\Phi(Z_t)]$ $(t = 1, 2, ...)$, wobei Φ die Verteilungsfunktion der Standardnormalverteilung ist. Der $AR(p)$ dient zur Modellierung der Korrelation und wird so konstruiert, dass er

standard-normalverteilt ist. Die Transformation $U_t = \Phi(Z_t)$ erzeugt dann gleichverteilte Zufallsvariablen im Intervall $(0, 1)$ [Dev86] und $Y_t = F_Y^{-1}[U_t]$ ergibt eine Zeitreihe mit der gewünschten Verteilung F_Y. In [CN96, BN05] wurden Verfahren zur Parameteranpassung von ARTA-Prozessen entwickelt. Da ARTA-Prozesse auf der Invertierung der Verteilungsfunktion basieren, eignen sie sich nur für Verteilungen für die F_Y^{-1} effizient berechnet werden kann, da die Invertierung sowohl für die Parameteranpassung als auch zur Erzeugung von Zufallszahlen durchgeführt werden muss. Für Phasenverteilungen kann die inverse Verteilungsfunktion im Allgemeinen nicht effizient berechnet werden. Allerdings ergibt sich für azyklische Phasenverteilungen, die sich als Kombination von endlichen Sequenzen von Exponentialverteilungen darstellen lassen, eine andere Möglichkeit Verteilung und $ARMA(p, q)$-Prozess zu kombinieren, wie wir im Folgenden zeigen werden.

3 Modellierung von korrelierten Daten mit Phasenverteilungen und ARMA-Prozessen

Um die Vorteile von azyklischen Phasenverteilungen (APH) gegenüber anderen Verteilungen, die für den ARTA-Ansatz geeignet sind, zu verdeutlichen, haben wir APHs (in diesem Fall Hyper-Erlang-Verteilungen mit r Zuständen ($HErD(r)$)) und einige andere Verteilungen für die F_Y^{-1} effizient berechnet werden kann an drei unterschiedliche Traces mit Netzwerktraffic angepasst. Aus Platzgründen zeigen wir hier nur die Ergebnisse für den Trace *BC-pAug89* [LTWW94]. Als Verteilungen wurden Exponential- und Lognormal-Verteilung gewählt, für die Maximum-Likelihood-Schätzer bekannt sind [LK00], sowie Verteilungen aus der Johnson-Familie [Whe80] und die Weibull-Verteilung. Die Hyper-Erlang-Verteilungen wurden mit dem Expectation-Maximization-Ansatz aus [TBT06] angepasst. Tabelle 1 enthält die Likelihood-Werte und die Momente der Verteilungen zu-

	Verteilung	Log-Likelihood	Moment 1	Moment 2	Moment 3
BC-pAug89	Exponential	−999999	1.0 (0.0%)	2.0 (52.7%)	6.0 (90.7%)
	Johnson SU	−959863	0.89 (11.0%)	1.8 (57.4%)	8.1 (87.5%)
	Weibull	−990007	0.95 (5.0%)	2.1 (50.3%)	7.3 (88.7%)
	Lognormal	−953799	1.05 (5.0%)	4.1 (2.9%)	56.9 (12.1%)
	HErD(2)	−911558	1.0 (0.0%)	4.5 (5.9%)	66.3 (2.4%)
	HErD(3)	−911135	1.0 (0.0%)	3.5 (16.9%)	34.4 (46.9%)
	HErD(4)	−874270	1.0 (0.0%)	4.1 (2.9%)	51.2 (20.9%)
	HErD(5)	−847551	1.0 (0.0%)	4.1 (2.9%)	50.8 (21.5%)

Tabelle 1: Likelihood und Momente für die angepassten Verteilungen

sammen mit dem relativen Fehler $(|\mu_i - \hat{\mu}_i|/\hat{\mu}_i) \cdot 100$ in Prozent, wobei μ_i und $\hat{\mu}_i$ das i-te Moment der Verteilung bzw. des Traces ist. Tabelle 1 zeigt deutlich, dass mit Phasenverteilungen üblicherweise eine bessere Anpassung sowohl bezüglich der Likelihood als auch der Momente möglich ist, insbesondere, wenn sich die Zustandszahl der APH-Verteilung erhöht. Diese Ergebnisse verdeutlichen, dass es sinnvoll ist Phasenverteilungen zur Modellierung von Netzwerktraffic einzusetzen,

Eine weitere Einschränkung der ARTA-Prozesse ergibt sich aus der Nutzung des $AR(p)$ Prozesses. Ein $AR(p)$ eignet sich, um p Autokorrelationskoeffizienten exakt zu modellieren, weitere Koeffizienten werden allerdings nicht mehr modelliert. Da Computernetzwerke üblicherweise eine signifikante Autokorrelation über eine große Anzahl von Koeffizienten aufweisen, führt dies zu sehr großen Modellbeschreibungen. Mit $ARMA(p,q)$ ist es dagegen möglich eine genaue Approximation von deutlich mehr als $p+q$ Koeffizienten zu erzielen. Diese Beobachtungen motivieren die Nutzung von Phasenverteilungen und $ARMA(p,q)$ Prozessen zur Modellierung von Netzwerktraffic, die wir im Folgenden vorstellen.

Dabei dient der $ARMA(p,q)$ der Modellierung der Autokorrelation und die Phasenverteilung mit n Zuständen der Modellierung der empirischen Verteilung. Dieser neuartige Prozesstyp aus [Kri12] wird als $CAPP(n,p,q)$ (*Correlated Acyclic Phase-type Process*) bezeichnet. Zunächst wird kurz vorgestellt, wie APH-Verteilung und ARMA-Prozess in einen stochastischen Prozess kombiniert werden können.

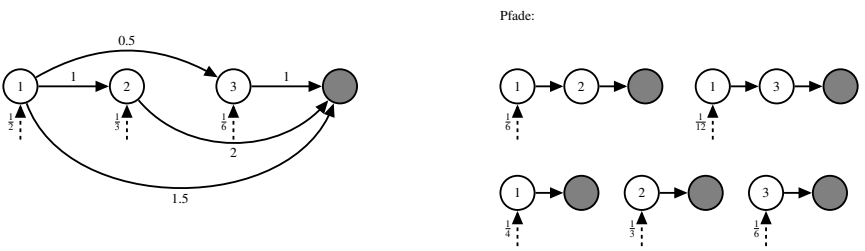


Abbildung 1: APH-Verteilung mit Pfaden

Für die Kombination ist es erforderlich, die APH-Verteilung anders darzustellen als durch die übliche Matrix-Notation. APH-Verteilungen lassen sich als eine Menge von Pfaden (elementary series) darstellen [Cum82], wobei jeder Pfad eine Sequenz von Zuständen von einem Initialzustand zum absorbierenden Zustand beschreibt. Jeder dieser Pfade beschreibt eine Hypo-Exponential-Verteilung, also eine Folge von Exponentialverteilungen mit unterschiedlichen Raten. Außerdem wird jedem Pfad eine Wahrscheinlichkeit zugeordnet, die sich aus der initialen Wahrscheinlichkeit des ersten Zustands des Pfades und den Transitionsraten auf dem Pfad ergibt. Ein Beispiel ist in Abbildung 1 dargestellt.

Sei τ_i die Wahrscheinlichkeit des i-ten Pfades ($i = 1, ..., m$). Wir definieren

$$\begin{array}{rcll} \underline{b}_1 & = & 0 & \\ \bar{b}_i & = & \underline{b}_i + \tau_i & i = 1, ..., m \\ \underline{b}_i & = & \bar{b}_{i-1} & i = 2, ..., m \end{array} \qquad \text{und} \qquad \delta(U,i) = \begin{cases} 1, & U \in [\underline{b}_i, \bar{b}_i) \\ 0, & \text{sonst} \end{cases} \tag{3}$$

Sei $\{X_t^{(\Lambda_i)}\}$ eine Sequenz von unabhängig und identisch verteilten Zufallsvariablen mit Hypo-Exponential-Verteilung, beschrieben durch einen Vektor Λ_i mit Länge S_i der die Transitionsraten des i-ten Pfades enthält. Sei $\{Z_t\}$ ein $ARMA(p,q)$ Prozess wie in Gleichung 2 definiert. Wir nehmen an, dass σ_ϵ^2 so gewählt wurde, dass $\{Z_t\}$ Standard-Normalverteilung hat und setzen $U_t = \Phi(Z_t)$, wobei Φ wieder die Standard-Normalverteilung ist.

$\{U_t\}$ beschreibt eine Sequenz von gleichverteilten Zufallsvariablen im Intervall $(0, 1)$ [Dev86], die korreliert sind, da die $\{Z_t\}$ ebenfalls Korrelation aufweisen. Die Reihe

$$Y_t = \sum_{i=1}^{m} \delta(U_t, i) X_t^{(\Lambda_i)} \tag{4}$$

beschreibt dann eine Sequenz von korrelierten Zufallsvariablen mit der gewünschten Phasenverteilung. Der ARMA-Prozess dient hierbei der Auswahl eines Pfades gemäß der Wahrscheinlichkeit τ_i. Da die Werte aus dem ARMA-Prozess korreliert sind, weist auch die Sequenz Y_t Korrelation auf.

Um die Prozessbeschreibung nutzen zu können, ist es allerdings notwendig, die Korrelationen $Corr[Y_t, Y_{t+h}]$ und $Corr[Z_t, Z_{t+h}]$ in Beziehung zu setzen. Gesucht ist eine Prozessbeschreibung $\{Z_t\}$ mit Autokorrelation $Corr[Z_t, Z_{t+h}]$, so dass $\{Y_t\}$ die gewünschte Korrelation $Corr[Y_t, Y_{t+h}]$ aufweist, die beispielsweise aus einem Trace ermittelt wurde.

Die Autokorrelation von $\{Y_t\}$ kann ausgedrückt werden durch

$$Corr[Y_t, Y_{t+h}] = \frac{E[Y_t Y_{t+h}] - E[Y]^2}{Var[Y]}. \tag{5}$$

$E[Y]$ und $Var[Y]$ sind bekannt und können mit Hilfe von Gleichung 1 berechnet werden. Für den fehlenden Term $E[Y_t Y_{t+h}]$ ergibt sich nach einigen Umformungen (für die detaillierte Herleitung sei auf [Kri12] verwiesen):

$$E[Y_t Y_{t+h}] = \sum_{i,j} \left(\left(\sum_{s=1}^{S_i} \frac{1}{\Lambda_i(s)} \right) \left(\sum_{s=1}^{S_j} \frac{1}{\Lambda_j(s)} \right) \int_{\Phi^{-1}(\underline{b}_j)}^{\Phi^{-1}(\bar{b}_j)} \int_{\Phi^{-1}(\underline{b}_i)}^{\Phi^{-1}(\bar{b}_i)} \varphi_{\rho_h}(z_t, z_{t+h}) dz_t dz_{t+h} \right) \tag{6}$$

wobei $\varphi_{\rho_h}(z_t, z_{t+h})$ die Dichtefunktion der bivariaten Standard-Normalverteilung mit Korrelation $\rho_h = Corr[Z_t, Z_{t+h}]$ ist. Der Term $E[Y_t Y_{t+h}]$ ergibt sich also als Summe über die Kombinationen der möglichen Pfade. Jeder Summand ist dabei das Produkt aus dem Mittelwert des ersten Pfads, dem Mittelwert des zweiten Pfads und dem Integral über die Dichtefunktion der bivariaten Standard-Normalverteilung. Für die Berechnung des Integrals existieren schnelle numerische Verfahren [DW90].

Die Parameteranpassung von CAPPs kann in zwei Schritten erfolgen, d.h. Phasenverteilung und ARMA-Prozess können getrennt voneinander angepasst werden, wodurch sich das Optimierungsproblem in zwei leichter zu lösende Probleme aufteilt. Für die Anpassung der APH-Verteilung kann auf ein beliebiges existierendes Verfahren zurückgegriffen werden (siehe z.B. Abschnitt 2.1). Ein wesentlicher Schritt bei der Konstruktion von CAPPs ist die Erzeugung des $ARMA(p, q)$ Prozesses, der zwei Anforderungen erfüllen muss. Zunächst muss die Autokorrelation so bestimmt sein, dass der CAPP die gewünschte Autokorrelation, die beispielsweise aus einem Trace ermittelt wurde, aufweist. Außerdem wurde verlangt, dass der Prozess standard-normalverteilt ist ($Z_t \sim N(0, 1)$). Die Parameteranpassung des ARMA-Prozesses gliedert sich also in drei Phasen: Bestimmung der Autokorrelation anhand der gewünschten Autokorrelation des CAPPs, Bestimmung der Parameter und Anpassung des Prozesses, so dass er standard-normalverteilt ist.

Die Autokorrelationsstruktur kann mit Hilfe von Gleichung 6 numerisch mit beliebiger Genauigkeit bestimmt werden. Sei $\hat{\rho_h}$ die lag-h Autokorrelation die der CAPP letztendlich aufweisen soll. Gesucht ist dann die ARMA-Autokorrelation ρ_h, so dass der CAPP gemäß Gleichung 6 Autokorrelation $\hat{\rho_h}$ hat. Die Bestimmung kann numerisch mit einem einfachen Suchverfahren [PTVF93] erfolgen. Nachdem die Autokorrelationskoeffizienten $\rho = (\rho_1, \rho_2, ..., \rho_K)$ für den ARMA-Prozess bestimmt worden sind, müssen Parameter gefunden werden, so dass der Prozess tatsächlich die gewünschte Autokorrelation aufweist. Dazu ist das Optimierungsproblem

$$min \sum_{k=1}^{K} \left(\frac{\rho_k^*}{\rho_k} - 1 \right)^2 \tag{7}$$

zu lösen, wobei ρ_k die gewünschte Korrelation und ρ_k^* die Korrelation des $ARMA(p, q)$-Modells ist, das während der Minimierung erzeugt wird.

Im letzten Schritt muss die Varianz σ_ϵ^2 der Rauschterme angepasst werden, so dass $Z_t \sim N(0, 1)$ Da für einen ARMA-Prozess Kovarianz und Varianz beide von σ_ϵ^2 abhängen [BD98], kann σ_ϵ^2 wie gewünscht gesetzt werden, ohne dabei die Autokorrelation zu ändern.

Für Gleichung 6 lassen sich einige interessante Eigenschaften nachweisen, die für die Durchführung des beschriebenen Verfahrens notwendig sind. Diese Eigenschaften sollen hier nur kurz erwähnt werden, für Details sei auf [Kri12] verwiesen. Zum Einen ist die Autokorrelation des CAPPs eine monoton steigende Funktion bezüglich der ARMA-Korrelation ρ, was für das oben beschriebene Suchverfahren nötig ist. Zum Anderen ist die Funktion stetig, so dass tatsächlich alle möglichen Korrelationswerte erreicht werden können. Für die Extremfälle $\rho \pm 1$ ist es außerdem möglich Gleichung 6 ohne numerische Berechnung des Integrals zu lösen. Dies ermöglicht eine einfache Berechnung der minimal und maximal möglichen Korrelation, die ein CAPP mit bestimmter Phasenverteilung aufweisen kann. Da die Darstellung von Phasenverteilungen nicht eindeutig ist hilft dies außerdem bei der Bestimmung von Transformationen in eine andere Darstellung derselben Verteilung, die eine höhere maximale Korrelation ermöglicht.

Neben CAPPs wurden in [Kri12] noch CHEPs (Correlated Hyper-Erlang Processes) definiert. CHEPs sind ein Spezialfall von CAPPs, für die als PH-Verteilung eine Hyper-Erlang-Verteilung genutzt wird. Durch diesen Verteilungstyp vereinfachen sich einige der Notationen, das Vorgehen und die Ideen sind aber im Prinzip identisch.

4 Tool-Unterstützung

Um die eingangs erwähnte mangelhafte Unterstützung von stochastischen Prozessen in Simulationswerkzeugen zu mildern, wurden mehrere Tools entwickelt, die den Einsatz von stochastischen Prozessen erleichtern sollen. Die Implementierung des oben beschriebenen Vorgehens zur Parameteranpassung von CAPPs wurde in das Toolset ProFiDo [BBK10] integriert. ProFiDo ist ein Framework zur Parameteranpassung von Verteilungen und Prozessen, das bereits Verfahren für Phasenverteilungen enthält und somit eine einfache Einbindung der Anpassung von CAPPs ermöglicht. Für das Simulationstool OMNeT++ [HV08],

das hauptsächlich zur Simulation von Rechnernetzen eingesetzt wird, für die seit langem bekannt ist, dass z.B. Zwischenankunftszeiten von Paketen Korrelationen und Abhängigkeiten aufweisen, wurde ein Modul zur Erzeugung von Zufallszahlen aus stochastischen Prozessen entwickelt [KB11], das neben CAPPs auch MAPs, ARMA- und ARTA-Prozesse unterstützt.

5 Experimente

Um die Qualität unseres Verfahrens zur Parameteranpassung einschätzen zu können wurden Experimente mit künstlich erzeugten und realen Traces durchgeführt. Aus Platzgründen sollen hier nur einige repräsentative Ergebnisse gezeigt werden. Eine umfangreiche experimentelle Bewertung findet sich in [Kri12]. Für die Bewertung wurden die Parameter von CHEPs/CAPPs an Tracedaten angepasst. Zum Vergleich wurden außerdem z.B. MAPs angepasst, da diese ebenfalls PH-Verteilungen als Grundlage nutzen, die Korrelation aber anders modelliert wird. Zur Einschätzung der Qualität zeigen wir Plots der Autokorrelationskoeffizienten und der Verteilungsfunktion. Zusätzlich wurden die Prozesse zur Erzeugung von Ankünften im einem simplen Warte/Bediensystem mit Queue-Länge 10 genutzt. Hier dient die Verteilung der Warteschlangenlänge als Vergleichsmaß.

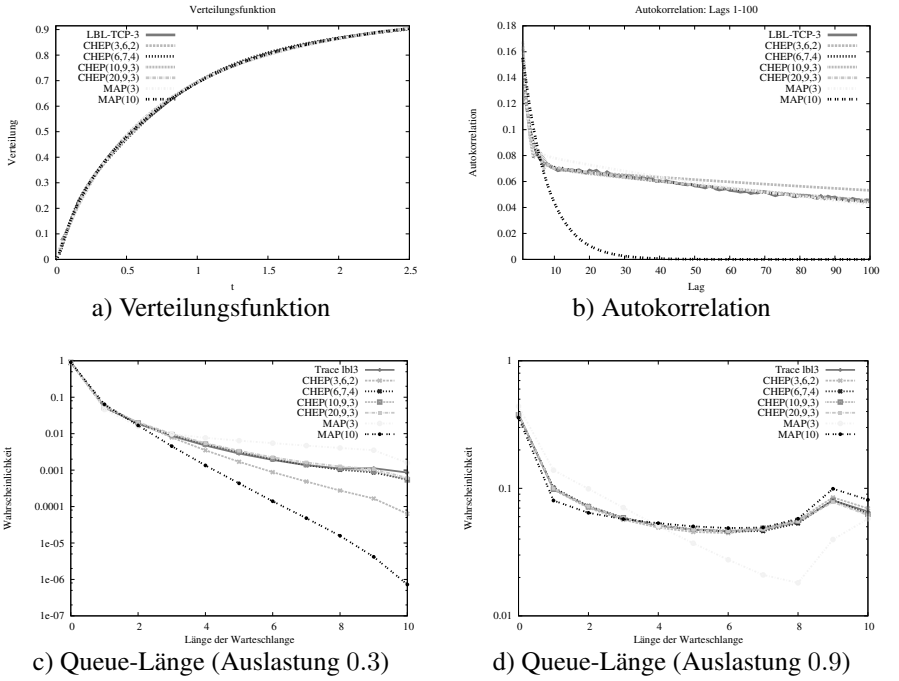
Abbildung 2 zeigt die Ergebnisse für den Trace *LBL-TCP-3* [PF95]. Aus der Abbildung lässt sich erkennen, dass die Anpassung der Verteilung für alle Modelle adäquat möglich war. Bei der Anpassung der Autokorrelation zeigt sich allerdings, das sich die Parameteranpassung für MAPs insbesondere bei einer größeren Anzahl von Zuständen schwierig gestaltet. Für CHEPs/CAPPs war hingegen in allen Fällen eine gute Anpassung möglich. Diese Erkenntnisse spiegeln sich auch im Queueing-Verhalten wider. Insbesondere für größere CHEPs/CAPPs ist die Verteilung der Queue-Länge nah an dem Verhalten für den realen Trace, während mit MAPs nur eine schlechtere Approximation möglich war.

6 Fazit

In diesem Artikel wurde ein Ansatz zur Modellierung von korrelierten Verkehrsdaten vorgestellt, der ARMA-Prozesse zur Modellierung der Korrelation und Phasenverteilungen zur Modellierung der empirischen Verteilung in einem neuen Prozesstyp kombiniert. Zur Parameteranpassung wurde ein Algorithmus skizziert, der in das bestehende Toolset ProFiDo integriert wurde. Anhand von Experimenten mit realen Daten wurde gezeigt, dass die Prozesse in der Lage sind sowohl Verteilung als auch Korrelation geeignet abzubilden.

Literatur

[AO97] S. Asmussen und C. A. O'Cinneide. Matrix-Exponential Distributions - Distributions with a Rational Laplace Transform. In *Encyclopedia of Statistical Sciences*, Seiten



a) Verteilungsfunktion b) Autokorrelation

c) Queue-Länge (Auslastung 0.3) d) Queue-Länge (Auslastung 0.9)

Abbildung 2: Ergebnisse für den Trace *LBL-TCP-3*

435–440, New York, 1997. John Wiley & Sons.

[BBK10] F. Bause, P. Buchholz und J. Kriege. ProFiDo - The Processes Fitting Toolkit Dortmund. In *Proceedings of QEST 2010*, Seiten 87–96. IEEE Computer Society, 2010.

[BD98] P.J. Brockwell und R.A. Davis. *Time Series: Theory and Methods*. Springer, 1998.

[BJ70] G. E. P. Box und G. M. Jenkins. *Time Series Analysis - Forecasting and Control*. Holden-Day, 1970.

[BK09] P. Buchholz und J. Kriege. A Heuristic Approach for Fitting MAPs to Moments and Joint Moments. In *Proceedings of QEST 2009*, Seiten 53–62, 2009.

[BN05] B. Biller und B.L. Nelson. Fitting Time-Series Input Processes for Simulation. *Operations Research*, 53(3):549–559, 2005.

[CB96] M.E. Crovella und A. Bestavros. Self-Similarity in World Wide Web Traffic: Evidence and Possible Causes. In *Proceedings of SIGMETRICS '96*. ACM, 1996.

[CN96] M.C. Cario und B.L. Nelson. Autoregressive To Anything: Time-Series Input Processes for Simulation. *Operations Research Letters*, 19(2):51–58, 1996.

[Cum82] A. Cumani. On the Canonical Representation of Homogeneous Markov Processes Modeling Failure-Time Distributions. *Micorelectronics and Reliability*, 22(3), 1982.

[CZS10] G. Casale, E.Z. Zhang und E. Smirni. Trace Data Characterization and Fitting for Markov Modeling. *Performance Evaluation*, 67(2):61–79, 2010.

[Dev86] L. Devroye. *Non-Uniform Random Variate Generation*. Springer, New York, 1986.

[DW90] Z. Drezner und G. O. Wesolowsky. On the Computation of the Bivariate Normal Integral. *Journal of Statistical Computation and Simulation*, 35:101 – 107, 1990.

[HV08] R. Hornig und A. Varga. An Overview of the OMNeT++ Simulation Environment. In *Proceedings of SIMUTools*, 2008.

[KB11] J. Kriege und P. Buchholz. Simulating Stochastic Processes with OMNeT++. In *Proceedings of the 4th International OMNeT++ Workshop*, 2011.

[Kri12] J. Kriege. *Fitting Simulation Input Models for Correlated Traffic Data*. Dissertation, Technische Universität Dortmund, Fakultät für Informatik, 2012.

[LK00] A. M. Law und W. D. Kelton. *Simulation Modeling and Analysis*. McGraw-Hill, Boston, 3rd. Auflage, 2000. ISBN 0-07-059292-6.

[LM03] A.M. Law und M.G. McComas. How The Expertfit Distribution-Fitting Software Can Make Your Simulation Models More Valid. In *Proceedings of the Winter Simulation Conference 2003*, Seiten 169–174, 2003.

[LMT93] M. Livny, B. Melamed und A. K. Tsiolis. The Impact of Autocorrelation on Queueing Systems. *Management Science*, 39:322–339, 1993.

[LTWW94] W. Leland, M. Taqqu, W. Willinger und D. Wilson. On the Self-Similar Nature of Ethernet Traffic. *IEEE/ACM Transactions on Networking*, 2(1):1–15, 1994.

[Neu81] M. F. Neuts. *Matrix-Geometric Solutions in Stochastic Models*. Johns Hopkins University Press, 1981.

[PF95] V. Paxson und S. Floyd. Wide-Area Traffic: The Failure of Poisson Modeling. *IEEE/ACM Transactions on Networking*, 3:226–244, 1995.

[PTVF93] W. H. Press, S. A. Teukolsky, W. T. Vetterling und B. P. Flannery. *Numerical Recipes in C - The Art of Scientific Computing*. Cambridge University Press, 2nd. Auflage, 1993.

[Ste94] W.J. Stewart. *Introduction to the Numerical Solution of Markov Chains*. Princeton University Press, 1994.

[TBT06] A. Thümmler, P. Buchholz und M. Telek. A Novel Approach for Phase-Type Fitting with the EM Algorithm. *IEEE Transactions on Dependable and Secure Computing*, 3(3):245–258, 2006.

[Whe80] R.E. Wheeler. Quantile Estimators of Johnson Curve Parameters. *Biometrika*, 67(3), 1980.



Jan Kriege studierte von 2001-2006 Informatik an der TU Dortmund und ist seit 2006 wissenschaftlicher Mitarbeiter in der Arbeitsgruppe „Modellierung und Simulation“. Nach seiner Diplomarbeit über logistische Netze beschäftigte er sich während der Promotion, die er 2012 abschloss, mir der Modellierung von Computer- und Kommunikationsnetzen. Seit 2012 ist Jan Kriege Lehrbeauftragter an der Universität Duisburg-Essen.

Messungen und Datenanalyse in Anbetracht von Rauschen und komplexem Bias – Fortschritte aus verbesserten bioinformatischen Algorithmen*

Paweł P. Łabaj
Chair of Bioinformatics, Boku University Vienna
pawel.labaj@boku.ac.at

Abstract: Die hier vorgestellte kumulative Dissertation im Bereich der Bioinformatik spiegelt die Bandbreite dieses Gebiets wieder und spannt einen Bogen von der direkten Auswertung von Meßergebnissen, über die Detektion von Signalen in einem komplexen Hintergrund, bis zur Frage der optimalen dynamischen Ressourceallokation bei der Exekution mehrstufiger Analyseabläufe. In jedem der Bereiche werden beispielhaft Fortschritte durch moderne bioinformatische Ansätze präsentiert. Insbesondere zeige ich (1) wie Genexpressionsmessungen aus Sequenziermethoden der nächsten Generation verbessert werden können, (2) wie empirische anwendungsspezifische Hintergrundmodelle die Entdeckung neuer funktionaler Proteinsequenzmotive auch in Proteinregionen von starkem kompositionellen Bias erlauben, und (3) erste Schritte auf bei der Überwachung von Ressourcebedarf in heterogenen Analyseabläufen in der Cloud.

1 Einleitung

Bioinformatik ist eine sehr heterogene Forschungsdisziplin: computergestützte Methoden werden eingesetzt, um Erkenntnisse aus biomedizinischen Daten zu gewinnen [Mus11]. Zu diesem Zweck werden entweder etablierte Methoden und Werkzeuge verwendet, um neue Daten bezüglich bestimmter biologischer Fragestellungen zu durchsuchen, oder es werden neue Methoden und Werkzeuge entwickelt und mit gut charakterisierten Datensets getestet. In beiden Fällen ist das Ziel, interessante Muster in Daten aus Laborexperimenten zu finden, die entweder von einem selber oder von Kooperationspartnern gemessen wurden, oder aus öffentlichen Datenbanken stammen.

2 Charakterisierung und Reduktion von Meßrauschen

Im Allgemeinen bestimmt die Meßgenauigkeit von Experimenten die Fähigkeit einer jeden Analyse, relevante Signale zuverlässig zu bestimmen – wie etwa die Unterschiede

*Englischer Titel der Dissertation: 'Measurement and data analysis in the face of noise and complex backgrounds – Advances from improved bioinformatics algorithms'

in einer Rastersuche (‘screen’) für differentielle Expression. Die Charakterisierung und Reduzierung des Rauschens ist daher ein wesentliches Ziel, um so eine höhere Analysenempfindlichkeit zu erreichen. Dies ist besonders für die neuartigen Hochdurchsatztechnologien aktuell, wie beispielsweise Plattformen für die genomweite Expressionsprofilierung mittels Microarray-Hybridisierung oder Sequenziermethoden der nächsten Generation („RNA-Seq“).

In RNA-Seq Protokollen werden Gentranskripte („RNAs“) sequenziert, welche die Aktivität der jeweiligen Gene indirekt widerspiegeln. Die resultierenden Daten bestehen dann aus vielen Millionen kurzer Sequenzstücke(den ‘Reads’). Die Anzahl von Reads, die zu einem bestimmten Gen passen, ist ein Maß seiner Expression (Aktivität). Während die Detektion neuer Transkripte mit der Gesamtzahl der sequenzierten Reads wächst, so stellen die nicht-zufällige Natur der biologischen Sequenzen und die stark asymmetrischen Verteilung deren Häufigkeiten eine wesentliche Herausforderung dar. Das betrifft speziell Studien zur Genregulation, weil die hier biologisch interessanten Gene, die Transkriptionsfaktoren, bereits in sehr geringer Kopienzahl biologisch kausal aktiv sein können.

Beim Einsatz von RNA-Seq zur Quantifizierung von Genexpression stellt sich die Frage, inwieweit Probleme bei der Detektion von Genen in kleinen Kopiezahlen die Qualität der Meßergebnisse bestimmen [JW09, TWP+10]. Meine Arbeit präsentiert dazu die erste umfassende Studie zur Zuverlässigkeit dieser Messungen [LLL+11]: Trotz der generell guten Korrelation zwischen wiederholten Messungen, kann diese Korrelation durch eine kleine Anzahl hoch exprimierter Transkripten dominiert werden, was im Einklang mit der beobachteten geringen Meßgenauigkeit für schwach exprimierte Transkripte steht [MWM+08].

Viele Gene haben verschiedene Spleißformen, die auch biologisch unterschiedliche Aktivitäten zeigen. Die Identifizierung der Spleißstellen ist essentiell für die zuverlässige Bestimmung und Quantifizierung von Spleißformen. Ich habe nun einen hybriden Ansatz für die Analyse von RNA-Seq Reads entwickelt, welcher Wissen über bekannte Spleißformen schon im Alignierungsschritt verwendet, wodurch die Identifizierung von Spleißstellen um das 2–3-fache verbessert werden konnte [LLL+11]. Als Ergebnis konnte ich die Anzahl der zuverlässig gemessenen Transkripte um 50% erhöhen. Um die Methode in der biomedizinischen Forschergemeinschaft leichter zugänglich zu machen, habe ich den Algorithmus auch als bedienerfreundliches Programm implementiert und validiert [LLWK12].

Selbst mit den verbesserten Analysemethoden konnten jedoch nur 41% aller bekannter Transkripte zuverlässig gemessen werden. Meine Analyse zeigt, daß über 75% aller Read-Treffer aus nur 7% des bekannten Transkriptoms kommen, und 99,5% aller Read-Treffer von 41% der bekannten Transkripte herrühren. Folglich stehen nur 0,5% der zugeordneten Reads für die Bewertung der verbleibenden 59% der Transkripte zur Verfügung. Das bedeutet auch, daß der größte Teil der Teststärke der Messung für die Mehrzahl der Transkripte nicht zur Verfügung steht.

Ich habe dann gezeigt, daß der beschriebene Effekt nicht leicht durch eine Erhöhung der Sequenzierungstiefe zu überwinden ist. Jede Verdopplung der Sequenzierungstiefe ergibt nur 5% mehr zuverlässig quantifizierbare Transkripte. Das legt nahe, die Stärke von RNA-Seq zur Identifizierung neuer Transkriptsequenzen einzusetzen, und dann zur effizienten quantitativen Messung benutzerdefinierte Microarrays einzusetzen [LTS+08].

Es sollte angemerkt werden, daß meine Arbeit zur Charakterisierung und Reduktion von Rauschen in RNA-Seq die Notwendigkeit und den Nutzen solcher grundlegender Studien neuartiger Technologien unterstreicht. Komplementär zu Untersuchungen systematischer Fehler, erlaubt uns doch nur ein gutes Verständnis der Rauschcharakteristik einer Meßmethode, effiziente Analyseansätze zu entwickeln und zu validieren, welche zur verläßlichen Extraktion biologisch relevanter Ergebnisse unerläßlich sind.

3 Erkennung von Signalen in einem komplexen Hintergrund

Die funktionale Interpretation genomweiter Daten aus Hochdurchsatz-Technologien bleibt eine wesentliche Herausforderung. Dabei werden weniger der technische Aufwand als konzeptuelle Schwierigkeiten in der Interpretation von Ergebnissen zu wesentlichen Stolpersteinen. Im Allgemeinen ist die Identifizierung biologisch relevanter Unterschiede oder konservierter Muster in einem „Hintergrund“ funktional bedeutungsloser Variation von Interesse. In der Analyse von Proteinsequenzen bedeutet dies die Detektion funktionaler Motive innerhalb nicht-funktionaler Variation. Es wird immer offensichtlicher [AWG+05], daß dieser Hintergrund nicht einheitlich ist, was die Entwicklung adaptiver Algorithmen mit komplexen Modellen zu einem aktiven und wichtigen Forschungsfeld macht.

Für eine Analyse, die eine sensitive und spezifische Detektion biologisch relevanter Signalen in einem variablen Hintergrund ermöglicht, sind nicht-triviale Ansätze erforderlich, die diese Hintergrundeffekte „abziehen“ können [XK05, TST+08]. Es stellt sich heraus, daß die Qualität der Analyse direkt von der Qualität des Hintergrundmodells abhängt [AWZY10]. Einige der ersten solcher kontextspezifischer Ansätze sind die Algorithmen, welche für die Erstellung der Proteinsequenz-Datenbank ‘Pfam’ verwendet wurden. Dabei werden die Hintergrundmodelle so angepaßt, daß sie die Natur der untersuchten Datensätze und die Fragestellung berücksichtigen [SED97]. Analog kann man adaptive Sequenzähnlichkeiten berechnen, indem Substitutionsfrequenzen auf die Aminosäurezusammensetzung jedes einzelnen Proteins eingehen [AWG+05]. Die jüngsten Entwicklungen in dem Feld sind problemspezifische Hintergrundmodelle, wie etwa die Erweiterung des Hintergrundmodells für die Bewertung von multiplen Sequenzalignierungen um die Sekundärstruktur der enthaltenen Sequenzen [SG08a].

Es lohnt sich zu überlegen, wie die Wahl eines Referenzdatensatzes die Fragenstellung beeinflußt, welche in einer Analyse untersucht werden können. Umgekehrt legt die Fragestellung fest, welche Referenzdatensätze für die Konstruktion eines Hintergrundmodells geeignet sind. Speziell, wenn es sich um Regionen mit ungewöhnlich niedriger Komplexität handelt: Diese Regionen sind in der Regel nicht konserviert, und werden daher als funktional irrelevant eingestuft. Also werden diese Bereiche in typischen Sequenzanalysen, wie Homologiesuchen und funktionaler Annotation, von vornherein ausgefiltert [WF93]. Es gibt jedoch zunehmend anekdotische Hinweise darauf, daß auch diese Regionen funktionale Rollen haben [KO03, KH06], wobei die prominentesten Beispiele homopolymere Aminosäureketten sind, die mit einer Reihe von Krankheiten in Verbindung gebracht werden [SG08b].

Bemerkenswert ist, daß die beobachteten Häufigkeiten dieser Ketten sich nicht nur der

Analyse mit Standardmodellen widersetzen [KBB+02]. Ich konnte zeigen, daß sie selbst von Markov-Ketten höherer Ordnung nicht vorhergesagt werden können [LSK11]. In der Arbeit, die ich hier präsentiere [LLB+10, LSK11], wird der Stellenwert der Entwicklung und Validierung von Modellen speziell für die gegebene Problemstellung durch eine Beispielstudie unterstrichen. In einer quantitativen Analyse der Verteilung homopolymerer Aminosäureketten konnte ich die unerwartete Anreicherung bestimmter Ketten in Signalpeptiden zeigen.

Mein Ergebnis stellt nun die erste Evidenz für eine funktionale Rolle einer ganzen Klasse von Aminosäureketten dar. Insbesondere zeige ich, daß Homopolymere aus Leucin in Signalpeptiden überrepräsentiert sind, nicht aber Ketten aus anderen hydrophoben Aminosäuren. Dieser Effekt ist am deutlichsten in Säugetieren. In menschlichen Proteinen finden sich circa 2/3 aller Leucinketten in Signalpeptiden – und das, obwohl weniger als 1/5 aller Proteine ein Signalpeptid haben. Das mag auch erklären, warum Leucinketten trotz ihrer generellen Toxizität [OKSI05] so häufig auftreten können. Interessanterweise und im Gegensatz zum allgemeinen Trend [SPG06] konnte ich für diese Homopolymere eine stärkere Konservierung zwischen Spezies zeigen als für die angrenzenden Sequenzen im Signalpeptid. Diese divergieren im Lauf der Evolution rascher als das restliche Protein [LXD+09]. Zusammen weist das stark auf eine noch unbekannte funktionale Rolle der Leucinketten hin.

Aus einem anderen Blickwinkel ist bemerkenswert, daß die langen Leucinketten, welche die am weitest verbreiteten Aminosäurehomopolymere darstellen, vor allem in transienten Proteinregionen vorkommen, welche aber im endgültigen Proteinprodukt ja abgespalten werden. Das zeigt, daß eine systematische Analyse von Proteinsequenzen, ohne eine getrennte Behandlung transienter Regionen ein stark verzerrtes Bild geben kann. Im diesem Fall betrifft das immerhin gut 1/5 aller Proteine in Säugern und verwandten Spezies.

Die hier vorgestellte Arbeit ist noch von weiterer Relevanz: Auch wenn die präsentierte beispielhafte Analyse von Aminosäureketten in Signalpeptiden einen sehr speziellen Anwendungsfall darstellt, so ist die Demonstration unseres Ansatzes der Entwicklung und des Einsatz eines empirischen anwendungsspezifischen Hintergrundmodells, direkt angepaßt an die untersuchten Daten einerseits und die zu beantwortende Frage andererseits, viel allgemeiner nützlich. Generell sucht man nämlich in der Mehrzahl der wissenschaftlichen Fragen nach einem Signal oder Muster innerhalb eines unbekannten komplexen Hintergrunds, da die Struktur und Störfaktoren in den Modellresiduen üblicherweise nicht bekannt sind [LS07].

4 Systeme für komplexe Analysen

Moderne Analysen in der Bioinformatik erfordern oft einen komplexen Ablauf mehrerer voneinander abhängiger Programmschritte. Die effiziente Ausführung dieser Schritte kann durch sogenannte Workflow-Systeme unterstützt werden. Die Anforderungen an solche Systeme in der bioinformatischen Forschung bringen jedoch eine Reihe spezifischer technischer und organisatorischer Herausforderungen mit sich, die über die in anderen wissenschaftlichen Disziplinen und allgemeinen Workflow-Systemen hinausgehen

[Kre01, Ste08].

Neben klassischen statischen Notwendigkeiten, wie der eingänglichen Datenkonvertierung, und Bedürfnissen zur Laufzeit, wie bei kontinuierlichen Konsistenzprüfungen, bringt die Arbeit mit wissenschaftlichen Workflows in der Bioinformatik weiters zusätzliche Herausforderungen über die gesamte Lebensdauer eines wissenschaftlichen Projektes. Insbesondere ist es durchaus üblich, daß der exakte Weg einer Analyse nicht im voraus bekannt ist, weil a priori viele Studien explorativ sind, und Daten untersuchen, die nicht nur neue Meßwerte bringen sondern auch unbekannte Strukturen aufweisen.

Effizienz-Erwägungen werden umso wichtiger, wenn Berechnungen teuer sind. Einerseits ist dies der Fall, wenn die moderne fortgeschrittene Modelle eingesetzt werden. Ihre Anwendung kann bereits für kleine Datensätze ressourcenintensiv sein [LSK11]. Auf der anderen Seite wird auch die Durchführung einfacher ad-hoc Ansätze nicht trivial bei der Analyse massiver Datensätze. Dieses Problem wird mit der rasenden Verbreitung von Hochdurchsatztechnologien wie moderner Microarrays und der Sequenziermethoden der nächsten Generation hochaktuell [Pen11]. Das traditionelle Arbeitsmodell im Gebiet, bei dem alle Daten zur lokalen Analyse aus dem Internet geholt werden, trifft immer mehr auf limitierte Bandbreiten. Oft ist die einzige praktische Lösung, Daten auf Festplatten mit der Post zu verschicken, oder Rechnungen auf entfernte Knoten zu verteilen, wo die Daten bereits in einer 'Cloud Computing'-Umgebung vorliegen.

Workflow-Management-Systeme sollten daher die notwendigen Abstraktionen zur Verfügung stellen, die die effektive Nutzung von Rechen- und Daten-Ressourcen ermöglichen [Rom08], um es Forschern zu erlauben, sich auf die Durchführung der Datenanalyse und deren Interpretation zu konzentrieren, damit sie effizient Entscheidungen treffen können, wann immer in der Analyse menschliche Weichenstellungen nötig werden. Auch wenn jedes der untersuchten gängigen Systeme manche dieser Fragen anspricht, gibt es kein System, das die nötigen Erfordernisse ausreichend erfüllt, und es ist hier noch ausreichend Raum für weitere Entwicklungen. Dabei ist festzuhalten, daß bestehende Workflow-Management-Systeme im Allgemeinen für die wiederholte Anwendung von Standard-Analysen entwickelt worden sind, welche aber typischerweise in einem industriellen Kontext zu finden sind, im Gegensatz zu hochdynamischen akademischen Anwendungsszenarios. Die Spezifikation neuer Komponenten oder Änderungen an einem Workflow sind nicht ausreichend leicht und können nicht flexibel genug auf dynamische Änderungen eingehen, die häufig in typischen wissenschaftlichen Analyse-Workflows in allen Bereichen zu erwarten sind, sei das nun in den Analyse-Anforderungen selbst, in externem Programmcode, oder öffentlichen Datenquellen.

Darüber hinaus setzen viele moderne Workflow-Systeme auf Web-basierte Dienste. Während der Einsatz von Analyse-Code über das Internet eine elegante und einfache Möglichkeit ist, um eine Vielzahl von Analyse-Werkzeugen zu verbinden, so bringen Abhängigkeiten von verteilten Ressourcen zusätzliche organisatorische und technische Herausforderungen. Insbesondere können Serviceverfügbarkeit variieren und Dienstleistungen in ihrer Implementation von Anbietern auch kurzfristig verändert werden [LGG11]. Das kann dann Eingabe- wie Ausgabeformate, Analyseparameter und Semantik betreffen. Selbst wenn Ausfälle und Versionsänderungen rechtzeitig angekündigt werden, so bleiben sie dennoch außerhalb der Kontrolle der Service-Nutzer und des Workflow-Systems. Kri-

tisch ist hier insbesondere, daß solche Änderungen unerwartete Effekte haben können, die im besten Fall zum Analyseabbruch und im schlimmsten Fall falsche oder inkonsistente Ergebnisse. Sogar wenn sogenannte Service Level Agreements eingesetzt werden, bleiben ernsthafte Probleme. Kommunikation ist oft nicht verschlüsselt, und ohne starke Authentifizierung und Datenverschlüsselung können weder Datenintegrität noch Vertraulichkeit garantiert werden. Schließlich sind Web-basierte Dienste auf einzelnen Server-Rechnern für die Analyse neu generierter großen Datensätze aufgrund der schieren Größe der Eingangsdaten und des entsprechend hohen Rechenaufwands begrenzt einsetzbar [Pen11].

Wenn wir uns nun Gedanken zum Ressourcenbedarf machen, so ist es erwähnenswert, daß die verschiedenen Analyseschritte sehr unterschiedliche Anforderungen in Bezug auf Rechenleistung, Speicherverbrauch, Speichersystem-Leistung und -Kapazität haben. Darüber hinaus können sich die Ressourcenbedürnisse einer komplexen Analysewährend ihrer Ausführung ändern. Rechenumgebungen, die eine flexible Zuweisung von Ressourcen erlauben können inzwischen durch die Integration einer Infrastruktur für verteiltes Rechnen geschaffen werden, wobei Cloud-Umgebungen, Rechnernetzwerke ('Compute Grids') und lokalen Rechnergruppen ('Cluster') zum Einsatz kommen [Ste08]. Es zeigt sich, daß das gezielte Management von Rechenressourcen eine weitere Anforderung für ein effizientes Workflow-System darstellt, das groß angelegte wissenschaftliche Analysen in der Bioinformatik unterstützen kann. Aktuelle Implementierungen integrieren jedoch solch ein Ressourcenmanagement nicht. Damit ist eine verteilte Rechen-Infrastruktur noch nicht effizient einsetzbar, wenn eine komplett erfolgreiche Exekution komplexer Analysen gewährleistet werden muß. Ein notwendiger erster Schritt dazu ist die Fähigkeit, die Workflow-Ausführung zu überwachen, um den Ressourcenverbrauchs zu charakterisieren, und den Status verfügbaren Ressourcen zu überwachen. Das ermöglicht dann in weiteren Schritten eine kontinuierliche Optimierung der Ausführung mehrerer Workflows unter Berücksichtigung der Bedürfnisse der gleichzeitig laufenden Programme. Wir haben dafür eine neue Technologie zur Überwachung von Cloud-Ressourcen zusammen mit einer Wissensmanagement-Strategie für die Optimierung von Workflow-Anwendungen Ausführung in Cloud-Umgebungen entwickelt und getestet [ELM+11]. Insbesondere konnten wir zeigen, wie wir Ressourcen-Engpässe zur Laufzeit erkennen und aktives Wissensmanagement einsetzen können, um dynamisch mehr Ressourcen in solchen Fällen zur Verfügung stellen können, um die erfolgreiche komplette Ausführung der Workflow-Anwendung zu garantieren. In zukünftigen Arbeiten wollen wir diese Ansätze in Prototyp-Workflow-Systemen integrieren, um die Konstruktion tiefer, komplexerer bioinformatischer Analysen zu unterstützen, inklusive der semi-interaktiven explorativen Datenanalyse Schritt-für-Schritt, die für zielgerichtete Analysen gerade in unbekanntem Terrain notwendig ist.

5 Publizierte Resultate meiner Arbeit im Überblick

Schlußendlich basieren alle Analysen auf Daten, die an irgendeinem Punkt gemessen worden sind. Dabei unterliegt jede Messung Fehlern, die entweder rein zufällig sind oder einen systemischen Bias widerspiegeln. Während die Notwendigkeit einer Charakterisie-

rung und Entfernung von Bias zunehmend erkannt wird, werden zufällige Fehler (das „ Rauschen“) nach wie vor oft nur implizit behandelt. Ich habe in meiner Arbeit gezeigt, wie Datenverarbeitungsmethoden einen wesentlichen Einfluß auf das Meßrauschen haben, und wie man entsprechend das Rauschen wesentlich reduzieren kann, um so die Sensitivität und Teststärke folgender Analysen quantitativer RNA-Seq Genexpressionsprofile zu erhöhen [LLL+11, LLWK12].

Zur Identifizierung biologisch relevanter Signale in einer See bedeutungsloser Variationen, ist es zuallererst nötig, die Natur dieses Hintergrunds zu verstehen und zu modellieren. Anhand einer beispielhaften Studie der Überrepräsentation bestimmter Aminosäureketten in Proteinsequenzen habe ich einerseits gezeigt, wie sehr applikationsspezifische Hintergrundmodelle in der Analyse von Sequenzen mit kompositionellem Bias notwendig sind. Andererseits demonstriert diese Arbeit und die dabei entdeckte Alleinstellung der in Säugetieren konservierten Überrepräsentation von Leucinketten in Signalpeptiden jedoch auch, daß selbst in schwierigen Situationen mit entsprechenden Modellen quantitative Analysen möglich sind, und zu biologisch besonders spannenden Ergebnissen führen können [LLB+10, LSK11].

Zur Interpretation von Analyseergebnissen sind oft komplexe Abläufe mit mehreren von einander abhängigen Schritten nötig. Dabei werden eine Vielzahl spezialisierter Analyseprogramme und unterschiedlicher Datentypen aus verschiedenen Quellen gemeinsam eingesetzt. Die Exekution dieser Schritte kann durch sogenannte ‘Workflow Systeme’ unterstützt werden. Solche Systeme werden mit den rasch anwachsenden Datenvolumen, die eine interaktive manuelle Analyse erschweren, inzwischen hochaktuell. Insbesondere die sich inzwischen stark etablierten Hochdurchsatzmethoden in Biologie und Medizin tragen dazu bei, wozu auch die in meiner Arbeit untersuchte Genexpressionsprofilierung gehört. Bei der Abwicklung dieser Analysen ist eine effiziente Nutzung der verfügbaren Computerressourcen eine knifflige Herausforderung, weil die einzelnen Analyseschritte so unterschiedliche Anforderungen haben können. Anhand eines typischen Beispiels habe ich mit Kollegen aus der Angewandten Informatik gezeigt, wie man ein System konstruieren kann, das den dynamischen Ressourcebedarf eines laufenden Workflow mit dem Ziel überwacht, letztendlich eine optimale Ressourcenzuteilung in einem ‘Cloud Computing System’ zu erwirken [ELM+11].

6 Zusammenfassung

In der Bioinformatik werden biologische Daten mit computergestützten Methoden analysiert. Das Ziel sind neue Erkenntnisse in den Lebenswissenschaften. Diese Dissertation präsentiert eigenständige Arbeiten aus drei ineinandergreifenden Bereichen des Gebiets.

Die moderne Molekularbiologie verwendet ein immer größeres Repertoire an Instrumenten für genomweite quantitative Messungen. Meßfehler setzen sich stets aus zufälligem Rauschen und systematischen Abweichungen zusammen. Meine Untersuchung einer neuen Plattform zur Profilierung von Genexpression durch Sequenziermethoden der nächsten Generation („RNA-Seq “) ergänzt Studien, die Quellen systemischer Fehler identifizieren. In meiner Arbeit zeige ich nämlich, wie Meßrauschen durch die Weiterverarbeitung der

Daten beeinflußt wird, und wie dieser Fehler beträchtlich reduziert werden kann und so die Sensitivität und Effizienz nachfolgender Analysen deutlich erhöht.

Zusätzlich zu der verbesserten genomweiten Messung quantitativer Kenngrößen, kann man auch ein exponentielles Wachstum biologischer Sequenzdaten beobachten. Damit bekommt die funktionale Interpretation dieser Sequenzen eine Schlüsselfunktion in der Bioinformatik. Dabei ist die Suche von biologisch relevanten typischen Mustern und Unterschieden vor dem Hintergrund einer funktional bedeutungslosen Varianz von Interesse. Anhand einer Studie des unerwartet häufigen Auftretens von Homopolymeren bestimmter Aminosäuren zeige ich die Notwendigkeit anwendungsspezifischer Hintergrundmodelle für eine Untersuchung von Sequenzregionen mit unüblichen Aminosäurezusammensetzungen.

Mit der Vielzahl an Datenquellen wachsen schließlich Komplexität und Rechenaufwand einer typischen Analyse, und legen Systeme zur Steuerung des Analysenablaufs nahe. Ich zeige hier, wie ein solches System aufgebaut werden kann, das dynamisch die heterogenen Ressourcenbedürfnisse der einzelnen Analyseschritte überwacht, um die Effizienz in einer Rechnerwolke zu optimieren.

Literatur

[AWG+05] Stephen F. Altschul, John C. Wootton, E. Michael Gertz, Richa Agarwala, Aleksandr Morgulis, Alejandro A. Schäffer und Yi-Kuo Yu. Protein database searches using compositionally adjusted substitution matrices. *FEBS J.*, 272(20):5101–9, 2005.

[AWZY10] Stephen F. Altschul, John C. Wootton, Elena Zaslavsky und Yi-Kuo Yu. The Construction and Use of Log-Odds Substitution Scores for Multiple Sequence Alignment. *PLoS Comput Biol*, 6(7):e1000852, 07 2010.

[ELM+11] Vincent Chimaobi Emeakaroha, Paweł Łabaj, Michael Maurer, Ivona Brandic und David P. Kreil. Optimizing Bioinformatics Workflows for Data Analysis Using Cloud Management Techniques. In *The 6th Workshop on Workflows in Support of Large-Scale Science*, Seattle, November 2011.

[GGM+10] Malachi. Griffith, Obi L. Griffith, Jill Mwenifumbo, Rodrigo Goya, A. Sorana Morrissy, Ryan D. Morin, Richard Corbett, Michelle J. Tang, Ying-Chen Hou, Trevor J. Pugh, Gordon Robertson, Suganthi Chittaranjan, Adrian Ally, Jennifer K. Asano, Susanna Y. Chan, Haiyan I. Li, Helen McDonald, Kevin Teague, Yongjin Zhao, Thomas Zeng, Allen Delaney, Martin Hirst, Gregg B. Morin, Steven J. M. Jones, Isabella T. Tai und Marco A. Marra. Alternative expression analysis by RNA sequencing. *Nat Methods*, 7(10):843–847, 2010.

[JW09] Hui Jiang und Wing Hung Wong. Statistical inferences for isoform expression in RNA-Seq. *Bioinformatics (Oxford, England)*, 25(8):1026–1032, April 2009.

[KBB+02] Samuel Karlin, Luciano Brocchieri, Aviv Bergman, Jan Mrazek und Andrew J. Gentles. Amino acid runs in eukaryotic proteomes and disease associations. *Proc Natl Acad Sci U S A*, 99(1):333–8, 2002.

[KH06] Igor B. Kuznetsov und Seungwoo Hwang. A novel sensitive method for the detection of user-defined compositional bias in biological sequences. *Bioinformatics*, 22(9):1055–1063, 2006.

[KO03] David P. Kreil und Christos A. Ouzounis. Comparison of sequence masking algorithms and the detection of biased protein sequence regions. *Bioinformatics*, 19(13):1672–81, 2003.

[Kre01] David P. Kreil. *From General Scientific Workflows to Specific Sequence Analysis Applications: The study of compositionally biased proteins*. Dissertation, University of Cambridge, 2001.

[LBA+09] Joshua Z. Levin, Michael F. Berger, Xian Adiconis, Peter Rogov, Alexandre Melnikov, Timothy Fennell, Chad Nusbaum, Levi A. Garraway und Andreas Gnirke. Targeted next-generation sequencing of a cancer transcriptome enhances detection of sequence variants and novel fusion transcripts. *Genome Biol*, 10(10):R115, 2009.

[LGG11] Burkhard Linke, Robert Giegerich und Alexander Goesmann. Conveyor: a workflow engine for bioinformatic analyses. *Bioinformatics*, 27(7):903–911, 2011.

[LLB+10] Paweł P. Łabaj, Germán G. Leparc, Anaïs F. Bardet, Günther Kreil und David P. Kreil. Single amino acid repeats in signal peptides. *FEBS Journal*, 277(15):3147–3157, 2010.

[LLL+11] Paweł P. Łabaj, Germán G. Leparc, Bryan E. Linggi, Lye Meng Markillie, H. Steven Wiley und David P. Kreil. Characterization and improvement of RNA-Seq precision in quantitative transcript expression profiling. *Bioinformatics*, 27(13):i383–i391, 2011.

[LLWK12] Paweł P. Łabaj, Bryan E. Linggi, H. Steven Wiley und David P. Kreil. Improviong RNA-Seq precision with MapAl. *Frontiers in Genetics*, 2012. in press.

[LS07] Jeffrey T Leek und John D Storey. Capturing Heterogeneity in Gene Expression Studies by Surrogate Variable Analysis. *PLoS Genet*, 3(9):e161, 09 2007.

[LSK11] Paweł P. Łabaj, Peter Sykacek und David P. Kreil. An analysis of single amino acid repeats as use case for application specific background models. *BMC Bioinformatics*, 12(1):173, 2011.

[LTS+08] Germán G. Leparc, Thomas Tüchler, Gerald Striedner, Karl Bayer, Peter Sykacek, Ivo L Hofacker und David P Kreil. Model-based probe set optimization for high-performance microarrays. *Nucleic Acids Res*, Dec 2008.

[LXD+09] Yu-Dong Li, Zhong-Yu Xie, Yi-Ling Du, Zhan Zhou, Xu-Ming Mao, Long-Xian Lv und Yong-Quan Li. The rapid evolution of signal peptides is mainly caused by relaxed selection on non-synonymous and synonymous sites. *Gene*, 436(1-2):8–11, 2009.

[Mus11] Arcady Mushegian. Grand Challenges in Bioinformatics and Computational Biology. *Frontiers in Genetics*, 2(0), 2011.

[MWM+08] Ali Mortazavi, Brian A Williams, Kenneth McCue, Lorian Schaeffer und Barbara Wold. Mapping and quantifying mammalian transcriptomes by RNA-Seq. *Nat Meth*, 5(7):621–628, Juli 2008.

[OKSI05] Yoko Oma, Yoshihiro Kino, Noboru Sasagawa und Shoichi Ishiura. Comparative analysis of the cytotoxicity of homopolymeric amino acids. *Biochim Biophys Acta*, 1748(2):174–9, 2005.

[Pen11] Elizabeth Pennisi. Will Computers Crash Genomics? *Science*, 331(6018):666–668, 2011.

[Rom08] Paolo Romano. Automation of in-silico data analysis processes through workflow management systems. *Briefings in Bioinformatics*, 9(1):57–68, 2008.

[SED97] Erik L. L. Sonnhammer, Sean R. Eddy und Richard Durbin. PFAM: a comprehensive database of protein domain families based on seed alignments. *Proteins*, 28(3):405–20, 1997.

[SG08a] Ruslan I. Sadreyev und Nick V. Grishin. Accurate statistical model of comparison between multiple sequence alignments. *Nucl. Acids Res.*, 36(7):2240–2248, 2008.

[SG08b] Pratibha Siwach und Subramaniam Ganesh. Tandem repeats in human disorders: mechanisms and evolution. *Front Biosci*, 13:4467–84, 2008.

[SPG06] Pratibha Siwach, Saurabh D. Pophaly und Subramaniam Ganesh. Genomic and evolutionary insights into genes encoding proteins with single amino acid repeats. *Mol Biol Evol*, 23(7):1357–69, 2006.

[Ste08] Lincoln D. Stein. Towards a cyberinfrastructure for the biological sciences: progress, visions and challenges. *Nat Rev Genet*, 9(9):678–688, 2008.

[TST+08] Morgane Thomas-Chollier, Olivier Sand, Jean-Valéry Turatsinze, Rekin's Janky, Matthieu Defrance, Eric Vervisch, Sylvain Brohée und Jacques van Helden. RSAT: regulatory sequence analysis tools. *Nucleic Acids Research*, 36(suppl 2):W119–W127, 2008.

[TWP+10] Cole Trapnell, Brian A. Williams, Geo Pertea, Ali Mortazavi, Gordon Kwan, Marijke J. van Baren, Steven L. Salzberg, Barbara J. Wold und Lior Pachter. Transcript assembly and quantification by RNA-Seq reveals unannotated transcripts and isoform switching during cell differentiation. *Nat Biotech*, 28(5):511–515, 2010.

[WF93] John C. Wootton und Scott Federhen. Statistics of local complexity in amino-acid-sequences and sequence databas. *Computers & chemistry*, 17(2):149–163, 1993.

[WI05] Zhijin Wu und Rafael A Irizarry. Stochastic models inspired by hybridization theory for short oligonucleotide arrays. *Journal of Computational Biology: A Journal of Computational Molecular Cell Biology*, 12(6):882–893, August 2005.

[XK05] Jun Xie und Nak-Kyeong Kim. Bayesian Models and Markov Chain Monte Carlo Methods for Protein Motifs with the Secondary Characteristics. *J Comp Biol*, 12(7):952–970, 2005.



Paweł P. Łabaj wurde am 31. Juli 1982 in Mielec in Polen geboren. Im Jahr 2001 absolvierte er in Zabrze das Gymnasium in einer physikalisch-mathematischen Klasse. In 2006 erhielt von der Schlesischen Technischen Universität in Gliwice den Titel Magister-Ingenieur der Informatik mit Auszeichnung. Seine Masterarbeit über ein System zur automatischen Analyse und Mustererkennung durch neuronale Netze war im Jahr 2006 als beste Arbeit des Jahres in ganz Polen ausgezeichnet worden. Die Arbeit entstand in Zusammenarbeit mit dem Institut für Medizinische Technik und Ausstattung in Zabrze. Danach war Paweł als wissenschaftlichen Mitarbeiter in der Abteilung Biomedizinische Informatik tätig. Im Jahr 2007 nahm er eine Stelle als Predoctoral Research Fellow am Chair of Bioinformatics an der Universität für Bodenkultur Wien an. Seit seiner Promotion ist er als Junior Scientist an diesem Institut beschäftigt. Er interessiert sich für verschiedene Aspekte der Bioinformatik, vor allem die biologische Sequenzanalyse, Next Generation Sequencing, Klassifizierungsmethoden, Merkmalsextraktion, Mustererkennung, Datenintegration und Workflow-Systeme.

Ein maschinengeprüftes, typsicheres Modell der Nebenläufigkeit in Java: Sprachdefinition, virtuelle Maschine, Speichermodell und verifizierter Compiler*

Andreas Lochbihler

Institut für Informationssicherheit, ETH Zürich
andreas.lochbihler@inf.ethz.ch

Abstract: Charakteristisch für die Programmiersprache Java sind sowohl ihre Sicherheitsgarantien wie beispielsweise Typsicherheit und die Sicherheitsarchitektur als auch die direkte Unterstützung von Threads. In der hier vorgestellten Dissertation [Loc12b] wird ein maschinengeprüftes Modell von nebenläufigem Java einschließlich des Java-Speichermodells entwickelt und die Auswirkungen der Nebenläufigkeit auf diese Garantien untersucht. Aus dem formalen Modell wurde automatisch ein ausführbarer Interpreter, Übersetzer und eine virtuelle Maschine einschließlich eines Bytecode-Verifizierers generiert, mit dem das Modell empirisch gegen Java-Benchmarks validiert wurde.

1 Einführung

Typsicherheit und die Sicherheitsarchitektur sind wichtige Garantien der Programmiersprache Java. Sie erlauben es, Code aus nicht vertrauenswürdigen Quellen in einer Sandbox ohne die Gefahr, dass sich das ausführende System mit Schadcode infiziert, auszuführen. Ein weiteres Kennzeichen Javas sind Threads und das Java-Speichermodell (JMM) zur nebenläufigen Ausführung. Verglichen mit dem intuitiven Modell für sequenzielle Konsistenz (SC), bei der die Thread-Einzelschritte verschränkt ausgeführt werden und Speicherveränderungen sofort für alle Threads sichtbar werden, erlaubt das JMM mehr Ausführungen, um aggressive Optimierungen bei der Übersetzung nach Bytecode und in der virtuellen Maschine (VM) selbst zu ermöglichen. Deswegen wirkt sich Nebenläufigkeit auch auf die Typsicherheit und Sicherheitsarchitektur aus, wie seit langem durch Beispiele bekannt ist [GJSB05, Pug00].

Die hier zusammengefasste Dissertation [Loc12b] untersucht diese Auswirkungen nun zum ersten Mal formal. Dazu wird ein formales Modell, genannt JinjaThreads, der Nebenläufigkeit durch Java-Threads einschließlich des JMMs konstruiert und im Detail analysiert. Grundlage des sequenziellen Teils ist Jinja [KN06], das eine sequenzielle Java-ähnliche Programmiersprache mit Quellcode, Bytecode und einem Übersetzer im Beweis-

*Englischer Titel der Dissertation: "A Machine-Checked, Type-Safe Model of Java Concurrency : Language, Virtual Machine, Memory Model and Verified Compiler"

assistent Isabelle/HOL [NPW02] formalisiert und maschinengeprüft als typsicher nachweist. Die Arbeit erweitert dieses Modell um Nebenläufigkeit durch Java-Threads (§2) und das JMM (§3) und überträgt die bisherigen Theoreme zur Typsicherheit und Korrektheit des Übersetzers (§4). Es zeigte sich, dass wegen neu entdeckter Schwachstellen des JMMs Typsicherheit eine Nicht-Standard-Modellierung erfordert und theoretisch sogar die Sicherheitsarchitektur ausgehebelt werden könnte. Zudem beweist die Arbeit die für Programmierer und Programmanalysen wichtige Garantie des JMMs, dass wettlauffreie Programme sich wie bei verschränkter Ausführung, d.h. sequenziell konsistent, verhalten. Insgesamt entstanden so der erste verifizierte Übersetzer für nebenläufiges Java und die erste formale Verbindung zwischen einer operationalen Java-Semantik und dem axiomatisch spezifizierten JMM.

Alle Definitionen und Beweise wurden von Isabelle/HOL geprüft und sind im Archive of Formal Proofs veröffentlicht [Loc07]. Damit zeigt diese Arbeit, dass heutzutage umfangreiche Programmiersprachen in handhabbarer Form in Theorembeweisern abgebildet werden können. Umgekehrt wäre diese Arbeit wegen der Komplexität des Modells ohne Maschinenunterstützung unmöglich gewesen, da nur so alle Auswirkungen einer Änderung oder Erweiterung auf andere Teile des Modells zuverlässig festgestellt werden konnten. Außerdem erlaubte die Verwendung von Isabelle, das formale Modell auszuführen und damit zu validieren (§5). Dazu wurde mit Isabelles Codegenerator automatisch aus der Formalisierung ein Interpreter, ein Übersetzer und eine virtuelle Maschine in Standard ML extrahiert. Durch eine Testsuite von Java-Programmen wurde damit das Modell von Quell- und Bytecode validiert.

2 Thread-Modellierung und verschränkte Ausführungen

Der erste Schritt zum nebenläufigen Modell von Java erweitert das sequenzielle Jinja um Java-Threads. Auf Sprachebene deckt JinjaThreads dynamische, unbeschränkte Thread-Erzeugung, Synchronisation über Monitore, Warten auf Benachrichtigung sowie Unterbrechung und Beitreten von Threads ab. JinjaThreads deckt somit alle Konstrukte für Nebenläufigkeit aus der Sprachspezifikation [GJSB05] außer den missbilligten oder zeitabhängigen Methoden und den Vergleichen-und-Tauschen-Operationen aus dem `java.util.concurrent`-Paket ab. Syntaktisch sind dafür nur geringe Anpassungen der sequenziellen Jinja-Sprache nötig (`synchronized`-Blöcke und `volatile`-Deklarationen), da die anderen Primitive als Aufrufe nativer Methoden realisiert sind.

Dagegen ändert sich die operationale Semantik grundlegend, da Synchronisationsprimitive implementiert und die Threads verschränkt ausgeführt müssen. Damit das Modell handhabbar bleibt, ist es wesentlich, möglichst viele Teile wiederzuverwenden, sowohl von Jinja als auch zwischen Quell- und Bytecode. Dazu wird die Semantik in sieben Schichten zerlegt (Abb. 1), von denen vorerst nur Nr. 2, 3 und 5 relevant sind. Da sowohl Quell- als auch Bytecode die gleichen Nebenläufigkeitskonstrukte benutzen, implementiert ein Transitionssystem $s -t{:}\alpha s\rightarrow s'$ diese sprachunabhängig in Schicht 5; es verschränkt die atomaren Schritte einer als Parameter gegebenen Einzelthreadsemantik (ETS) $t \vdash (x, h) -\alpha s\rightarrow (x', h')$ (t bezeichnet den Thread, x den thread-lokalen Zustand und h



Abbildung 1: Schichtenmodell der Semantik

den gemeinsamen Speicher). Insbesondere übernimmt es vollständig die Verwaltung des globalen Systemzustands s, d.h., der Threads, Sperren, Wartemengen und Unterbrechungen.

Entsprechend kann sich die ETS auf die Umsetzung der Syntax in atomare Berechnungsschritte konzentrieren (Schicht 3). Für Quellcode kann dafür die strukturelle operationelle Semantik (SOS) aus Jinja mit nur kleinen Anpassungen wiederverwendet werden, gleiches gilt für den funktionalen Stil der VM. Dies gilt nicht nur für die Defintionen, sondern auch für die deutlich aufwändigeren Beweise zur Typsicherheit (s.u.). Die Ausführung der Synchronisationsprimitive wird dabei an Schicht 5 delegiert, in dem die Transitionen mit entsprechenden abstrakten Aktionsanweisungen αs versehen werden, beispielsweise fordert *Lock*$\rightarrow l$ eine Sperre auf dem Monitor l an und *Unlock*$\rightarrow l$ gibt sie wieder frei. Für native Methoden werden diese Anweisungen bereits in Schicht 2 generiert und von Schicht 3 lediglich weitergeleitet.

Diese Aktionsanweisungen ermöglichen es, dass die Schichten 3 und 5 jeweils ohne Kenntnis der Implementierung der anderen Schicht definiert werden können. Die vollständige Semantik von Quellcode oder Bytecode erhält man einfach durch Instanziierung des ETS-Parameters. Dadurch ist automatisch sichergestellt, dass die lokalen Zustände der Threads gegen Zugriffe aus anderen Threads geschützt sind, und umgekehrt wird verhindert, dass die ETS direkt den Systemzustand manipulieren kann. Manchmal erfordert dies zwar eine aufwändigere Modellierung einzelner Aspekte. Beispielsweise gibt es in der SOS zwei Transitionen für das Starten eines Threads – eine für den erfolgreichen Start und eine mit einer Ausnahme, falls der Thread schon zuvor gestartet worden war. Dadurch wird die ETS nichtdeterministisch, und erst Schicht 5 entscheidet anhand der Aktionsanweisungen, welche davon im aktuellen Systemzustand die richtige ist. Jedoch stellt diese Trennung sicher, dass Aussagen und Beweise auf einem geeigneten Abstraktionsniveau formuliert bzw. geführt werden können, da alle relevanten Interaktionen zwischen den Threads durch die Aktionsanweisungen erfasst werden. Dies reduziert die Komplexität der Beweise und fördert die Wiederverwendung, wie am Beweis der Typsicherheit gut zu sehen ist:

```
class C {
  static int x = 0, y = 0;
}
```

	Thread t1	Thread t2
1:	`C.y = 1;`	`C.x = 1;` :3
2:	`int r1 = C.x;`	`int r2 = C.y;` :4

Abbildung 2: Beispiel-Programm mit zwei Threads

Theorem 1 (Typsicherheit)**.** *Ausgehend von einem korrekten JinjaThreads-Programm und passenden Startzustand gilt für alle über* $\_ -\_:\_\rightarrow \_$ *erreichbaren Zustände* s*, in denen die Ausführung endet (d.h., es gibt keine Transition* $s -\_:\_\rightarrow \_$*), dass jeder Thread* t *in* s *entweder verklemmt oder vollständig ausgewertet (d.h. ein Wert, dessen Typ kompatibel zum deklarierten Typ von* t *ist, oder eine unbehandelte Ausnahme) ist.*

Verklemmungen verkomplizieren die Typsicherheitsaussage, da selbst eine typkorrekte Ausführung eventuell nicht mehr vollständig auswertet. Deswegen muss obige Aussage Verklemmungen explizit berücksichtigen, aber dafür benötigt man eine Formalisierung von Verklemmungen. Da diese nur durch Synchronisation zwischen Threads entstehen können, erlauben die Aktionsanweisungen eine exakte semantische Charakterisierung mittels eines größten Fixpunkts, die genauer als die üblichen syntaktischen Approximationen ist und damit die Typsicherheitsaussage verstärkt. Außerdem lässt sich abstrakt in Schicht 5 für alle ETS zeigen, dass eine Ausführung nicht zu Ende ist, solange auch nur ein Thread weder verklemmt noch vollständig ausgewertet ist – vorausgesetzt, dass Typsicherheit bereits für die ETS gilt und nur erfüllbare Aktionsanweisungen verwendet werden. Dank dieser Aussage lassen sich also Jinjas Typsicherheitsbeweise für Quell- und Bytecode für den nebenläufigen Fall einfach wiederverwenden und die beiden neuen Typsicherheitsbeweise können den Verklemmungsfall einfach und auf die gleiche Weise abhandeln.

3 Das Java-Speichermodell

Bis jetzt wurde noch nicht auf die Modellierung des allen Threads gemeinsamen Speichers eingegangen, in dem alle Objekte und Arrays liegen. JinjaThreads modelliert diesen Teil des Systemzustands (Variablekonvention h für Halde in den ETSen) in zwei austauschbaren Modulen mit gleicher Schnittstelle (Schicht 1 in Abb. 1). Zum einen führt die in der Literatur übliche (endliche) Abbildung von Adressen auf die gespeicherten Daten zusammen mit der verschränkten Ausführung der Threads zur gewohnten SC, bei der jede Veränderung des Speicher durch einen Thread sofort für alle anderen Threads sichtbar wird. Beispielsweise kann das Paar der lokalen Variablen `r1` und `r2` der beiden Threads in Abb. 2 am Ende der Ausführung nur die Wertkombinationen $(0, 1)$, $(1, 0)$ und $(1, 1)$ enthalten, aber nicht $(0, 0)$.

Das JMM erlaubt hingegen alle vier Kombinationen, da heutige Prozessoren nur ein schwächeres Speichermodell bieten. Wenn beispielsweise die beiden Threads aus Abb. 2 auf verschiedenen Kernen mit getrennten Caches ausgeführt werden, können die geschriebenen Werte aus den Zeilen 1 und 3 noch in dem jeweiligen Cache feststecken, wenn bereits die nachfolgenden Leseoperationen der Zeilen 2 und 4 ausgeführt werden, die folglich beide

```
class A {
  void f() {}
}
A x = null, y = null;
```

Thread t1	Thread t2
1: r1 = x;	4: r2 = y;
2: if (r1 != null) r1.f();	5: x = r2;
3: y = new A();	

Abbildung 3: Ein Programm, bei dem eine Methode vor der Erzeugung des Zielobjekts aufgerufen werden kann.

den initialen Wert 0 aus dem Hauptspeicher lesen. Um SC zu garantieren, müsste der Compiler bzw. die VM zwischen den Schreib- und Lesebefehlen jeweils Synchronisationscode einfügen, der die Programmausführung über Gebühr verlangsamen würde.

Um auch komplexere Optimierungen bei der Übersetzung von Java-Programmen zu erlauben, kann es im JMM sogar passieren, dass Werte aus dem Speicher gelesen werden, die erst später zum ersten Mal erzeugt werden. Beispielsweise darf in Abb. 3 der Übersetzer Zeile 3 in Thread `t1` vor die Zeilen 1 und 2 vorziehen, so dass das neu erstellte Objekt Ziel des Methodenaufrufs in Zeile 2 sein kann (Ablauf 3, 4, 5, 1, 2); in der Semantik wird der Thread aber wie angegeben ausgeführt, also Zeile 2 immer vor 3. Um solche Effekte trotzdem zu erlauben, verwaltet das Schicht-1-Modul für das JMM nur den Allokationsstatus der Adressen und Typinformationen über die zu speicherden Werte, aber nicht die Werte selbst. Dies übernehmen drei weitere Semantik-Schichten: Nr. 4 generiert neue Ereignisse, die den Start und das Ende eines Threads markieren; Nr. 6 generiert die Menge aller möglichen Traces durch das Transitionssystem von Schicht 5, die alle Speicher- und Synchronisationsoperationen (einschließlich der Ereignisse aus Nr. 4) aufzeichnen; Nr. 7 wählt aus diesen Kandidaten die erlaubten Ausführungen aus. Die Auswahlkriterien sind der Kern des JMM, erst sie stellen sicher, dass die gelesenen und geschriebenen Werte der Speicherzellen zusammen passen. Um sogenannte Werte aus dem Nichts zu verhindern, reicht es jedoch nicht aus, einen einzelnen Trace zu betrachten; die Kriterien benötigen die Menge aller Kandidaten-Traces, um deren Teile untereinander in Beziehung zu setzen. Außerdem müssen auch unendliche Traces betrachtet werden, da das JMM unterstellt, dass aller Speicher bereits am Anfang einer Ausführung initialisiert wird – selbst wenn das entsprechende Objekt erst später zur Laufzeit erzeugt wird.

Um die Komplexität des Speichermodells einem durchschnittlichen Java-Programmierer nicht zumuten zu müssen, garantiert das JMM, dass korrekt synchronisierte Programme sich wie unter SC verhalten. Korrekte Synchronisation bedeutet dabei, dass keine SC-Ausführung einen Datenwettlauf enthalten darf, was immer durch ausreichende Synchronisation erreicht werden kann.

Theorem 2 (DRF-Garantie)**.** *Ist ein Programm korrekt synchronisiert, dann sind alle Ausführungen unter dem JMM nicht von den SC-Ausführungen unterscheidbar.*

Der Beweis dieses Theorems ersteckt sich über alle Schichten der Semantik, insbesondere verlangt er, dass ein sequenziell konsistentes Präfix eines Trace in sequenziell konsistenter Weise fortgesetzt werden kann. Da gezeigt wird, dass die Sonderbehandlung von Speicherinitialisierungen bei sequenziell konsistenten Präfixen ohne Bedeutung ist, lässt sich die Fortsetzung korekursiv konstruieren.

Frühere Formalisierungen der Auswahlkriterien und DRF-Garantie [AŠ07, HP07] hatten keine Verbindung mit einer operationalen Java-Semantik und konnten so die Komplikationen der Speicherinitialisierung ignorieren. Ebenso konnten sie die an die Trace-Menge gestellten Annahmen nicht nachweisen. Erst durch die neu geschaffene Verbindung mit der operationalen Semantik lässt sich diese Garantie also für konkrete Programme formal nutzen.

Ein wesentlicher Grund für die Komplexität des JMMs ist, dass es auch die Semantik von Programmen mit Datenwettläufen definiert. Dies ist notwendig, um die Typsicherheit und Sicherheitsarchitektur Javas zu garantieren. Deswegen beziehen sich die weiteren Untersuchungen dieses Abschnitts explizit auch auf Programme mit Wettläufen.

Zuerst wird gezeigt, dass das JMM jede SC-Ausführung erlaubt. Damit ergibt sich folgendes Verhältnis zwischen SC und dem JMM: Für wettlauffreie Programme sind die gleichen Ausführungen beobachtbar, bei Wettläufen erlaubt das JMM mehr Ausführungen als SC. Da immer eine SC-Ausführung existiert, folgt unmittelbar, dass das JMM in sich widerspruchsfrei ist – dies ist wegen der Komplexität und axiomatischen Art der Auswahlkriterien nicht offensichtlich.

Theorem 3 (Widerspruchsfreiheit)**.** *Das JMM erlaubt jede SC-Ausführung. Somit hat jedes Programm mindestens eine erlaubte Ausführung.*

Zum Thema Typsicherheit wird anhand neuer Beispielprogramme gezeigt, dass es zu Laufzeitproblemen kommen kann, wenn in Schicht 1 Typinformationen wie in der Literatur üblich in den angelegten Objekten und Arrays gespeichert werden. Beispielsweise kann in Abb. 3 das Ziel des Methodenaufrufs in Zeile 2 nicht bestimmt werden, wenn das Objekt an der referenzierten Adresse noch nicht angelegt worden ist. Dazu kann es wie oben beschriebenen durch Optimierungen während der Übersetzung kommen, die das JMM zwar erlaubt, die aber in der Semantik nicht vorweg genommen werden.

Außerdem lassen sich mit Datenwettläufen einer Variablen vom Typ T Referenzen auf Objekte eines beliebigen anderen Typs unterschieben, beispielsweise einem `String`-Zeiger eine Referenz auf ein `Integer`-Objekt; die Folge sind Zugriffsfehler, die Typsicherheit ist also verletzt. Obwohl die Auswahlkriterien eigentlich genau dies verhindern sollen, lässt sich mit Speicherallokationen ein subtiles Beispiel konstruieren, für das das JMM solche Ausführungen doch erlaubt. Als Lösung wird vorgeschlagen, den Adressraum statisch nach den zu speichernden Werten zu partitionieren und die Menge der Traces auf typ-korrekte Leseoperationen einzuschränken.[1] Dadurch unterscheidet sich eine Referenz auf ein `String`-Objekt *syntaktisch* von einer auf ein `Integer`-Objekt, so dass sie beim Vergleich verschiedener Traces in den Auswahlkriterien nicht mehr verwechselt werden können. Dann überträgt sich Typsicherheit (Thm. 1) auf das JMM, da beide obigen Szenarien nicht mehr möglich sind. Beispielsweise ist die Methodenaufrufzielauflösung unabhängig davon, ob das Zielobjekt bereits alloziiert wurde, da die Referenz selbst die für die Zielauswahl nötigen Informationen enthält.

[1] Durch die Einschränkung auf typkorrekte Leseoperationen wird das JMM „per Konstruktion“ typsicher. In [Loc12a] zeige ich, dass diese Einschränkung unnötig ist, da die Auswahlkriterien selbst nur Traces mit typkorrekten Leseoperationen erlauben – somit ist das JMM wirklich typsicher. Diese Einschränkung hilft bei der Standard-Modellierung in Schicht 1 nicht, da dann erlaubte Ausführungen, wie das Beispiel aus Abb. 3 zeigt, ausgeschlossen würden.

Eine leichte Abwandlung des zweiten Beispiels führt zu einem Angriff auf die Sicherheitsarchitektur Javas, die auf die Unveränderbarkeit von `String`s vertraut. Mittels Datenwettläufen lassen sich Referenzen fälschen, um so Zugriff auf die internen Datenstrukturen der `String`-Klasse zu erhalten. Die Einschränkungen bei Typsicherheit helfen hier nicht weiter, weil die gefälschte Referenz vom richtigen Typ ist und sich nicht syntaktisch von der richtigen unterscheidet. Allerdings handelt es sich hier nur um einen hypothetischen Angriff, da das JMM nur das erlaubte Verhalten in realen VMs einschränkt – mir ist bisher keine Optimierung bekannt ist, die zu dem Verhalten im Beispiel führen kann. Trotzdem zeigen diese Beispiele eine grundsätzliche Schwachstelle in der Spezifikation des JMMs auf, die bei einer künftigen Überarbeitung angegangen werden sollte.

4 Der Übersetzer

JinjaThreads formalisiert auch einen nicht-optimierenden Compiler *J2JVM*, der Quellcode-Programme in Bytecode übersetzt. Er verbindet – wie schon in Jinja – die beiden Sprachen zu einem einheitlichen Modell. Bei der Kompilation sind `synchronized`-Blöcke am schwierigsten, da die Blockstruktur des Quellcodes im Bytecode nicht mehr vorhanden ist. Dies betrifft die Registerallokation, da ein weiteres Register die Monitoradresse während der Ausführung des Blocks zwischenspeichern muss, und die Ausnahmebehandlung, da die Sperre auch bei einer ausgelösten Ausnahme durch generierten Behandlungscode freigegeben werden muss.

Das folgende Theorem fasst die Korrektheitsaussagen der Übersetzerverifikation zusammen:

Theorem 4 (Korrektheit des Übersetzers)**.** *Sei P ein wohlgeformtes JinjaThreads-Programm. Dann gilt folgendes:*

(i) Der Bytecode-Verifizierer akzeptiert das übersetzte Programm J2JVM P.

(ii) P und J2JVM P haben das gleiche Verhalten, d.h., jeder (erlaubte) Trace von P ist auch ein (erlaubter) Trace von J2JVM P und umgekehrt.

(iii) P ist korrekt synchronisiert genau dann, wenn J2JVM P es ist.

Während der erste Punkt lediglich eine Erweiterung des Beweises aus Jinja benötigt, lässt sich der alte Korrektheitsbeweis zum Verhalten nicht übertragen, da dieser auf der nicht mehr vorhandenen Big-Step-Semantik aufbaute. Stattdessen muss der Beweis nun gegen die SOS geführt werden. Der Bisimulationsbeweis wird dadurch wesentlich aufwändiger, da auch alle Zwischenzustände der Berechnungen zueinander in Beziehung gesetzt werden müssen und manche Konstrukte im Quell-, andere im Bytecode mehr Berechnungsschritte erfordern. Bisimulation stellt unter anderem auch sicher, dass der Übersetzer keine neuen Verhalten einführt. Beispielsweise ist zu zeigen, dass die generierte Entsperrinstruktion am Ende eines `synchronized`-Blocks niemals mit einer `NullPointerException` oder `IllegalMonitorStateException` fehlschlägt, da dies die Blockstruktur im Quellcode ausschließt.

Im Beweis zeigt sich wieder, wie wesentlich die Modularität der Semantik für die Handhabbarkeit ist: Da Quell- und Bytecode die gleiche Semantik für Nebenläufigkeit verwenden, genügt es, die Bisimulation für einen einzelnen Thread zu zeigen. Da die Interaktionen mit anderen Threads in den Aktionsanweisungen gekapselt werden, folgt daraus, dass auch die Kombination der Threads bisimilar ist. Somit braucht man sich im eigentlichen Beweis nicht um die Aktionen anderer Threads und den durch die verschränkte Ausführung erzeugten Nichtdeterminismus kümmern. Da der übliche Begriff der schwachen Bisimulation in diesem Fall für die Komposition nicht ausreicht, wurde eigens der Begriff der Verzögerungsbisimulation mit expliziter Divergenz entwickelt. Divergenz bezeichnet hier die Nichttermination eines Threads, der dabei aber keine beobachtbaren Aktionen ausführt. Der Einbezug von Divergenz stellt sicher, dass der Übersetzer die Terminationseigenschaften des Programms erhält und keine neuen Verklemmungen einführt.

5 JinjaThreads als Java-Interpreter

Angesichts des Umfangs und der Komplexität des Modells lässt nicht mehr einfach sicherstellen, dass es Java adäquat abbildet. Eine formale Verifikation ist hier nicht möglich, weil die Spezifikation von Java nicht formal ist. Stattdessen wurden mit Isabelles Codegenerator automatisch aus der Formalisierung ausführbare Implementierungen in Standard ML extrahiert. Dies liefert einen Interpreter, Übersetzer und eine virtuelle Maschine samt Bytecode-Verifizierer. Der Codegenerator generiert aus bewiesenen Gleichungen der Formalisierung ein funktionales Programm, dessen Ausführungschritte je einer Termersetzung in der Logik entsprechen. Dadurch gelten automatisch alle bewiesenen Theoreme auch für das Ergebnis der Berechnung, da die Schritte direkt in der Logik simuliert werden können. Das bedeutet insbesondere, dass Interpreter und VM typsicher und der Übersetzer verifiziert sind.

Nun kann das Modell validiert werden, indem Java-Programme geprüft, übersetzt, ausgeführt und das Ergebnis mit spezifizierten Erwartungen verglichen wird. Zuvor müssen aber die Programme in JinjaThreads' abstrakter Syntax übertragen werden, auf der alle drei arbeiten. Dazu wurde das Konvertierungstool Java2Jinja (`http://pp.ipd.kit.edu/projects/quis-custodiet/Java2Jinja/`) als Eclipse-Plugin entwickelt, das zusätzlich nicht unterstützte Aspekte wie beispielsweise innere Klassen und Generics, sofern möglich, emuliert. Außerdem bietet es eine Benutzerschnittstelle für die Übersetzung und Ausführung einzelner Java-Programme mit den generierten Komponenten sowie automatisierte Läufe ganzer Testsuites an.

JinjaThreads wurde mit Hinblick auf einfache Beweise und ohne Effizienzgedanken entwickelt. Deswegen sind drei Anpassungen nötig, um akzeptable Ausführungszeiten zu erreichen: (i) Ein eigenes Modul implementiert Schicht 1 mit effizienten, verifizierten Rot-Schwarz-Bäumen als sequenziell konsistenten Objektspeicher. (ii) Zum Programmstart werden Lookup-Tabellen für Deklarationen erzeugt, die dann während der Prüfung und Ausführung des Programms statt wiederholter Neu-Berechnungen verwendet werden. (iii) Ein Abwickler bestimmt den nächsten auszuführenden Thread, so dass nur eine statt aller Verschränkungen berechnet wird. Alle Anpassungen wurden korrekt bewiesen,

wobei neben der Flexibilität des Code-Generators die Modularität der Formalisierung entscheidend waren. Auf diese Weise wird der generierte Code in der Effizienz vergleichbar mit anderen Java Formalisierungen, die von Anfang an auf eine effiziente Ausführung hin entwickelt wurden. Gegenüber diesen bietet JinjaThreads den Vorteil, dass der Compiler verifiziert und Interpreter und VM typsicher bewiesen wurden. Für die Verarbeitung von 100 000 Objekten in einem klassischen Erzeuger-Verbraucher-Beispiel braucht die VM beispielsweise 63 s.

Die so erzielte Effizienz genügte, um 189 Testprogramme mit Java2Jinja und JinjaThreads zu bearbeiten, darunter 24 OpenJDK-Regressionstests. Bei der Validierung wurde lediglich ein Fehler in der Implementierung der Divisions- und Modulo-Operatoren für negative Ganzzahlen gefunden und korrigiert. Somit lässt sich sagen, dass JinjaThreads ein getreues Modell von nebenläufigem Java ist.

6 Zusammenfassung und Ausblick

JinjaThreads gehört mit 84 000 Zeilen Formalisierung, 848 Definitionen und 3 857 Lemmata zu den größten Anwendungen des Theorembeweisers Isabelle/HOL. Zum Vergleich, der sequenzielle Vorgänger Jinja begnügte sich mit 17 kLoC. Dem stehen aber auch der erweiterte Sprachumfang und eine detailgetreue Modellierung der Nebenläufigkeit einschließlich des JMMs entgegen. Auch hier wird wieder sichtbar, wie wichtig eine modulare Struktur ist: Beispielsweise entfallen von 13 kLoC für das JMM 10 kLoC auf die Formalisierung, der Nachweis der sprachspezifischen Annahmen des DRF-Beweises braucht nur 3 kLoC für Quell- und Bytecode zusammen.

JinjaThreads ist heute das umfassendste formale Modell von nebenläufigem Java einschließlich des JMMs. Entstanden ist es im Rahmen des Projekts Quis Custodiet (`http://pp.ipd.kit.edu/projects/quis-custodiet/`). Dort stellt es die semantische Grundlage für die Verifikation von Verfahren zur Informationsflusskontrolle (IFC) in nebenläufigen Java-Programmen. Dazu ist ein solches umfassendes und vereinheitlichtes Modell unabdingbar, da erst die Verbindung der verschiedenen Teile deren Interaktion korrekt erfasst und es erlaubt, die belastbaren Aussagen zur Theorie der Programmiersprache Java formal zu nutzen. Beispielsweise verlassen sich die IFC-Verfahren auf Typsicherheit und die DRF-Garantie; deren Verifikation kann also nur gelingen, da diese schon in dieser Arbeit nachgewiesen wurden. In diesem Kontext sind auch die ausführbaren Teile von Interesse, da sie sicherstellen, dass die durch die IFC-Verfahren nachgewiesenen Eigenschaften auch zur Laufzeit wirklich gelten.

Die aufgezeigten Probleme bei der Typsicherheit und Sicherheitsarchitektur werfen die Frage auf, wie diese Schwachstelle des JMMs behoben werden kann. In beiden Fällen sind Werte, die aus dem Nichts auftauchen, Ursache des Problems; der vorgestelle Ansatz rettet zwar die Typsicherheit, löst das Problem aber nicht abschließend. Zusammen mit den bereits bekannten Schwächen des JMMs deutet dies darauf hin, dass eine weitere Revision nötig ist. Es ist aber offen, wie eine überzeugende Antwort aussehen wird. Das Konzept des „Werts aus dem Nichts“ jedenfalls scheint als Kriterium zu unklar und allgemein zu sein –

wären die Annahmen der Sicherheitsarchitektur präzise formuliert, könnte man diese für das nächste JMM nachweisen.

Literatur

[AŠ07] David Aspinall und Jaroslav Ševčík. Formalising Java's Data-Race-Free Guarantee. In Klaus Schneider und Jens Brandt, Hrsgg., *Theorem Proving in Higher Order Logics (TPHOLs 2007)*, Bd. 4732 von *LNCS*, Seiten 22–37. Springer, 2007.

[GJSB05] James Gosling, Bill Joy, Guy Steele und Gilad Bracha. *The Java Language Specification, Third Edition*. Addison-Wesley, 2005.

[HP07] Marieke Huisman und Gustavo Petri. The Java Memory Model: a Formal Explanation. In *Verification and Analysis of Multi-threaded Java-like Programs (VAMP 2007)*, Bericht ICIS-R07021, Seiten 81–96. University of Nijmegen, 2007.

[KN06] Gerwin Klein und Tobias Nipkow. A Machine-Checked Model for a Java-Like Language, Virtual Machine and Compiler. *ACM Transactions on Programming Languages and Systems*, 28(4):619–695, 2006.

[Loc07] Andreas Lochbihler. Jinja with Threads. *Archive of Formal Proofs*, 2007. `http://afp.sf.net/devel-entries/JinjaThreads.shtml`, Formal proof development.

[Loc12a] Andreas Lochbihler. The Java Memory Model is Type Safe. Bericht 2012-23, Karlsruhe Reports in Informatics, 2012.

[Loc12b] Andreas Lochbihler. *A Machine-Checked, Type-Safe Model of Java Concurrency : Language, Virtual Machine, Memory Model and Verified Compiler*. Dissertation, Fakultät für Informatik, Karlsruher Institut für Technologie, 2012.

[NPW02] Tobias Nipkow, Lawrence C. Paulson und Markus Wenzel. *Isabelle/HOL — A Proof Assistant for Higher-Order Logic*, Bd. 2283 von *LNCS*. Springer, 2002.

[Pug00] William Pugh. The Java memory model is fatally flawed. *Concurrency: Practice and Experience*, 12:445–455, 2000.



Andreas Lochbihler, geboren 1981, studierte von 2001 bis 2006 Informatik mit Schwerpunkt mathematische Modellierung an der Universität Passau und während eines Auslandsjahrs an der University of Edinburgh. Nach dem Diplom-Abschluss mit Auszeichnung arbeitete er als wissenschaftlicher Mitarbeiter: bis März 2008 am Lehrstuhl für Softwaresysteme an der Universität Passau und danach bis 2012 am Lehrstuhl für Programmierparadigmen am Karlsruher Institut für Technologie. 2012 wurde er mit seiner in dieser Zeit verfassten Dissertation über die Semantik der Nebenläufigkeit in der Programmiersprache Java *summa cum laude* promoviert. Seit 2013 forscht er als Postdoktorierender am Institut für Informationssicherheit der ETH Zürich über die Sicherheit von Protokollen und entwickelt Ansätze zur Generierung fehlerfreier Protokoll-Implementierungen.

Fehlertolerante Industrielle Wireless-Mesh-Network-Infrastruktur *

Georg Lukas

Institut für Verteilte Systeme (IVS)
Otto-von-Guericke-Universität Magdeburg
glukas@ovgu.de

Abstract: Drahtlose Kommunikation spielt eine immer größere Rolle in industriellen Anwendungen. Gleichzeitig erfordern es diese Anwendungen, dass das Netzwerk Ende-zu-Ende-Dienstgüte garantieren und umsetzen kann. Drahtlose vermaschte Netzwerke (Wireless Mesh Networks, WMNs) sind hervorragend für die Flexibilitätsanforderungen gerüstet, bieten aber keine inhärente Dienstgüte. In der Doktorarbeit werden Methoden der Fehlertoleranz angewendet, um eine für industrielle Anwendungen geeignete WMN-Infrastruktur mit Dienstgütegarantien bereitzustellen. Die Infrastruktur wird aus den industriellen Anforderungen entwickelt und umgesetzt. Ihre Praxistauglichkeit belegt sie durch eine Evaluierung in einem Tele-Robotik-Szenario in einer realen Testumgebung.

1 Kontext und Motivation

Die Vernetzung industrieller Anlagen gewinnt immer mehr an Bedeutung. Besonders im Zuge der steigenden Anforderungen an Flexibilität und Effizienz soll vermehrt drahtlose Kommunikation zum Einsatz kommen. Die industriellen Anwendungen stellen allerdings hohe Anforderungen an das Kommunikationssystem. Für Aufgaben wie die Steuerung einer Anlage oder die manchmal nötige Fernsteuerung eines fahrerlosen Transportsystems (FTS) müssen für die Ende-zu-Ende-Übertragung Garantien bezüglich Latenz, Paketverlustrate und verfügbarer Bandbreite (*Dienstgüte* bzw. *QoS*) gegeben werden.

Um den genauen Dienstgütebedarf zu ermitteln, wurde eine Analyse der potentiellen Anwendungsklassen mit hohen Ansprüchen – Steuerung/Regelung und videobasierte Tele-Operation mobiler Roboter – durchgeführt. Für eine erfolgreiche Umsetzung der Regelung stationärer Maschinen sind Latenzzeiten von 10 ms (Round-Trip-Time) zu garantieren. Für die Tele-Operation sind Latenzen bis zu 200 ms akzeptabel, allerdings stellt diese Anwendung zusätzlich hohe Durchsatzanforderungen (einige $\mathrm{MBit/s}$) an das Medium und benötigt eine unterbrechungsfreie Verbindung selbst dann, wenn sich die Kommunikationsteilnehmer durch die Anlage bewegen (spezifiziert als Obergrenze für aufeinander folgende Paketverluste, *Omission Degree*).

*Englischer Titel der Dissertation: “Fault-tolerant Industrial Wireless Mesh Network Infrastructure”[Luk12]

Die bisher existierenden Kommunikationssysteme bieten entweder nicht die notwendige Durchsatzkapazität (Wireless Sensor Networks, WSN, z.B. WirelessHART[Wir10]) oder nicht die Möglichkeit, sich ohne Kommunikationsunterbrechung im gesamten Anlagenbereich zu bewegen (Infrastruktur-WLAN, z.B. ^{flex}WARE[SJB09]). Eine Kombination dieser Funkverfahren ist zwar prinzipiell denkbar, erschwert aber einerseits die Administration (zwei getrennte Netzwerke müssen gewartet und Übergangspunkte zwischen ihnen aufgebaut werden), andererseits kollidieren teilweise die genutzten Frequenzbänder (2.4 GHz ISM), was zu einer gegenseitigen Beeinträchtigung der Netzwerke führen kann.

Eine gemeinsame drahtlose Kommunikationsinfrastruktur, die Echtzeitanwendungen mit hohen Durchsätzen ermöglicht, würde nicht nur den administrativen Aufwand senken, sondern auch neue Anwendungen im Industriealltag ermöglichen, wie z.B. auf Sensorfusion basierte Kooperation mobiler Roboter und Augmented Reality.

2 Herausforderungen

Industrielle Anwendungen benötigen Garantien über den Durchsatz, die Latenz und die zulässigen Paketverluste für den gesamten Pfad vom Sender zum Empfänger (Ende-zu-Ende-Dienstgüte). Gleichzeitig können sich Netzwerkteilnehmer bewegen und es ist möglich, dass Komponenten ausfallen und dadurch die Erfüllung der Garantien gefährden.

Die Bereitstellung solcher Garantien für drahtlose Kommunikation ist besonders herausfordernd, da sowohl das Medium als auch die (mobilen) Teilnehmer ständiger Veränderung unterworfen sind. Solche Veränderungen können dadurch verursacht werden, dass sperrige Objekte im Lagerbereich einer Halle abgestellt werden, oder dass bei einer Rekonfiguration des Produktionsprozesses andere Anlagen zum Einsatz kommen, die die Ausbreitung der Funksignale beeinflussen. Gleichzeitig sorgt die Mobilität von Kommunikationsteilnehmern dafür, dass ihre Signalstärke sich verändert (was häufig zu einem Wechsel der Modulation und der Datenrate führt), oder eine bestehende Funkverbindung gänzlich abreißen kann.

Diese Veränderungen sorgen dafür, dass die für die Erfüllung der Anforderungen zur Verfügung stehenden Ressourcen ständig schwanken. Werden dann mehr Daten in das Netz gesendet als es übertragen kann, kommt es zu einer Überlast-Situation, Paketverluste und Latenzen steigen an und es können keine Garantien mehr gegeben werden. Darüber hinaus muss die Infrastruktur auch mit auftretenden Fehlern umgehen können, und selbst beim Ausfall einzelner Knoten noch einen zuverlässigen Dienst bereitstellen.

Gleichzeitig soll für die Entwickler industrieller Applikationen die Komplexität der Kommunikationsinfrastruktur derart abstrahiert werden, dass eine Entwicklung auch ohne ein Verständnis der komplexen Vorgänge bei der Signalausbreitung und Medienzuteilung möglich ist.

3 Konzept

Im Rahmen der Doktorarbeit wurden Methoden der Fehlertoleranz angewendet, um eine industrielle Kommunikationsinfrastruktur auf Basis drahtloser vermaschter Netzwerke bereitzustellen. Hierzu wurde zunächst ein Fehlermodell entwickelt, welches alle auftretenden Einflüsse auf die Ende-zu-Ende-Dienstgüte als Fehler klassifiziert. Um Fehler zu erkennen und in angemessener Zeit darauf reagieren zu können, wurden *schichtübergreifende Monitoring-Mechanismen* entwickelt, deren Messdaten aggregiert und zentral in *QoS-Modellen* abgespeichert werden. Diese Modelle werden herangezogen, um auf Basis der Anwendungsanforderungen zu entscheiden, welche Datenströme zugelassen werden (*Admission*) und so eine Überlastung des Netzes zu vermeiden. Die entwickelten Komponenten arbeiten in einem Regelkreis (Abbildung 1), der sich stätig an den Ist-Zustand des Netzwerks anpasst. Gleichzeitig sorgen proaktive Elemente wie lokales Rerouting dafür, dass Fehlerzustände soweit möglich vermieden werden.

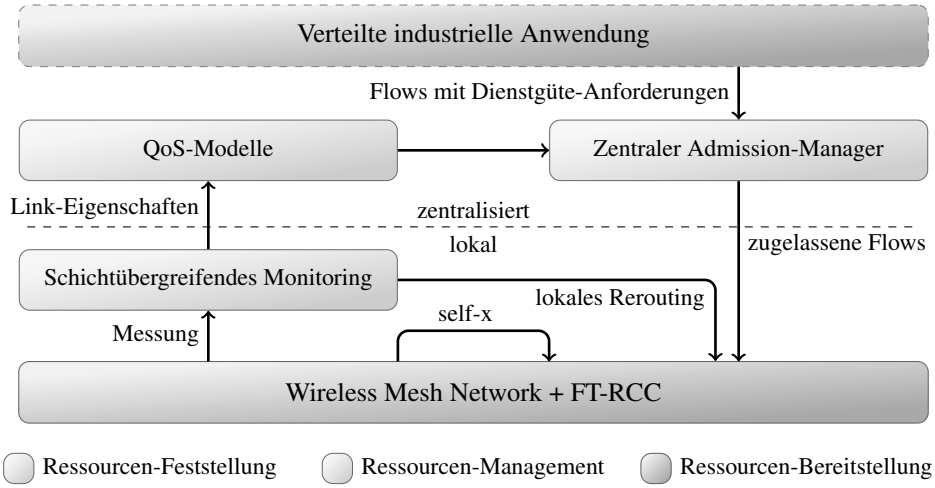


Abbildung 1: Fehlertolerante Industrielle WMN-Infrastruktur

3.1 Zugrundegelegte Technologien

Als Grundlage der Kommunikationsinfrastruktur wurden drahtlose vermaschte Netzwerke (Wireless Mesh Networks, WMN [AWW05]) auf Basis des WLAN-Standards ausgewählt. Sie bestehen aus stationären *Mesh-Routern*, die den Kern der Infrastruktur bilden, und potentiell mobilen *Mesh-Clients*, auf denen die Anwendungen laufen. WMNs sind durch ihre *self-x*-Eigenschaften (Selbst-Organisation und -Heilung) sehr gut geeignet, eine flexible und der hohen Dynamik gerecht werdende Infrastruktur aufzubauen. Hinzu kommt die hohe Durchsatzkapazität und weite Verfügbarkeit der zugrundeliegenden WLAN-Hardware.

Um hinreichende Abdeckung einer Anlage durch Funksignale und redundant verfügbare Verbindungen zwischen Mesh-Routern zu gewährleisten, wird eine nach „*Fault-tolerant Radio Coverage and Connectivity in WMNs*" (FT-RCC, [IN12]) vorausgeplante Mesh-Router-Infrastruktur vorausgesetzt. Auf diese Weise kann der Fokus der Arbeit auf die nicht minder schweren Herausforderungen der Bereitstellung von Ende-zu-Ende-Dienstgüte gelegt werden.

3.2 Fehlertoleranz-Ansatz

Die durch FT-RCC bereitgestellte physikalische Infrastruktur deckt bereits Ausfälle von Mesh-Knoten und inadäquate Abdeckung durch Funksignale ab. Ausgehend davon wurden die möglichen Auslöser für Verletzungen der Dienstgütegarantien in einem eigenen Fehlermodell zusammengefasst. Diese Auslöser leiten sich aus der Umgebungs- und Teilnehmerdynamik im Netzwerk ab. Hier wurden vier mögliche Ursachen herausgearbeitet:

1. *Verringerung der Link-Übertragungskapazität* – die Kapazität einer Verbindung besagt, wie schnell Daten zwischen zwei Mesh-Knoten übertragen werden können. Sie hängt von der WLAN-Senderate und den nötigen Wiederholungsversuchen ab und variiert je nach Entfernung, Anwesenheit von Hindernissen und Ausbreitungseffekten.
2. *Verschlechterung der Link-Dienstgüteeigenschaften* – die nichtfunktionalen Eigenschaften eines Links (Latenz, Paketverlustrate, omission degree) sind für die darüber laufenden Übertragungen relevant und hängen von den selben Einflussfaktoren ab wie die Link-Kapazität.
3. *Ungültige Links* – wenn ein mobiler Teilnehmer sich von einem Knoten entfernt oder ein Knoten ausfällt, werden logische Verbindungen im WMN abgerissen. Es dauert jedoch einige Zeit (in gängigen WMNs mehr als 10 s), bis der Ausfall erkannt und der Link nicht mehr verwendet wird. In der Zwischenzeit ist die Kommunikation unterbrochen.
4. *Überlastung des Mediums* – wenn mehr gleichzeitige Übertragungen auf dem Medium stattfinden, als die summierte Kapazität aller Links zulässt, müssen Datenpakete verworfen werden oder länger auf ihre Übertragung warten. Daher muss eine Überlastung um jeden Preis verhindert werden. Dafür wird selbst die kontrollierte Deaktivierung von (niedriger priorisierten) Flows in Kauf genommen.

Ausgehend von diesem Fehlermodell wurden die Komponenten des Regelkreises aufgebaut. Es wurden Monitoring-Module für Link-Kapazität, Link-Dienstgüteeigenschaften und Link-Ausfälle entwickelt, und ein zentraler Admission-Manager eingesetzt, der anhand der gemessenen Daten die Anwendungsgarantien kontrolliert und eine Überlastung verhindert. Der zweite wichtige Fehlertoleranz-Baustein ist eine Kapazitätsreserve, die der Admission-Manager für lokale Reparaturmaßnahmen zurückhält, statt sie an Anwendungen zu vergeben. Diese Reserve kompensiert zum einen die Zeit zwischen dem Auftreten und der Erkennung eines Fehlers, zum anderen ermöglicht sie, dass ein Knoten lokal Maßnahmen trifft, ohne diese vorher mit dem zentralen Manager koordinieren zu müssen.

3.3 Verteiltes Monitoring

Alle Mesh-Knoten (einschließlich der mobilen Teilnehmer) überwachen stetig ihre Links und melden deren Zustand an einen zentralen Knoten, der alle Informationen zu Dienstgüte-Modellen zusammenfasst. Um möglichst korrekte und aktuelle Daten zu erhalten, wurden dabei schichtübergreifende Ansätze entwickelt, die Informationen aus der MAC-Schicht, wie die WLAN-Senderate, die Häufigkeit von Wiederholungen und ausbleibende Bestätigungspakete (ACKs), ermitteln und für die Modellbildung nutzen.

Um Informationen über die Latenzen und die Link-Auslastung zu erhalten, wird eine Cross-Layer-Version der ETT-Metrik (*Estimated Transmission Time*) eingesetzt. Die gewonnenen Daten werden als Linkkosten durch das WMN-Routingprotokoll weitergegeben und für die Berechnung der Gesamtlast genutzt [LLN11]. Für die Paketverlustmessung kommt ein verteiltes Verfahren zum Einsatz, bei dem jeder Knoten die ankommenden Pakete von allen seinen Nachbarn zählt und periodisch mit den jeweiligen Sendern abgleicht.

Besondere Aufmerksamkeit verdient jedoch die beschleunigte Erkennung von Link-Ausfällen [LLN10]. Entsprechend dem Empfang von ACK-Paketen wird der Zustand jedes Links permanent durch ein Link-Fehler-Modell als *funktionsfähig* oder *ausgefallen* eingestuft. Wird ein Linkausfall erkannt, werden alle weiteren Datenpakete über eine alternative Verbindung gesendet und der Ausfall dem zentralen Manager bekannt gegeben. Diese Vorgehensweise erlaubt es, die Anzahl verlorener Pakete um mehrere Größenordnungen auf maximal 4 Verluste pro ausgefallenem Link zu reduzieren.

3.4 QoS-Modelle

Die Aufgabe der QoS-Modelle ist es, die Monitoring-Informationen zu aggregieren und über eine gemeinsame Schnittstelle bereitzustellen. Für jedes im Einsatzszenario relevante QoS-Attribut gibt es dabei ein separates Modell. Dieser Ansatz erlaubt es, das Gesamtsystem im Funktionsumfang an die Anwendungsanforderungen anzupassen oder später durch weitere QoS-Attribute zu ergänzen.

Eine Sonderstellung nimmt das Modell für die Medienauslastung an: da die Kapazität des Mediums begrenzt ist, wird mit seiner Hilfe entschieden, ob das Medium durch eine neue Verbindung (und die durch diese erzeugte Last T) eventuell überlastet werden könnte. Damit ist dieses Modell im Gegensatz zu jenen für Latenz und Paketverluste immer erforderlich.

Die anderen Modelle müssen Informationen darüber bereitstellen, ob eine bestimmte Ende-zu-Ende-Anforderung an das jeweilige Attribut erfüllt werden kann oder nicht. Dazu müssen aus den vorgehaltenen Link-Eigenschaften die jeweiligen Ende-zu-Ende-Eigenschaften abgeleitet werden. Um diese Berechnung zu ermöglichen, enthält jedes Modell auch die nötigen Rechenvorschriften (Tabelle 1).

Tabelle 1: Ende-zu-Ende Rechenvorschriften für unterschiedliche Dienstgüteattribute

Link-Eigenschaft	*Ende-zu-Ende*	*Rechenvorschrift*
Link-Kosten c	Auslastung U	$U = T \sum c_i$
Latenz l	Latenz L	$L = \sum l_i$
Paketverlust p	Zustellwahrscheinlichkeit D	$D = \prod(1 - p_i)$

3.5 Zentraler Admission-Manager

Der zentrale Admission-Manager erfüllt die wichtigste Aufgabe bei der Bereitstellung der Dienstgüte. Unter Verwendung der QoS-Modelle muss er für jeden Anwendungsdatenstrom (*Flow*) entscheiden, ob dieser unter den momentanen Netzwerkbedingungen zugelassen werden kann. Dabei darf der Flow das Netzwerk nicht überlasten und die von ihm geforderten Ende-zu-Ende-Eigenschaften müssen gewährleistet sein. Hier kommt auch die Fehlertoleranz zum Tragen: diese Bedingungen müssen auch dann erfüllt werden, wenn sich die Netzwerksituation durch Mobilität oder Knotenausfall verändert.

Obwohl es möglich ist, eine korrekte verteilte Zugangskontrolle zu realisieren, ist der Kommunikationsaufwand dafür immens groß. Für die Vernetzung einer Industrieanlage ist eine zentrale Lösung (mit entsprechend redundanter Absicherung) besser geeignet, da der Gesamtaufwand geringer ist, und der zentrale Knoten durch seine Lage in der Topologie gut von allen Teilnehmern erreicht werden kann.

Bei der Berechnung der Medienauslastung werden alle von den existierenden Flows verwendeten Links und die dort jeweils erzeugte Auslastung aufsummiert. Dazu kommt noch der für den Betrieb des Netzwerks nötige Datenverkehr (Hello-Nachrichten, Monitoring, Flow-Reservierungen). Soll ein neuer Datenstrom zugelassen werden, wird die durch ihn voraussichtlich erzeugte Auslastung dazuaddiert. Übersteigt die Summe den für die Reserve vorgesehenen Schwellwert, muss der Datenstrom abgelehnt werden.

Kann das Netzwerk einen angeforderten Flow aufnehmen, werden zusätzlich seine QoS-Anforderung mittels der Modelle geprüft. Auch hierbei wird eine Reserve für den Fall einer Verschlechterung vorgehalten. Nur wenn alle Überprüfungen positiv verlaufen, wird der Flow genehmigt und die Anwendung darf Daten versenden.

Verschlechtert sich der Zustand des Netzwerks, wird das als *error state* betrachtet. Dabei treffen die beteiligten Knoten zunächst einmal lokal Maßnahmen, um den Fehler zu kompensieren – so wird z.B. ein alternativer Pfad im Netzwerk genutzt. Gleichzeitig wird die Änderung auch in die QoS-Modelle übertragen, so dass der Admission-Manager zentral Maßnahmen treffen kann. Dazu wird zunächst geprüft, ob die QoS-Anforderungen nach wie vor erfüllt werden und ob noch keine Überlast herrscht. Sind die Bedingungen noch ausreichend, wird der error state aufgehoben, ansonsten wird eine Fail-Safe-Maßnahme eingeleitet und der betroffene Datenstrom kontrolliert beendet. Durch die Festlegung des Reserveumfangs kann dabei abgewogen werden, wie viel Dynamik das Netzwerk kompensieren können soll, ohne einen Fail-Safe-Zustand einzuleiten.

3.6 Anwendungsintegration

Gegenüber den Anwendungen wird vom zentralen Admission-Manager eine Schnittstelle definiert, über die Flows reserviert werden können. Ein Flow ist dabei eine Ende-zu-Ende-Verbindung, für die eine Anwendung Dienstgüteanforderungen definiert, die vom Netzwerk erfüllt werden müssen. Jeder Flow wird definiert über Sender, Empfänger, die generierte Netzwerklast und seine Dienstgüteanforderungen. Dabei muss die Infrastruktur durch Monitoring erzeugte QoS-Modelle für alle Dienstgüteattribute bereithalten, die durch Anwendungen angefordert werden können. In der vorliegenden Umsetzung wurden die beiden wichtigsten Attribute Paketverluste und Latenz behandelt, weitere sind jedoch durch die flexibel ausgestaltete Attributsprache[SL09] möglich.

4 Umsetzung und Evaluierung

Die entwickelten Konzepte wurden als Module für das am Lehrstuhl entwickelte Routing-Protokoll AWDS (Ad-hoc Wireless Distribution System) entwickelt. Die Umsetzung erfolgte in C++ und kann auf Linux-Systemen sowie im Netzwerk-Simulator ns-2 eingesetzt werden. Eine für Embedded-Linux abgestimmte Version wird zur Zeit für die Integration in die WLAN-Router eines Herstellers für Industriekommunikation vorbereitet.

Um die praktische Einsetzbarkeit der entwickelten Infrastruktur zu belegen, wurden zunächst alle Komponenten individuell evaluiert. Die Evaluierung erfolgte soweit möglich in einer realen Testumgebung, um Verfälschungen durch ungenaue Simulationsmodelle auszuschließen.

Im Anschluss wurde das Gesamtsystem in einem Praxistest auf seine Vollständigkeit und Anwendbarkeit für industrielle Anwendungen getestet. Dabei wurde auch die Notwendigkeit der einzelnen Komponenten geprüft. Hierzu wurde die Fernsteuerung eines mobilen Roboters aus einer Leitzentrale als Anwendung herangezogen. Gleichzeitig sorgten bis zu vier Hintergrunddatenströme für eine Auslastung des Mediums.

Die Fernsteuerung wurde als Anwendung ausgewählt, weil sie neben einer Obergrenze für Latenzen auch Mobilität und hohe Kapazitätsanforderungen für die Videoübertragung mitbringt. Ferner kann man daran direkt sehen, wenn die Latenzanforderungen verletzt werden und der Roboter nicht mehr unmittelbar auf Steuerbefehle reagiert. Die genauen Anforderungen sind in Tabelle 2 zusammengefasst.

Tabelle 2: Flow-Parameter bei der Evaluierung

Flow	*Prio.*	*Last**	*Attribute*
Fernsteuerung (`control`)	8	16	RTT $\leq 200\,\mathrm{ms}$, OD ≤ 5
Roboter-Video (`video`)	8	6400	$L \leq 100\,\mathrm{ms}$, $p_{loss} \leq 5\,\%$
4x Hintergrunddaten (`bg`)	1	3000	–

* Lastangabe in $\mathrm{Kbit/s}$

RTT = Round-Trip Time, OD = Omission Degree, L = Latenz

4.1 Eignung für industrielle Anwendungen

Um die Funktionsfähigkeit der Infrastruktur zu zeigen, wurde ein Netzwerk aus neun stationären Mesh-Routern in einem Teil des Fakultätgebäudes aufgebaut. In diesem Netzwerk konnte sich der mobile Roboter frei bewegen. Entsprechend der Mobilität wurde eine Kapazitätsreserve von 30% vorgesehen. Für den Versuch startete der Roboter in der Nähe der Leitzentrale, entfernte sich zunächst über einen Flur, um dann zurück zu kommen und sich über einen anderen Flur wieder zu entfernen. Die Erwartung dabei war, dass bei steigender Entfernung sich die durch die Videoübertragung erzeugte Netz-Auslastung erhöht. Um die Anforderungen des Videostroms weiter zu erfüllen, würden nach und nach Hintergrund-Datenströme beendet werden. Wenn der Roboter sich der Leitzentrale nähert, sollten durch freiwerdende Kapazität wieder zusätzliche Datenströme zugelassen werden. Gleichzeitig sollte eine Erfassung des Steuerkanals belegen, dass die Anforderungen an Latenz und Omission Degree selbst bei den auftretenden Linkausfällen nicht verletzt werden.

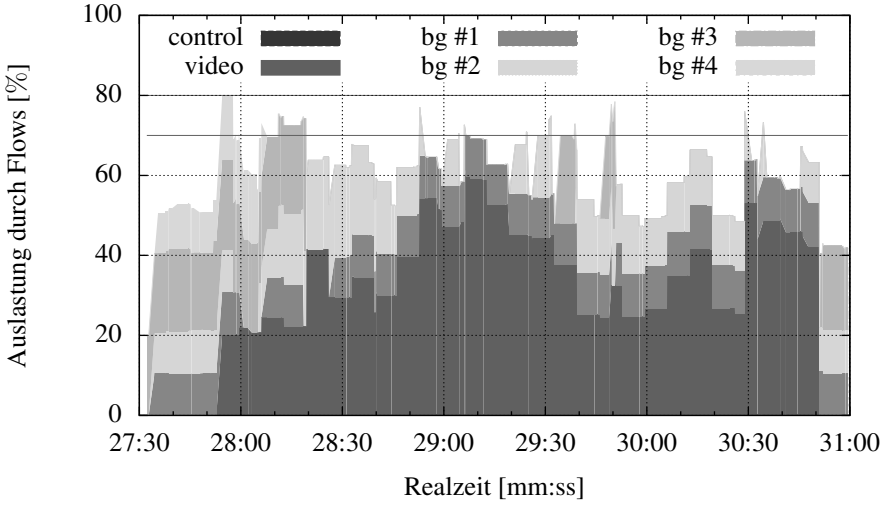


Abbildung 2: Vollständige Infrastruktur: Flows & Auslastung

In Abbildung 2 ist die durch den Admission-Manager festgestellte Auslastung des Netzwerks als Summe der einzelnen Datenströme abgebildet. Bei 28:50 und 30:28 ist der Anstieg der Auslastung durch die Videoübertragung deutlich zu sehen, stellenweise werden alle bis auf einen Hintergrundtransfers angehalten, was den Erwartungen entspricht. Abbildung 3 zeigt ein Histogramm der Ende-zu-Ende-Latenzen des Steuerkanals. Es ist deutlich zu erkennen, dass die meisten Nachrichten in weniger als 1 ms übertragen wurden, die höchste Latenz liegt unterhalb von 200 ms. Diese Messungen bestätigen, dass die Komponenten der Infrastruktur funktionieren und dass sie im Zusammenspiel die Anforderungen der Tele-Robotik-Anwendung erfüllen können. Weitere Experimente haben ferner belegt, dass alle entwickelten Komponenten dazu beitragen, und dass durch Weglassen eines der Module die Dienstgüteanforderungen nicht mehr erfüllt werden können.

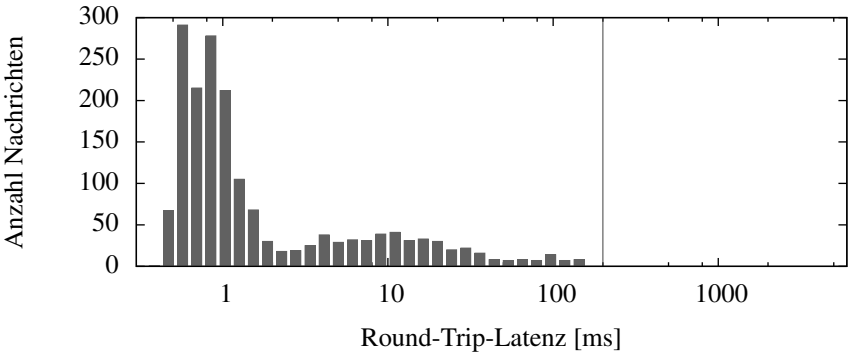


Abbildung 3: Vollständige Infrastruktur: Latenz Fernsteuerung

5 Zusammenfassung

Die Bereitstellung zuverlässiger Funkkommunikation für industrielle Anlagen ist eine große Herausforderung. In der zugrundeliegenden Doktorarbeit wurde eine Kommunikationsinfrastruktur entwickelt, welche die Vorteile der WMN-Technologie (Selbstorganisation und -reparatur, hohe Kapazität) mit einem Fehlertoleranz-Ansatz zur Steigerung der Zuverlässigkeit kombiniert.

Die Umsetzung als Regelkreis erlaubt es, zeitnah auf durch Dynamik und Mobilität verursachte Veränderungen zu reagieren. Durch die Bereitstellung von Ressourcenreserven kann der Dienst selbst in der Zeit zwischen Auftreten und Erkennen eines Fehlers aufrecht erhalten werden. Der zentralisierte Ansatz eignet sich für Anlagen bis zu einigen Hundert Meter Größe, und erlaubt die Einbindung mobiler Stationen. Dabei können Ende-zu-Ende-Dienstgütegarantien für Anwendungsdatenströme durchgesetzt werden.

Die Evaluierung hat gezeigt, dass die Infrastruktur in der Lage ist, die unterbrechungsfreie Fernsteuerung eines mobilen Roboters über ein größeres Areal zu gewährleisten. Damit ermöglicht das resultierende System den drahtlosen Betrieb industrieller Echtzeit-Anwendungen.

Die zur Erhöhung der Zuverlässigkeit entwickelten Mechanismen erlauben nicht nur speziell auf die QoS-Schnittstellen angepasste Anwendungen, sondern verbessern den Dienst allgemein. Insbesondere durch die beschleunigte Link-Ausfallerkennung und die Nutzung der Link-Kapazität als Routing-Metrik profitieren auch reguläre Anwendungen von einem schnelleren und zuverlässigeren Netz. Dies hat ein Netzwerktechnik-Hersteller zum Anlass genommen, die in der Doktorarbeit entwickelten Verfahren in seine Industrie-WLAN-Produktreihe zu integrieren.

Durch die im Vergleich zu bestehenden industriellen Funklösungen deutlich höhere Kapazität und Zuverlässigkeit werden auch neue Anwendungen möglich, die mit bisheriger Technologie nur schwer umsetzbar wären. So kann man z.B. die Techniker in einer Fabrik mit Augmented-Reality-Schnittstellen ausstatten, die aktuelle Sensorwerte aus den

Anlagen projizieren. Außerdem können die Mess- und Videodaten von verschiedenen Robotern aggregiert und mittels Sensorfusion für eine bessere Kooperation miteinander und Integration in die Umgebung genutzt werden.

Literatur

[AWW05] I.F. Akyildiz, X. Wang und W. Wang. Wireless Mesh Networks: a survey. *Computer Networks*, 47(4):445–487, 2005.

[IN12] Svilen Ivanov und Edgar Nett. *Wireless Mesh Networks*, Kapitel Achieving Fault-tolerant Network Topology in Wireless Mesh Networks. Intech, 2012.

[LLN10] Timo Lindhorst, Georg Lukas und Edgar Nett. Modeling Fast Link Failure Detection for Dependable Wireless Mesh Networks. In *IEEE International Symposium on Network Computing and Applications*, Seiten 44–51. IEEE, July 2010.

[LLN11] Georg Lukas, Timo Lindhorst und Edgar Nett. Modeling Medium Utilization for Admission Control in Industrial Wireless Mesh Networks. In *IEEE International Symposium on Reliable Distributed Systems*, Seiten 65–74. IEEE, 2011.

[Luk12] Georg Lukas. *Fault-tolerant Industrial Wireless Mesh Network Infrastructure*. Dissertation, Otto-von-Guericke-Universität Magdeburg, September 2012.

[SJB09] Thilo Sauter, Jürgen Jasperneite und Lucia Lo Bello. Towards New Hybrid Networks for Industrial Automation. In *ETFA'09: Proceedings of the 14th IEEE international conference on Emerging technologies & factory automation*, Seiten 1141–1148, Piscataway, NJ, USA, 2009. IEEE Press.

[SL09] Michael Schulze und Georg Lukas. MLCCA – Multi-Level Composability Check Architecture for Dependable Communication over Heterogeneous Networks. In *14th International Conference on Emerging Technologies and Factory Automation (ETFA 2009)*, Mallorca, Spain, September 2009.

[Wir10] IEC 62591 Ed. 1.0 – Industrial communication networks - Wireless communication network and communication profiles - WirelessHART, 2010.



Georg Lukas wurde am 24. September 1980 in Jekaterinburg geboren. Nach seinem Informatikstudium blieb er an der Otto-von-Guericke-Universität Magdeburg, um im Bereich der zuverlässigen Funkkommunikation zu promovieren.

Neben der universitären Forschung im Bereich WLAN-Kommunikation hat Herr Lukas freiberuflich als IT-Consultant gearbeitet, wo er Website-Security-Audits und Software-Anpassungen durchgeführt hat. Zur Zeit ist er als Berater bei der Firma rt-solutions.de GmbH tätig und entwickelt nebenberuflich Smartphone-Anwendungen für Amateurfunk- und Netzwerkkommunikation.

Exakte Algorithmen für Erfüllbarkeitsprobleme

Robin A. Moser

Institut für Theoretische Informatik, ETH Zürich
robin.moser@inf.ethz.ch

Abstract: Die Erfüllbarkeitsprobleme SAT und CSP dürfen mit Fug als die "natürlichsten" aller NP-vollständigen Probleme bezeichnet werden. Die vorliegende Arbeit befasst sich mit deren algorithmischen Behandlung. Sie besteht aus zwei Teilen.

Der erste Teil befasst sich mit Erfüllbarkeitsproblemen, deren Lösbarkeit aus dem bekannten Lovász Local Lemma folgt. Während seit dessen Entdeckung im Jahre 1975 durch Paul Erdős und László Lovász feststeht, dass Erfüllbarkeitsprobleme mit einer nirgends zu dichten Konzentration an Klauseln immer eine erfüllende Belegung zulassen, war ein algorithmisches Verfahren zur tatsächlichen Bestimmung dieser Lösung lange nicht bekannt. Wir verfeinern frühere Ansätze, das Local Lemma algorithmisch zu machen und präsentieren schliesslich einen Polynomialzeitalgorithmus, der für beinahe alle bisher bekannten Anwendungen des Local Lemma einen konstruktiven Beweis liefert.

Im zweiten Teil verlassen wir die Klasse der in polynomieller Zeit lösbaren Probleme und betrachten stattdessen den von Uwe Schöning im Jahre 1999 vorgeschlagenen und analysierten randomisierten Exponentialzeitalgorithmus für allgemeine Klauselerfüllungsprobleme. Als Hauptbeitrag neben weiteren Aspekten verfeinern wir frühere Ansätze, diesen Algorithmus zu derandomisieren und präsentieren schliesslich die erste deterministische Variante, welche gegenüber dem Zufallsalgorithmus nicht an Effizienz einbüsst.

1 Klauselerfüllungsprobleme

Bei einem *Klauselerfüllungsproblem* sind wir mit einer Menge $\{x_1, x_2, \ldots, x_n\}$ von n Variablen konfrontiert, von denen eine jede einen von d Werten, nennen wie sie $\{1, 2, \ldots, d\}$ annehmen kann. Der Lösungsraum besteht also aus d^n vielen möglichen Kombinationen von Werten. Eine solche Kombination nennen wir eine *Belegung*. Dazu ist eine Liste von Klauseln gegeben, wobei eine *Klausel* eine Vorschrift der Art $C = (x_{i_1} \neq v_1 \vee x_{i_2} \neq v_2 \vee \ldots \vee x_{i_k} \neq v_k)$ sei. Dabei sind v_1 bis v_k feste Werte aus $\{1, 2, \ldots, d\}$, und die einzelnen Disjunkte $x_{i_j} \neq v_j$ werden *Literale* genannt. Für die Menge der in der Klausel vorkommenden Variablen schreiben wir $\mathrm{vbl}(C)$.

Wie dieser Darstellung leicht zu entnehmen ist, ist eine Klausel nur genau dann *verletzt*, wenn von allen k Variablen, von denen die Klausel spricht, eine jede genau denjenigen Wert annimmt, welchen die Klausel verbietet. In allen anderen Fällen ist die Klausel erfüllt. Eine solche Probleminstanz bestehend aus einer gegebenen Liste von Klauseln nennen wir eine *Formel*. Das Klauselerfüllungsproblem besteht nun darin, zu entscheiden, ob es möglich ist, den Variablen Werte zuzuweisen dergestalt, dass alle Klauseln gleich-

zeitig erfüllt sind. Beim *Entscheidungsproblem* lautet die korrekte Antwort lediglich entweder `ja` oder `nein`, beim *Suchproblem* hingegen soll die Antwort im positiven Fall eine korrekte Wertebelegung beinhalten (und im negativen Fall wiederum `nein` lauten).

Haben in einem Klauselerfüllungsproblem alle Klauseln dieselbe Grösse k und können alle Variablen je genau d Werte annehmen, dann spricht man von einem (d, k)-Klauselerfüllungsproblem oder abgekürzt (d, k)-ClSP (engl. "Clause Satisfaction Problem"). Im speziellen Fall, wo $d = 2$ ist, sprechen wir auch von einer k-SAT Formel (von engl. "satisfiability problem", *Erfüllbarkeitsproblem*).

In den Siebzigerjahren haben Cook und Levin unabhängig voneinander das Prinzip der NP-Vollständigkeit entdeckt und bewiesen, dass *Erfüllbarkeitsprobleme*, darunter das Klauselerfüllungsproblem, NP-vollständig sind. Seither wurde für Hunderte natürlicher Probleme die Zugehörigkeit zu dieser Klasse nachgewiesen. Die Erfüllbarkeitsprobleme nehmen darunter aber bis heute eine sehr herausragende Rolle ein, welche weit über ihre historische Bedeutung hinausgeht.

Dies begründet sich darin, dass die allermeisten NP-vollständigen Probleme eine einfache wenn nicht unmittelbare Übersetzung in ein Erfüllbarkeitsproblem zulassen, während dies umgekehrt nur selten der Fall ist. Will man, um ein klassisches Beispiel zu nennen, einen Graphen so mit drei Farben färben, dass keine zwei mit einer Kante verbundenen Knoten die gleiche Farbe erhalten (ein prominentes NP-vollständiges Problem), dann lässt sich dies durch ein Klauselerfüllungsproblem darstellen: jeder Knoten wird durch eine Variable repräsentiert, welche einen von drei Werten annehmen kann, und für jede Kante fügen wir dem Problem drei 2-Klauseln hinzu, eine für jede verbotene Farbübereinstimmung. Da beide Probleme NP-vollständig sind, gibt es auch die umgekehrte Transformation, welche ein Klauselerfüllungsproblem in einen Graphen überführt, der genau dann 3-färbbar ist, wenn das Ausgangsproblem erfüllbar war. Doch so eine Transformation erfordert nichttriviale Konstruktionen.

Will man, um ein weiteres klassisches Beispiel zu bemühen, entscheiden, ob ein Graph einen Hamiltonkreis besitzt, also einen Pfad welcher jeden der n Knoten genau einmal besucht, so kann man n Variablen $x_1, x_2, \ldots, x_n$ verwenden, wobei jede einen Wert aus $\{1, 2, \ldots, n\}$ annehmen kann und der Wert von x_i anzeigt, in welchem Schritt des Pfades Knoten i besucht werden soll. Es müssen lediglich noch Klauseln zugefügt werden, um sicherzustellen, dass keine zwei Knoten denselben Index erhalten, und dass keine zwei Knoten mit aufeinanderfolgenden Indizes nicht mit einer Kante verbunden sind. Die umgekehrte Transformation hingegen benötigt hochgradig nicht-triviale Konstruktionen. Es lassen sich zahllose weitere Beispiele auflisten.

Es ist deshalb gerechtfertigt, Klauselerfüllungsprobleme als prototypische NP-schwere Probleme anzusehen und ihnen eine besonders grosse Aufmerksamkeit zu widmen. Neue Erkenntnisse über diese Probleme und ihre Lösbarkeit lassen sich mit grosser Wahrscheinlichkeit ohne Umwege auf eine Vielzahl anderer Probleme übertragen.

Weitere Bedeutung kommt Erfüllbarkeits- und Klauselerfüllungsproblemen auch durch deren industrielle Anwendungen zu. Chiphersteller überprüfen die Entwürfe ihrer Mikroprozessoren systematisch auf Fehler, indem sie sie in Erfüllbarkeitsprobleme umwandeln, für die sodann eine erfüllende Belegung gesucht wird. Infolgedessen hat sich ein gesamter

Forschungs- und Industriezweig entwickelt, welcher mit der Herstellung von SAT-Solvern, also Software zur Lösung von Erfüllbarkeitsproblemen, bemüht ist. Während sich die dort angewendeten Methoden zum heutigen Zeitpunkt auffallend stark unterscheiden von denjenigen, die wir in der Theorie und somit etwa in dieser Arbeit betrachten, so darf man dennoch hoffen, dass ein tieferes Verständnis des Problems zukünftig auch praktische Anwendungen inspiriert.

1.1 Inhalt der Arbeit

Die meisten Forscher gehen davon aus, dass für Probleme aus der NP-vollständigen Klasse und damit für Erfüllbarkeitsprobleme keine Polynomialzeitlösung existiert. Stärker noch gilt es allgemein als sehr wahrscheinlich, dass der schnellste Algorithmus für Erfüllbarkeitsprobleme eine exponentielle Laufzeit hat ("Exponentialzeithypothese"). Damit soll deren Betrachtung aber nicht abgeschlossen sein. Im Gegenteil bietet sich weiterhin eine ganze Reihe interessanter Ansatzpunkte.

Zum Einen kann man versuchen, Klassen von Probleminstanzen zu identifizieren, für welche das Problem effizient lösbar wird. Forscher etwa, die sich mit SAT-Solvern für die Praxis beschäftigen, konzentrieren sich dabei auf die von verschiedenen industriellen Applikationen herrührenden Problemklassen und untersuchen deren statistische Eigenschaften. Statistische Physiker betrachten zufällig generierte Erfüllbarkeitsprobleme, für die Zusammenhänge zum Verhalten gewisser physikalischer Systeme entdeckt wurden. Sie sind an Verfahren interessiert, die über die Eingabeverteilung mit hoher Wahrscheinlichkeit erfolgreich sind. Für uns und in dieser Arbeit von Interesse sind hingegen Problemklassen, welche anhand einfach zu erkennender kombinatorischer Kriterien (in casu der Grad an Konflikten zwischen Klauseln) identifizierbar sind.

Zum Andern kann man auch für das allgemeine Problem selbst unter der Exponentialzeithypothese nach einem "schnellen" Algorithmus suchen, in dem Sinne, dass die Basis der Exponentialfunktion möglichst klein und damit das Wachstum möglichst moderat bleiben soll. Wie im Folgenden zusammengefasst enthält die Arbeit je einen Teil aus jeder der beiden Teildisziplinen.

2 Das Local Lemma

2.1 Ausgangslage

Ein guter erster Ansatzpunkt für das Studium von Klauselerfüllungsproblemen dürfte die Frage sein, was es zu einer unerfüllbaren Probleminstanz braucht. Zunächst fällt uns auf, dass eine gewisse Anzahl Klauseln notwendig ist. Betrachten wir zum Beispiel die Klasse der (d, k)-ClSP Formeln, so stellt sich heraus, dass die kleinste unerfüllbare Formel dieser Klasse d^k Klauseln besitzt. Ein Beispiel dieser Grösse ist leicht zu konstruieren: wir verwenden genau k Variablen und fügen zu der Formel sämtliche d^k möglichen Klauseln

über diesen Variablen hinzu. Dadurch sind alle Belegungen verboten, jede von genau einer Klausel, und somit wird das Problem unerfüllbar. Anderseits zeigt ein einfaches Argument nach der auf Erdős zurückgehenden *probabilistischen Methode*, dass jede Instanz mit weniger Klauseln erfüllbar sein muss. Wenn wir nämlich die Werte aller Variablen nach einer Uniformverteilung zufällig und voneinander unabhängig wählen, dann hat jede Klausel eine Wahrscheinlichkeit von genau d^{-k}, verletzt zu sein. Der Erwartungswert der Anzahl verletzten Klauseln wäre dann $m \cdot d^{-k}$, wenn m die Anzahl Klauseln in der Formel ist. Ist m aber kleiner als d^k, so ist dieser Erwartungswert kleiner eins, und somit muss es eine positive Wahrscheinlichkeit geben, dass die Anzahl verletzter Klauseln null wird. Das ist aber nur möglich, wenn eine erfüllende Belegung existiert.

Damit ist ein erstes, einfach zu erkennendes Kriterium ausgearbeitet, von dem direkt auf die Erfüllbarkeit einer Formel geschlossen werden kann. Die Aussage ist allerdings noch schwach, da die Klasse der Formeln mit derart wenigen Klauseln nicht sehr vielfältig und daher von minderem Interesse ist.

Im Jahre 1975 haben Erdős und Lovász [EL75] eine Entdeckung gemacht, welche diese einfache Überlegung zu einem der stärksten und am meisten angewendeten Werkzeugen der Kombinatorik weiterentwickelte. Sie stellten fest, dass in einem unerfüllbaren Problem nicht nur die Gesamtzahl der Klauseln mindestens d^k betragen muss, sondern dass darüberhinaus eine fast so grosse Anzahl an Klauseln an einer einzigen Stelle konzentriert auftreten muss[1]. Ein intuitives Verständnis hierfür ist leicht zu entwickeln: in unserem einfachsten Beispiel einer unerfüllbaren Formel haben wir d^k Klauseln, alle über denselben k Variablen, aufeinandergestapelt. Hätten wir die Klauseln so lose wie möglich verteilt, d.h. so, dass keine zwei eine gemeinsame Variable verwenden, so wäre die Formel selbstverständlich erfüllbar; man könnte jede Klausel einzeln und unabhängig erfüllen. Irgendwo zwischen den beiden Extremen muss bezüglich des Grades an Klauselüberlappung ein Schwellwert liegen, von welchem an die Konstruktion einer unerfüllbaren Formel möglich wird. Wie Erdős und Lovász festgestellt haben, liegt dieser Schwellwert nahe bei d^k, nämlich ungefähr bei d^k/e, wobei e die Eulersche Zahl ist. Dies führte zur einfachsten Form des inzwischen sehr bekannten und vielseitig angewendeten Lovász Local Lemma.

Theorem 1 ([EL75] Symmetrisches Lovász Local Lemma für ClSPs)**.** *Sei F eine (d,k)-ClSP Formel. Für jede Klausel $C \in F$ sei die* Nachbarschaft *von C definiert als $\Gamma_F(C) := \{D \in F \mid C \neq D,\ vbl(C) \cap vbl(D) \neq \emptyset\}$. Falls für alle Klauseln $C \in F$ gilt $|\Gamma_F(C)| \leq d^k/e - 1$, dann ist F erfüllbar.*

Inzwischen existieren von diesem Theorem diverse Verallgemeinerungen und Weiterentwicklungen, von denen wir in der Arbeit einige zitieren. Für uns von zentralem Interesse ist jedoch die Frage ob nun, da wir wissen, dass ein Klauselerfüllungsproblem mit einer nirgends zu dichten Konzentration an Klauseln immer erfüllbar ist, darüberhinaus auch die Möglichkeit besteht, für solch eine Formel eine erfüllende Belegung algorithmisch effizient zu *ermitteln*.

Diese sich nach der Entdeckung des Lemmas sofort aufdrängende Frage blieb lange unbe-

[1] Was wir hier verschweigen, ist die Tatsache, dass Erdős und Lovász sich nicht mit dem Klauselerfüllungsproblem, sondern mit dem sehr nahe verwandten Hypergraphen-Färbungsproblem beschäftigten. Wir übertragen ihre Erkenntnisse hier stillschweigend auf das für uns interessante Problem.

antwortet. Erst im Jahre 1991 gelang Beck [Bec91] ein erster Durchbruch. Er wies einen Algorithmus aus, welcher erfüllbare Belegungen in Polynomialzeit liefern konnte für Formeln, welche eine dem Local Lemma gleichartige aber restriktivere Bedingung erfüllen. Wenn nämlich in einem (d, k)-Klauselerfüllungsproblem die Nachbarschaft jeder Klausel aus höchstens (ungefähr) $d^{k/48}$ anderen Klauseln besteht, dann lässt sich ein zweiphasiges Verfahren darauf anwenden, bei dem zunächst alle Variablen eine Belegung erhalten, dann "schlecht erfüllte" Formelteile isoliert und die dort vorgefundenen Variablen neu belegt werden. Stark vereinfacht gesagt ist dieses Verfahren deswegen effizient, weil durch das Ausscheiden "gut erfüllter" Formelteile das Klauselerfüllungsproblem in kleine Komponenten zerfällt, die man einzeln lösen kann und die so klein sind, dass der dafür verwendete Algorithmus nicht mehr effizient sein muss. Um allerdings das Finden einer erfüllenden Belegung unter diesem Verfahren garantieren zu können, ist es notwendig, dass selbst nach dem Zerlegungsvorgang alle übrigbleibenden Formelteile das Local Lemma erfüllen. Um dies zu erreichen ist die erheblich verstärkte Bedingung notwendig. Der Korrektheitsbeweis verwendet sodann die Originalversion des Local Lemma.

Auf diesen Durchbruch hin gab es verschiedene Versuche, die restriktive Konstante von $1/48$ im Exponenten (wodurch die Nachbarschaften auf die 48ste Wurzel (!) des Schwellwertes im nichtkonstruktiven Local Lemma beschränkt bleiben) zu vergrössern. Kurz darauf erreichte Alon [Alo91] eine Verbesserung auf $1/8$ und vereinfachte Beck's Verfahren massgeblich, was es weiteren Verbesserungen auf zunächst $1/6$ [Mos06], dann durch Srinivasan [Sri08] auf $1/4$ und schliesslich auf $1/2$ [Mos08] zugänglich machte. Alle diese Verfahren bestanden aber weiterhin aus einer Zuweisungsphase und einer Neuzuweisungsphase mit einigen fixierten Variablen, was ihnen inhärente Grenzen setzt.

In der vorliegenden Arbeit präsentieren wir stattdessen eine iterative Methode, welche die Konstante im Exponenten beseitigt und darüberhinaus eleganter ist, da sie auf den ursprünglichen nicht-konstruktiven Beweis nicht mehr zurückgreift und stattdessen einen unabhängigen konstruktiven Beweis für die Aussage des Local Lemma selbst liefern kann.

2.2 Ein einfacher Algorithmus

Wir betrachten den folgenden, denkbar einfachen Algorithmus zum Finden einer erfüllenden Belegung für eine erfüllbare ClSP-Formel F. Wir beginnen mit einer zufällig gewählten Belegung aller Variablen. Solange die Belegung die Formel noch nicht erfüllt, wählen wir eine beliebige verletzte Klausel aus, löschen die gegenwärtigen Belegungen der Variablen in dieser Klausel und ersetzen sie durch neue uniform zufällig Gewählte.

Es ist leicht nachzuprüfen, dass dieser Algorithmus mit Wahrscheinlichkeit eins terminiert, wennimmer die Eingabeformel erfüllbar ist. Erwartungsgemäss ist die erwartete Zeit bis dahin allerdings im Allgemeinen exponentiell in der Anzahl n der Variablen. Liegt nun jedoch eine Formel vor, welche die Bedingungen des Local Lemma erfüllt, dann können wir beweisen, dass dieser Algorithmus (sehr) effizient ist, nämlich eine erwartete Laufzeit hat, welche linear ist in der Anzahl m der Klauseln.

Algorithmus 1 LocalSolver(F)

Vorbedingung: Eine erfüllbare ClSP-Formel F.
Nachbedingung: Ausgabe ist eine erfüllende Belegung.

```
1: α ← eine uniform zufällige Belegung der Variablen
2: while ∃C ∈ F : α verletzt Klausel C do
3:     C ← irgendeine von α verletzte Klausel
4:     for x ∈ vbl(C) do
5:         α(x) ← neue uniform zufällige Belegung für x
6:     end for
7: end while
```

2.3 Eckpfeiler der Analyse

Die grobe Grundidee der Analyse lässt sich am besten informationstheoretisch erläutern[2]. Nehmen wir an, der Algorithmus produziere zur Laufzeit ein Ausführungsprotokoll, in welchem alle seine Aktionen festgehalten werden. Dazu gehören die in zeitlicher Abfolge aufgelisteten Klauseln, welche von dem Algorithmus zum Korrigieren ausgewählt worden sind sowie die zufällig ausgewählten Variablenzuweisungen. Das zentrale Element des Beweises ist die Feststellung, dass aus solch einem Protokoll letzteres, also die Variablenwerte, weggelassen werden kann. Denn diese sind aus der Liste der korrigierten Klauseln leicht zu rekonstruieren: weiss man, dass die Klausel $(x \neq 5 \vee y \neq 7 \vee z \neq 2)$ korrigiert wurde, dann kann man daraus schliessen, dass die Variablen x, y und z zu diesem Zeitpunkt die Werte 5, 7 und 2 hatten.

Und nun stellt man sich die Frage nach dem Informationsgehalt eines Ausführungsprotokolls, das nur die Liste der korrigierten Klauseln enthält. Sollte der Algorithmus wider erwarten sehr lange ausgeführt werden, dann kann dies nur aus dem Grunde geschehen, dass wiederholt durch das Korrigieren von Klauseln andere Klauseln verletzt worden sind. Das Korrigieren einer Klausel kann jedoch nur Klauseln in deren Nachbarschaft in Mitleidenschaft ziehen. Es muss mithin in einem langen Ausführungsprotokoll viele Stellen geben, wo benachbarte Klauseln aufeinanderfolgen. Solch ein Protokoll ist komprimierbar, wenn die Nachbarschaften wie in einer Local Lemma Formel klein sind, denn statt die nachfolgende Klausel mit ihrem globalen Index zu kodieren, können wir stattdessen einen lokalen Index der Klausel bezüglich der Nachbarschaft des Vorgängers verwenden. Tatsächlich stellt sich heraus, dass, wenn die Nachbarschaften um einen hinreichend grossen konstanten Faktor kleiner sind als d^k, es *weniger* Bits braucht um einen durchschnittlichen Eintrag des Ausführungsprotokolles zu kodieren als zufällige Bits (die Variablenwerte) aus diesem Protokoll nach dem vorhin beschriebenen Verfahren rekonstrukiert werden können. Das ist aber ein Widerspruch, denn es wurden uniform zufällige Bits verwendet,

[2]Im Sinne der wissenschaftlichen Aufrichtigkeit sei an dieser Stelle darauf hingewiesen, dass sich nach Veröffentlichung der Arbeit [Mos09] herausstellte, dass ein sehr ähnlich gearteter, auf Informationstheorie beruhender Beweis bereits in einer unabhängigen Arbeit von Schweitzer [Sch09] entdeckt worden war, in welcher jedoch die wichtige Schlussfolgerung fehlte, dass sich daraus ein algorithmisches Verfahren ableiten lässt und nicht nur eine interessante Beweismethode für bereits bekannte kombinatorische Ergebnisse.

die nach dem einfachsten informationstheoretischen Grundsatz nicht komprimierbar sind. Ausführungsprotokolle können also im Mittel nicht so lang sein, dass sich diese Kompression "lohnt"; sie müssen im Mittel kurz sein und damit der Algorithmus im Erwartungswert effizient.

Um das Ergebnis mit den besten Konstanten und für allgemeinere Fälle zu erhalten muss der Beweis allerdings etwas technischer geführt werden, indem sogenannte, nochimmer auf die Arbeit von Beck [Bec91] zurückgehende "Zeugenbäume" verwendet werden. Beide Pfade verfolgen wir in Kapitel 2 der Arbeit.

3 Schöning's Algorithmus

3.1 Motivation und Ausgangslage

Im zweiten Teil verlassen wir die in Polynomialzeit lösbaren Problemklassen und interessieren uns stattdessen für Algorithmen, welche auf das Lösen des allgemeinen Klauselerfüllungsproblems zugeschnitten sind. Nach dem heutigen Stand der Forschung müssen wir davon ausgehen, dass die Laufzeit solcher Algorithmen exponentiell ist, aber wir können uns um eine möglichst kleine Basis der Exponentialfunktion bemühen.

Exponentialzeitalgorithmen für SAT und ClSP haben ebenfalls eine lange Geschichte. Der triviale Algorithmus, welcher alle möglichen Belegungen aufzählt und jede Einzelne prüft, benötigt zur Lösung einer beliebigen (d,k)-ClSP Formel über n Variablen $d^{n+o(n)}$ Zeit. Im Jahre 1985 waren Monien und Speckenmeyer [MS85] die Ersten, welche einen Algorithmus vorschlugen, der durch rekursive Fallunterscheidungen in lokalen Klauselkonfigurationen eine Laufzeit von $c^{n+o(n)}$ für einen Wert $c < d$ erreicht. Im Anschluss an ihre Arbeit veröffentlichten diverse Forscher immer leistungsfähigere aber auch kompliziertere Rekursionsverfahren. Die Kulmination dieses Forschungszweigs wurde mit dem über 70 Seiten umfassenden Paper von Kullmann [Kul09] und der darauf aufbauenden Arbeit von Rodošek [Rod96] erreicht. Letzterer konnte 3-SAT, also $(2,3)$-ClSP, in Zeit $\mathcal{O}(1.476^n)$ lösen, was gegenüber der trivialen Zeit von $2^{n+o(n)}$ eine beachtliche Verbesserung darstellt.

Durch den neuen Trend zur Randomisierung inspiriert wurden diese aufwändigen Verfahren aber sehr plötzlich durch neue, viel einfachere Techniken überholt. Im Jahre 2013 sind nurmehr zwei randomisierte SAT-Algorithmen mit einer konkurrenzfähigen Laufzeit im Rennen. Einer von ihnen ist der lokale Suchalgorithmus von Uwe Schöning, der eine Laufzeit von $\mathcal{O}(1.334^n)$ im Falle von 3-SAT ausweist. Wir zeigen in vorliegender Arbeit, dass Schöning's Algorithmus ausserdem sehr leicht derandomisiert werden kann, ohne dass, wie es bei früheren Versuchen dazu der Fall war, eine Einbusse bei der Laufzeit in Kauf genommen werden müsste. Mit einer zusätzlichen Verbesserung von Makino et. al. [MTY11] erreicht unsere deterministische Variante eine Laufzeit von $\mathcal{O}(1.331^n)$. Während es in der randomisierten Disziplin effizientere Algorithmen gibt (namentlich den sogenannten *PPSZ-Algorithmus*), ist für diese keine verlustfreie Derandomisierung bekannt, sodass unser Verfahren unter den Deterministischen gegenwärtig das Schnellste ist.

Dieses Kapitel ist eine gemeinsame Arbeit mit Dominik Scheder [MS11].

3.2 Algorithmus und randomisierte Analyse

Wie der Local Lemma Solver aus dem ersten Teil belegt Schöning's Algorthmus zunächst alle Variablen mit uniform zufälligen Werten, wählt dann in jedem Schritt eine beliebige, gegenwärtig verletzte Klausel aus und ändert deren Belegung. Der einzige Unterschied besteht im Vorgehen bei dieser Änderung: statt alle Variablen zufällig neu zu belegen, wählt der Algorithmus nur eine Variable aus der Klausel zufällig aus und ändert deren Wert.

Algorithmus 2 Schöning(F)

Vorbedingung: Eine erfüllbare (d,k)-ClSP Formel F.
Nachbedingung: α is eine erfüllende Belegung für F.

1: $\alpha \leftarrow$ eine uniform zufällige Belegung der Variablen
2: **while** $\exists C \in F : \alpha$ verletzt Klausel C **do**
3: $\quad C \leftarrow$ irgendeine von α verletzte Klausel
4: $\quad x \leftarrow$ eine uniform zufällig gewählte Variable aus vbl(C)
5: $\quad \alpha(x) \leftarrow$ ein uniform zufälliger Wert aus $\{1..d\} \setminus \alpha(x)$
6: **end while**

Wie Schöning zeigen konnte, hat dieser Algorithmus im Falle einer erfüllbaren 3-SAT Formel eine Wahrscheinlichkeit von mindestens $(3/4)^{n+o(n)}$, innert $\mathcal{O}(n)$ Schritten eine erfüllende Belegung zu entdecken. War der Algorithmus innert dieser Zeit nicht erfolgreich, bricht man ihn ab und beginnt einen neuen Versuch mit einer zufälligen Anfangsbelegung. Daraus ergibt sich ein randomisiertes Verfahren mit der gewünschten erwarteten Laufzeit von $(4/3)^{n+o(n)}$.

3.3 Derandomisierung

Die erste derandomisierte Variante von Schöning's Algorithmus wurde von Dantsin et. al. geliefert [DGH$^+$02] und hatte, im 3-SAT-Fall, eine Laufzeit von $\mathcal{O}(1.481^n)$. Brüggemann und Kern [BK04] verbesserten diese Laufzeit auf $\mathcal{O}(1.473^n)$. Schliesslich verbesserten Scheder [Sch10] und dann Kutzkov und Scheder [KS10] die Laufzeit auf $\mathcal{O}(1.465^n)$ und $\mathcal{O}(1.439^n)$. Die neue von uns vorgestellte Version erreicht $\mathcal{O}(1.334^n)$ Zeit, also dieselbe Laufzeit wie die randomisierte Variante im Erwartungswert.

Die Derandomisierung fusst auf einer Grundidee, wonach zunächst die randomisierte Variante genauer analysiert wird um die Anzahl der tatsächlich benötigten Zufallsbits zu minimieren. Betrachtet man die statistischen Eigenschaften des Algorithmus, so stellt man fest, dass nur ganz bestimmte Typen charakteristischer Ausführungen regelmässig zu einer erfüllenden Belegung führen. So kann man sich etwa im Falle von 3-SAT auf

Ausführungen beschränken, bei denen die Anfangsbelegung einen Abstand (Anzahl unterschiedlich belegte Variablen) von genau $n/3$ zu einer festen, erfüllenden Belegung aufweist und bei denen weiters genau n Korrekturschritte ausgeführt werden von denen ein Anteil von genau $2/3$ den Abstand zur erfüllenden Belegung verkleinert während $1/3$ den Abstand vergrössert. Betrachtet man eine Ausführung des Algorithmus nur gerade *dann* als erfolgreich wenn alle diese Ereignisse eintreten und vernachlässigt alle anderen Fälle, so summieren sich die erfolgreichen Fälle noch immer zu einer Wahrscheinlichkeit von $(3/4)^{n+o(n)}$ auf, womit man nichts verloren hat.

Für eine Derandomisierung genügt es also, eine Menge von Ausführungen aufzuzählen, unter denen mindestens eine mit den beschriebenen Eigenschaften zu finden ist. Wie sich herausstellt lässt sich dies mithilfe sogenannter *Überdeckungscodes* leicht bewerkstelligen. Zunächst verwendet man einen Code aus regelmässig über den Lösungsraum verteilten Belegungen, von denen aus jeder Punkt im Raum höchstens Abstand $n/3$ hat. In so einem Code ist auf jeden Fall eine geeignete Anfangsbelegung zu finden. Sodann führt man – statt wie im randomisierten Fall jeden Korrekturschritt einzeln – Blöcke von Korrekturschritten für eine grössere Menge von unabhängigen, verletzten Klauseln gleichzeitig durch, wobei die zu korrigierenden Variablen in jeder Klausel wiederum anhand eines Überdeckungscodes ausgewählt werden. Diesmal bietet der Überdeckungscode die Garantie, dass mindestens eines der Codeworte in $2/3$ der Klauseln eine Verbesserung und höchstens in $1/3$ der Klauseln eine Verschlechterung der Situation bewirkt. Indem man beinahe-optimale Überdeckungscodes verwendet (die glücklicherweise effizient konstruierbar sind) und die Anfangsbelegungen mit den Blöcken von Korrekturschritten zu einem rekursiven Algorithmus zusammensetzt, erreicht man schliesslich das Ziel einer verlustfreien Derandomisierung.

Bibliographie

[Alo91] Noga Alon. A Parallel Algorithmic Version of the Local Lemma. *Random Structures and Algorithms*, 2(4):367–378, 1991.

[Bec91] József Beck. An Algorithmic Approach to the Lovász Local Lemma. I. *Random Structures and Algorithms*, 2(4):343–365, 1991.

[BK04] Tobias Brueggemann und Walter Kern. An Improved Deterministic Local Search Algorithm for 3-SAT. *Theoretical Computer Science*, 329(1-3):303–313, 2004.

[DGH+02] Evgeny Dantsin, Andreas Goerdt, Ewald A. Hirsch, Ravi Kannan, Jon M. Kleinberg, Christos H. Papadimitriou, Prabhakar Raghavan und Uwe Schöning. A Deterministic $(2-2/(k+1))^n$ Algorithm for k-SAT Based on Local Search. *Theoretical Computer Science*, 289(1):69–83, 2002.

[EL75] Paul Erdős und László Lovász. Problems and Results on 3-Chromatic Hypergraphs and Some Related Questions. In A. Hajnal, R. Rado und Vera T. Sós, Hrsg., *Infinite and Finite Sets (to Paul Erdős on his 60th birthday), Vol. II*, Seiten 609–627. North-Holland, 1975.

[KS10] Konstantin Kutzkov und Dominik Scheder. Using CSP To Improve Deterministic 3-SAT. *CoRR*, abs/1007.1166, 2010.

[Kul09] Oliver Kullmann, Hrsg. *Theory and Applications of Satisfiability Testing - SAT 2009, 12th International Conference, SAT 2009, Swansea, UK, June 30 - July 3, 2009. Proceedings*, Jgg. 5584 of *Lecture Notes in Computer Science*. Springer, 2009.

[Mos06] Robin A. Moser. On the Search for Solutions to Bounded Occurrence Instances of SAT, Semester Thesis, ETH Zürich, 2006.

[Mos09] Robin A. Moser. A Constructive Proof of the Lovász Local Lemma. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC 2009)*, Seiten 343–350, 2009.

[Mos12] Robin A. Moser. *Exact Algorithms for Constraint Satisfaction Problems*. Dissertation, ETH Zürich, 2012.

[MS85] Burkhard Monien und Ewald Speckenmeyer. Solving Satisfiability in less than 2^n Steps. *Discrete Applied Mathematics*, 10:287–295, 1985.

[MS11] Robin A. Moser und Dominik Scheder. A Full Derandomization of Schöning's k-SAT Algorithm. In *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing (STOC 2011)*, Seiten 245–252, 2011.

[MTY11] Kazuhisa Makino, Suguru Tamaki und Masaki Yamamoto. Derandomizing HSSW Algorithm for 3-SAT. In *COCOON*, Seiten 1–12, 2011.

[Rod96] Robert Rodošek. A New Approach on Solving 3-Satisfiability. In *AISMC*, Seiten 197–212, 1996.

[Sch09] Pascal Schweitzer. Using the Incompressibility Method to Obtain Local Lemma Results for Ramsey-Type Problems. *Information Processing Letters*, 109(4):229–232, 2009.

[Sch10] Dominik Scheder. Using a Skewed Hamming Distance to Speed Up Deterministic Local Search. *CoRR*, abs/1005.4874, 2010.

[Sri08] Aravind Srinivasan. Improved Algorithmic Versions of the Lovász Local Lemma. In *Proceedings of the 19th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2008)*, Seiten 611–620, Philadelphia, PA, USA, 2008. Society for Industrial and Applied Mathematics.



Dr. Robin A. Moser studierte ab 2002 an der ETH Zürich Informatik mit Spezialisierung auf theoretische Informatik. Im Jahre 2007 absolvierte er ein Praktikum als Softwareingenieur am Genfer Forschungsinstitut für Teilchenphysik CERN. Darauf schloss er sich Anfang 2008 der Forschungsgruppe von Professor Emo Welzl ("Kombinatorische Algorithmen") im Rahmen des *Fast Track* Programms der ETH Zürich an. Er erhielt 2008 den *Master of Science ETH in Computer Science* und 2013 den Titel *Doctor of Sciences ETH* für seine hier beschriebene Arbeit.

Verteiltes Dokumenten-orientiertes Prozessmanagement im Gesundheitswesen

Christoph P. Neumann

Friedrich-Alexander-Universität Erlangen-Nürnberg
christoph.neumann@fau.de

Abstract: In Situationen die eine organisationsübergreifende Zusammenarbeit über regionale Grenzen hinaus erfordern ist es notwendig die Systemfunktionalitäten zur Prozessunterstützung von den bestehenden Anwendungssystemen zu entkoppeln. In dieser Arbeit wird ein Ansatz für verteilte Fallführung vorgestellt, der Ad-hoc-Kooperationen mit Hilfe von aktiven Dokumenten ermöglicht ohne zuvor die lokalen Anwendungssysteme zu integrieren. Eine verteilte Fallakte wird dazu eingesetzt zusammenarbeitende Prozessbeteiligte zu koordinieren. Als aktives Dokument führt das Fallakten-Artefakt sein eigenes Anzeige- und Steuer-Programm eingebettet mit sich. Die Fallakte beinhaltet beliebige elektronische Dokumente mit medizinischem Inhalt, die zwischen den Beteiligten ausgetauscht werden. Außerdem beinhaltet sie die Prozessstruktur für einen organisationsübergreifenden Therapieplan in Form einer gemeinsamen Arbeitsliste. Zur Veranschaulichung des Konzepts dient ein organisationsübergreifender Anwendungsfall, dazu dient der kooperative Behandlungsprozess für Brustkrebs-Patientinnen.

1 Einleitung

Die richtige Form von IT-Unterstützung für organisationsübergreifende Kooperationen zu finden ist in vielen Domänen eine ungelöste Herausforderung. In Deutschland ist das zentrale Element für medizinische Kooperation bis heute der klassische Austausch von papierbasierter Information auf traditionellen Wegen. Das Gesundheitswesen leidet, hinsichtlich der Zusammenarbeit von Ärzten, unter sogenannter *Systemfragmentierung*, was bedeutet, dass Patienten häufig von mehreren Leistungserbringern behandelt werden, ohne dass die Zusammenarbeit koordiniert stattfindet. (z. B. [TOG10]). Seit den 80er Jahren begegnet man dieser Systemfragmentierung mit Bestrebungen sogenannter *Versorgungskontinuität* (engl. „continuity of care“) und *integrierter Versorgung*. Dennoch gehört die unzureichende Verfügbarkeit von patientenbezogener Information bis heute zu den prominentesten Problemen medizinischer Zusammenarbeit (z. B. [DMC+10]).

Ein grundlegender Hemmfaktor für eine erfolgreiche IT-Unterstützung ist die ungelöste Aufgabe der Systemintegration (z. B. [Len09]). Roland Bergers bedeutende Studie von 1997 beschreibt die Vision einer „integrierten multimedialen elektronischen Patientenakte“ [Ber97] als IT-basierte Lösung für eine integrierte Versorgung. Dieses Konzept ist als Kürzel auch in seiner englischen Übersetzung bekannt, als Electronical Health Record (EHR). Die Verwirklichung solch großflächiger oder bundesweiter EHR-Infrastrukturen liegt jedoch nach wie vor in weiter Ferne. Auch derzeitige Anstrengungen, wie das staat-

liche Großprojekt „Elektronische Gesundheitskarte“ (eGK), werden in absehbarer Zeit keine Besserung erreichen.

Im weiteren Verlauf der Einleitung werden die Problemstellung und die Ziele der Arbeit dargestellt sowie die Vision einer verteilten Fallakte erzählerisch mit Hilfe einer Benutzerszene veranschaulicht. Der anschließende Abschnitt beschreibt Methoden ‘aktiver’ Dokumente sowie des Prozessmanagements und stellt die konzeptionellen Beiträge des Ansatzes dar. Der letzte Abschnitt diskutiert Ergebnisse und offene Fragestellungen.

1.1 Problemstellung

Der primäre Anwendungsfall ist ein überregionales und sektorenübergreifendes medizinisches Szenario. Zu Beginn des Projekts gab es für meinen Doktorvater und mich eine Prämisse: „Es existiert keine adäquate IT-Infrastruktur zur Unterstützung spontan entstehender verteilter Zusammenarbeit“. Dies gilt für das Gesundheitswesen genauso wie für andere Domänen. Daher standen zwei grundsätzliche wissenschaftliche Fragestellungen im Vordergrund: (1) „Können wir eine Infrastruktur entwickeln, die es ermöglicht emergente Ad-hoc-Prozesse zu unterstützen?“ sowie (2) „Bis zu welchem Ausmaß können wir einen Informationsaustausch realisieren ohne irgendeine Systemintegration voraussetzen zu können?“. Eine solche Infrastruktur muss Funktionalitäten jenseits von E-Mail bereitstellen und an typische Anforderungen solcher Kooperationen angepasst sein.

Der anfängliche Aufwand um einen Informationsaustausch zu etablieren muss möglichst gering sein. Insgesamt suchen wir nach einem anpassbaren und dezentralisierten Ansatz. Die traditionelle Vorgehensweise um organisationsübergreifende medizinische Prozesse zu steuern, basiert auf Papierdokumenten mit spezifischer Semantik, beispielsweise Überweisungsschein und Arztbrief. Wir übernehmen dieses papierbasierte Interaktionsparadigma und erweitern es elektronisch, sodass komplexere Anwendungsfälle ermöglicht werden. Die Papierformulare werden zu digitalen Informationseinheiten, die aus den beteiligten lokalen Systemen als Dokument exportiert werden[1] und Gegenstand eines verteiltes Publish/Subscribe-Systems werden, das die Fallakten zwischen den jeweils Beteiligten synchronisiert. Das Werkzeug für die Fallführung ist zu einem einzigen installationslosen Datei-Artefakt zusammengeschnürt, welches zwischen den Teilnehmern vervielfältigt werden kann und den Datenbestand einer einzelnen verteilten Fallakte verwaltet.

Das daraus resultierende Artefakt entspricht der Idee eines aktiven Dokuments. Dieses Konzept wurde erstmalig von Dourish et al. für deren Placeless Documents [DEL+00] beschrieben und wird später noch weiter ausgeführt. Aus diesem Zusammenhang heraus nennt sich das primäre Artefakt meines Ansatzes α-*Doc*, wobei das „α“ symbolisch für den Begriff „aktiv“ steht. Der konzeptionelle Ansatz nennt sich distributed Document-oriented Process Management (dDPM) und die Referenz-Implementierung als Software-Prototyp heißt α-*Flow*. Die verschiedenen Aspekte des α-*Flow*-Systems und des dDPM-Ansatzes wurden bereits in diversen Publikationen veröffentlicht (u. a.

[1] Ein wichtiges Merkmal aller Informationseinheiten, die organisationsübergreifend ausgetauscht werden, ist, dass sie notwendigerweise ausgedruckt werden können. Über die Druckbarkeit ist eine grundsätzliche Garantie gegeben, diese als digitales Dokument erfassen zu können (in mindestens einem Dateiformat; ungeachtet dessen Tauglichkeit für semantische Integration).

[NSWL11, NWL12, NHL12, NL12]). Das System ist implementiert und evaluiert. Sowohl der Ansatz als auch weitere technische Details sind in meiner Dissertation beschrieben [Neu12]. Im Vergleich zu den gerade genannten Publikationen ist der Beitrag dieser Veröffentlichung eine Zusammenfassung meiner Arbeit.

1.2 Benutzerszene: Erzählung einer hypothetische Kooperation

Zur Veranschaulichung der Vision für verteilte organisationsübergreifende Fallführung beschreibt dieser Abschnitt eine Benutzerszene aus einem hypothetischen Brustkrebs-Szenario. Die Erzählung ist stilistisch in Analogie zu Bergers Studie [Ber97] geschrieben. Die Benutzerszene wurde von mir ursprünglich in [NL12] publiziert.

„ ... Die Patientin ist im Begriff den Behandlungsraum des Gynäkologen zu verlassen. Erst gestern hat sie einen Knoten in ihrer Brust ertastet. Der Gynäkologe hat soeben eine Sonographie beendet, derzufolge das Knotengewebe auffällig erscheint und weiterer Klärung bedarf. Er grübelt über den typischen weiteren Behandlungsverlauf: Zunächst wird er sie zu einem Radiologen schicken, für eine Mammographie. Bestätigt die Röntgenuntersuchung den Verdacht auf Krebs, muss die Patientin zu einem Kollegen am örtlichen Krankenhaus, für eine Biopsie. Dann könnte es zur Primärtherapie kommen, durch welche das betroffene Gewebe operativ entfernt wird. Vermutlich werden in Kürze ein halbes Duzend Ärzte mit der Patientin beschäftigt sein und die bevorstehende Überweisung zum Radiologen ist tatsächlich der Beginn einer komplexen Zusammenarbeit, um das Leben seiner Patientin zu retten.

Der Arzt sitzt vor seinem Computerbildschirm und hat einen Überweisungsschein erstellt. Statt die Datei auszudrucken zieht er sie einfach per Drag'n'Drop auf ein spezielles Icon auf seinem Desktop. Dadurch wird die Überweisung in eine Fallaktendatei überführt. Seine Kollegen werden einfach Teilnehmer am Fall indem sie eine Kopie der Fallaktendatei zugestellt bekommen. Die Fallaktendatei ist ein aktives Dokument: Änderungen an einem Replikat werden automatisch mit allen anderen verteilten Replikaten synchronisiert. Die verteilte Fallakte lässt emergente Teilnehmer-Komplexität zu. Die Fallakte beinhaltet den Überweisungsschein als erste Informationseinheit. Außerdem erfasst die Akte bereits die elektronische Rücksendeadresse des Gynäkologen. Der Arzt speichert eine Kopie der Fallakte auf die Chipkarte seiner Patientin.

... Am Empfang des Radiologen öffnet die Arzthelferin die Fallakte ohne besondere Software-Installation. Das Doppelklicken der Fallakte startet den eingebetteten Editor, in welchem die Arzthelferin den enthaltenen Überweisungsschein in ihrem lokalen System öffnen kann. Im Rahmen der Patientenaufnahme speichert die Arzthelferin die Fallaktendatei als Anhang im lokalen Patientenverwaltungssystem, damit ihr Chef nach der Untersuchung darauf Zugriff hat.

... Der Radiologe ist mit der Mammographie fertig. Normalerweise würde er einen Arztbrief per Post an den Gynäkologen schicken. Stattdessen öffnet er die Fallaktendatei. Per Drag'n'Drop zieht er seinen Arztbrief in den Bereich des eingebetteten Editors. Weil die Fallakte die elektronische Adresse aller beteiligten Ärzte kennt, kann das aktive Dokument den neuen Befund an die elektronische Post-Box des Gynäkologen schicken. Der Radiologe mag diese Form der Fallakte, denn das aktive Dokument hält Kontextinformation der Kollaboration bereit und macht die Zusammenarbeit einfach.

... Die Patientin kehrt in die Praxis des Gynäkologen zurück und er öffnet seine Kopie der Fallakte. Die Fallakte synchronisiert automatisch ihren Inhalt mit der elektronischen Post-Box des Gynäkologen. Der radiologische Befund erscheint als neueste Informationseinheit. Er öffnet den Arztbrief und liest, dass der Wert des Indikators BI-RADS höher ist als vier. Das bedeutet, dass er seine Patientin ans örtliche Krankenhaus zur Biopsie schicken muss und er bereitet einen weiteren Überweisungsschein vor, den er wieder der Fallakte hinzufügt.

Erneut kopiert er die aktuelle Fallaktendatei auf die Chip-Karte seiner Patientin. Das Krankenhaus wird den OP-Bericht der Biopsie beisteuern. Die Gewebeprobe und die Fallakte werden zu einem Pathologen geschickt. Er wird den Histologiebericht zur Fallakte hinzufügen. Die Fallaktendatei des Gynäkologen wird stets jede Informationseinheit empfangen, die durch andere Teilnehmer in Zukunft beigesteuert wird.

Der Gynäkologe schaut seiner Patientin in die Augen. Er beruhigt sie, denn es gibt noch die Hoffnung, dass die Gewebeuntersuchung zeigt, dass es sich nur um eine benigne (gutartige) Neoplasie handelt. ...“

2 Methoden und wissenschaftlicher Beitrag

Die Benutzerszene beinhaltet verschiedene Arten der Mensch-Maschine-Interaktion. Zu Beginn findet eine Transformation des ersten Überweisungsscheins in ein aktives Dokument (α-*Doc*) für verteilte Fallführung statt. Abbildung 1 veranschaulicht die Fallaktendatei-Erstellung und die späteren Änderungen an der verteilten Fallakte. Die Abbildung skizziert die Benutzerszene aus einer technischeren Perspektive. Wir gehen der Einfachheit halber davon aus, dass der Überweisungsschein im prominenten Dateiformat HL7 CDA vorliegt; dies ist in der Abbildung durch den Kreis mit der Aufschrift „XML“ angedeutet. Im Wesentlichen spielt das Dateiformat für das Hinzufügen und die interne Verwaltung keine Rolle. Die vier großen rechteckigen Formen, die mit “α-*Doc*” gekennzeichnet sind, veranschaulichen das aktive Dokument in verschiedenen Inhaltszuständen an unterschiedlichen Zeitpunkten an den zwei beispielhaft beteiligen Orten.

2.1 Merkmale von aktiven Dokumenten

Der initiale Überweisungsschein ist eine eigenständige Datei. Die Überweisung und der Mammographiebericht werden zu Inhaltseinheiten als Teil der Fallakte. Die Fallakte ist ein aktives Dokument und damit ebenfalls eine Datei, die intern „molekular“ strukturiert ist. Ärzte können es sich so vorstellen, dass es sich im Wesentlichen um ein (selbst-ausführbares) ZIP-Archiv handelt. Genauer gesagt erlaubt die plattformneutrale Programmiersprache Java ausführbare ZIP-Dateien in Form von JAR-Dateien.

Die bildliche Vereinnahmung des mit „XML“ gekennzeichneten Kreises in das aktive Dokument ist im wahrsten Sinn gemeint. Die Kreise als Inhaltseinheit innerhalb des α-*Doc* werden von kleinen Rechtecken begleitet; dabei handelt es sich um Deskriptoren als eigene Dateien. Die Deskriptoren erlauben letztlich die Speicherung beliebiger Prozess-relevanter Metadaten zur jeweiligen Inhaltseinheit. Einfache Beispiele sind der Name der Inhaltseinheit sowie eine generierte ID desjenigen Prozessteilnehmers, der die Inhaltseinheit beigesteuert hat. Die Inhaltseinheit und ihr Deskriptor sind dann mit einem

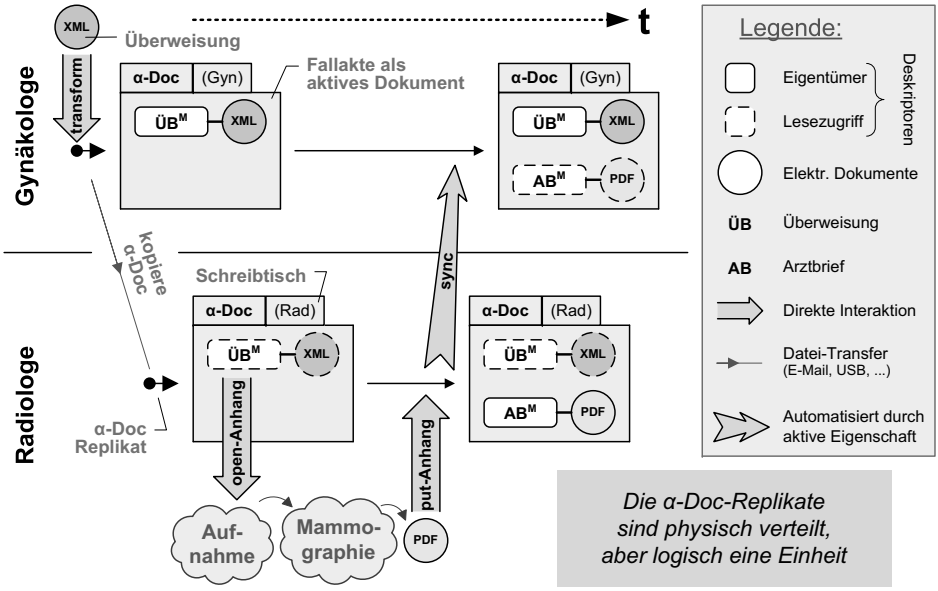


Abbildung 1: Ein α-*Doc*, das sich entsprechend der Benutzerszene verändert.

gestrichelten Rahmen versehen, wenn die Inhaltseinheit nicht durch den lokalen Benutzer beigesteuert wurde und somit der aktuelle Benutzer nicht der verantwortliche Autor ist.

Die Benutzerszene beschreibt, dass das aktive Dokument auf einer Chip-Karte gespeichert werden kann. Ebenfalls möglich sind USB-Sticks oder jegliches Speichermedium, das Dateien erlaubt. Von einer Dateisystem-Perspektive ist das molekulare, aktive Dokument eine einfache transportierbare Datei und es ist möglich beliebige Kopier- oder Verschiebe-Operationen anzuwenden oder sie als E-Mail-Anhang zu verschicken oder sie als Dateianhang in einem Patientenverwaltungssystem zu speichern. Dieses Merkmal wird durch den „kopiere α-*Doc*“-Pfeil in Abbildung 1 symbolisiert. Dadurch wird das α-*Doc* als Datei repliziert.

Auf der Seite des Radiologen kann das α-*Doc* ausgeführt werden und ein eingebetteter Editor listet die enthaltenen Inhaltseinheiten auf. Der Editor ermöglicht es, die einzelnen Inhaltsdateien genauso leicht zu öffnen wie eine E-Mail-Anwendung einen Dateianhang, das heißt sie werden mittels einer lokal verfügbaren Anwendung geöffnet. Jeder Teilnehmer kann weitere Inhaltseinheiten beisteuern, zum Beispiel den mit „PDF“ gekennzeichneten Kreis, stellvertretend für den Mammographiebericht, mittels einfachem Drag’n’Drop.

Nachdem ein neuer Beitrag lokal eingefügt wurde, müssen alle anderen bekannten Teilnehmer mit einer Kopie der Inhaltseinheit aktualisiert werden. Dies wird durch den speziell geformten „sync“-Pfeil dargestellt. Jeder Beitrag muss mit allen anderen α-*Doc*-Replikaten desselben Falles synchronisiert werden. Hervorzuheben ist, dass ein α-*Doc* nur dann aktiv ist, wenn es bewusst durch den Benutzer ausgeführt wird. Deswegen sind die verteilten Replikate nicht (notwendigerweise) zum selben Zeitpunkt online; stattdessen herrscht eine Offline-Charakteristik der Netzwerkknoten vor. Daher bedingt der Synchronisationsmechanismus eine zugrundeliegende „store-and-forward“-

Nachrichteninfrastruktur. Ein eigenes Synchronisationsprotokoll wurde speziell für diese Rahmenbedingungen entwickelt.

Die Benutzerszene konzentriert sich auf die operative Einbettung, also die Art und Weise wie sich eine α-*Doc*-Fallakte in die medizinischen Routineabläufe der Ärzte integrieren soll. Sie betont dadurch naturgemäß vor allem die Anforderungen an ein aktives Dokument. Verwandte Ansätze in diesem Bereich sind selten; Ansätze aus verschiedenen Informatikgebieten mit konzeptionellen Ähnlichkeiten zu aktiven Dokumenten werden in [Neu12] vergleichend gegenübergestellt. Als System für plattformneutrale und institutionsübergreifende aktive Dokumente ist das α-*Flow*-System einzigartig. Ein komplementärer Aspekt zu aktiven Dokumenten ist die prozessbezogene Perspektive, also welche Form der Prozessunterstützung durch ein α-*Doc* als eingebettete Anwendung für den Benutzer bereitgestellt werden kann.

2.2 Merkmale der Prozessunterstützung

Den Begriff „Prozess“ kann man definieren als „organizational form that encapsulates the interdependence of tasks, roles, people, departments, and functions“ [BAN03]. Darüber hinaus werden verschieden Unterklassifizierungen vorgenommen. Beispielsweise unterscheiden Medina-Mora et al. Materialprozesse, Informationsprozesse und Geschäftsprozesse (vgl. [MMWFF92]). McCready unterscheidet drei Typen von Arbeitsabläufen [McC92]: ad-hoc Abläufe, administrative Abläufe und Produktionsabläufe. Georgakopoulos et al. verwenden eine Klassifikation, welche systemorientierte Abläufe und menschorientierte Abläufe gegenüberstellt. Ferner können drei Stufen der Prozesskonzeption unterschieden werden: semiformelle Prozessbeschreibung, formelle Workflow-Spezifikation und ausführbare Workflow-Automatisierung (vgl. [GHS95]).

Die namenhafte Workflow Management Coalition (WfMC) stellt ein Begriffsglossar bereit. Leider deckt diese terminologische Referenz den Prozess-Begriff nicht im weitesten Sinn ab, stattdessen betrachtet die WfMC ausschließlich „*Geschäftsprozesse*“ und fasst den Workflow-Begriff als den automatisierbaren Teil eines Geschäftsprozesses auf. Damit ist die wortgetreue und automatisierungszentrische WfMC-Definition zu restriktiv im Gesamtkontext des breiten Feldes der Prozessunterstützung. Rusinkiewicz und Sheth liefern in [RS94] eine allgemeinere Definition: „*Workflows* are activities involving the coordinated execution of multiple tasks performed by different processing entities. A *task* defines some work to be done and can be specified in a number of ways, including a textual description in a file or an email, a form, a message, or a computer program. A *processing entity* that performs the tasks may be a person or a software system“.

Zusammenfassend betrachtet ist die Trennschärfe zwischen den Begriffen „Prozessunterstützung“ (im weitesten Sinn) und „Workflow-Management“ (im engsten Sinn) nicht sonderlich hoch. Mein dDPM-Ansatz befasst sich mit menschorientierten, wissensgetriebenen, Ad-hoc-Informationsprozessen. Die durch dDPM bereitgestellte Prozessunterstützung besteht aus folgenden grundlegenden Aspekten:

- Erfassen der *Prozessteilnehmer* (Wer?) an unterschiedlichen *Institutionen* (Wo?)
- Erfassen der *Arbeitseinheiten* als Prozessschritte (Was?)
- Erfassen der Prozessplanung in Form einer priorisierten *Arbeitsliste* ($\sim$ Wann?) und Ergänzen von Prozessschritten auf bedarfsorientierte Weise

- Unterstützen einer Konsensfindung hinsichtlich einer verteilten Prozessplanung durch Synchronisation der Arbeitsliste zwischen räumlich getrennten Standorten
- Verteilen der Ergebnisse der Arbeitsschritte ohne notwendigerweise die Semantik der Inhaltseinheiten zu kennen
- Erfassen von prozessbezogenen Statusattributen jeder Arbeitseinheit
- Verwalten der Prozesshistorie durch Versionierung der Arbeitsliste und Arbeitseinheiten sowie der Ergebnisdokumente
- Exportieren und Importieren von Arbeitslisten als Prozessschablonen
- Ergänzen von Prozessteilnehmern auf bedarfsorientierte Weise

Prozessunterstützung wird also insbesondere durch eine gemeinsame Arbeitsliste bereitgesellt, die den Ablauf im Sinn von Was/Wann/Wo/Wer artikuliert. Zur Unterstützung der Prozessausführung dient das Routing bzw. die Synchronisation der Dokumentartefakte.

2.3 Dokumentenorientierte Arbeitsliste: Karten und Kennzeichnungen

Als dokumentenorientierte Form der Prozessplanung übernimmt dDPM das Prinzip „Karten-repräsentieren-Aufgaben“ aus dem Bereich agiler Softwareentwicklung. Methoden wie Kanban und Scrum benutzen einen Satz aus Karten um die Arbeitsliste eines Teams zu verwalten. Im Fall von Scrum werden beispielsweise notwendige Systemanpassungen auf *Task-Karten* geschrieben. Im Verlauf einer Scrum-Entwicklungsepisode (auch „Sprint“ genannt) ändern Task-Karten ihren Prozessstatus von „offen“ nach „in_Bearbeitung“ und schließlich nach „abgeschlossen“.

Es ist entscheidend, dass diverse prozessbezogene Attribute einer Scrum-Karte möglich sind, welche als Adornments bezeichnet werden können. Adornments[2] sind textuelle oder graphische Kennzeichnungen. Beispiele für Scrum-Adornments sind einmalig fixierte numerische Werte als Aufwandsschätzung für jede Karte sowie dynamisch zugewiesene Marker zur Kennzeichnung des verantwortlichen Entwicklers bzw. Prozessbeteiligten. Letztlich sind mehrere Scrum-Eigenschaften Vorbild für das α-*Flow* Metamodell: (1) Aufgaben durch Karten zu repräsentieren, (2) Prozessfortschritt durch wechselnden Kartenstatus zu erfassen und (3) Kartenstatus durch Adornments zu kennzeichnen.

Agile Prozessplanung wurde bislang erfolgreich in der nebenläufigen Produktentwicklung und Produktionsplanung sowie in der Softwaretechnik angewendet. In [Neu12] wird detaillierter ausgeführt wie die Prozesscharakteristiken gut mit denjenigen zusammenpassen, die man im diagnostisch-therapeutischen Zyklus (empirische Prozesse; stilles Wissen) und in medizinischen Leitlinien (nicht-linear; mehrere mögliche Lösungen) beobachten kann. Dennoch bedeutet diese Scrum-Analogie nicht, dass wir von Ärzten erwarten, dass sie der Scrum-Philosophie folgen. Stattdessen passt diese Art der Ablaufrepräsentation durch Karten gut zu dem von Lawrence Weed erfundenen Problem-Oriented Medical Record (POMR), einem System zur klinischen Dokumentation. Solche POMR-basierten Systeme verwenden ein SOAP[3]-strukturiertes, kartenbasiertes Aufzeichnungsmodell (vgl.

[2] Der Begriff „Adornment“ wird ebenfalls im Rahmen der Unified Modeling Language (UML) benutzt: ein UML-Adornment fügt demjenigen Element zu dem es gehört weitere Bedeutung oder Semantik hinzu, es hat sowohl eine textuelle als auch graphische Repräsentation; prominente Beispiele für UML-Adornments sind die diamantgeformten Indikatoren für Komposition oder Aggregation.

[3] SOAP im Kontext von POMR ist eine Abkürzung für „subjective, objective, assessment, plan“.

[Wee68]). Die Kanban- und Scrum-Analogie erweitert das POMR-Konzept um die Ablaufplanung, indem noch unvollständig ausgefüllte Karten für geplante Behandlungsschritte erzeugt werden, die man als Platzhalter für zukünftige POMR-Dokumentationen verstehen kann. Der Therapieplan kann dabei durch Repriorisierungen oder durch Hinzufügen bzw. Löschen von Karten umgestaltet werden.

Was die Prozessformalisierung angeht, wurde die Idee der „*inhaltsorientierten Ablaufmodelle*“ übernommen. Dabei wird der Prozessfortschritt durch die Anwesenheit von Inhaltseinheiten ausgedrückt sowie durch Bedingungen auf einem inhaltlichen Zustand der Daten. Derzeit vertreten folgende wissenschaftliche Ansätze dieses Prinzip: „data-driven“/COREPRO, „resource-driven“, „artifact-centric“/ArtiFact™ sowie „object-aware“/PHILharmonicFlows. Eine weitere Idee, die von dDPM übernommen wurde, ist die elektronische Durchlaufakte, wie beispielsweise ProMInanD und POLITeam aus den 90ern. Durchlaufakten verkörpern Ad-hoc-Abläufe, durch dynamisches Umleiten von Dokumenten zwischen Prozessteilnehmern. In Analogie zu elektronischen Durchlaufakten ist eine zentrale Grundannahme von dDPM, dass Prozessschritte durch Karten ausgedrückt sowie durch Bereitstellen eines Ergebnisberichts erledigt werden können. Die Karten sind also planbare Teilabschnitte der Akte, welche sukzessive durch verschiedene Teilnehmer ausgefüllt werden. In [Neu12] wird der Zusammenhang zwischen Fortschreiten des Kartenstatus und Erledigung von Arbeitseinheit umfassend erörtert.

3 Ergebnisse und Zusammenfassung

Insgesamt kombiniert dDPM (1) das inhaltsorientierte Ablauf-Paradigma mit (2) den dokumentenorientierten Aspekten einer Durchlaufakte und (3) agiler Prozessplanung. In dieser Kombination ermöglicht dDPM eine dokumentenorientierte Fallführung. Das Prozessmodell basiert auf einer eingehenden Prozessanalyse der Brustkrebsbehandlung, wobei diese auf persönlichen Interviews mit akkreditierten Gynäkologen aus dem Umfeld des Brustkrebszentrums Amberg basiert. Dabei werden dreiundzwanzig Elemente eines Prozessmodells für verteilte Fallführung identifiziert und beschrieben. Diese bilden sowohl die Referenz für die prototypische Implementierung als auch ein Rahmenwerk um verwandte Arbeiten in einer vergleichenden Evaluation bewerten zu können. Das resultierende Prozessmodell enthält dabei keine Elemente oder Annahmen, die unmittelbar auf das Gesundheitswesen eingeschränkt sind, wenngleich der Ansatz hauptsächlich in diesem Kontext diskutiert wird.

Aus Anwendersicht stell jedes α-*Doc* eine eingebettete Anwendung für verteilte Fallführung zur Verfügung und dies bedeutet den Zusammenschluss von (1) gruppenbasiertem E-Mail mit einem (2) gemeinsamen Arbeitslisten-Editor und einem (3) Versionsverwaltungssystem. Um eine Microsoft-Produktmetapher zu verwenden könnte man sagen, bei einem α-*Doc* handle es sich um ein autonomes verteiltes Mini-SharePoint. Bei jeglichem derartigen Vergleich sollte man berücksichtigen, dass Groupware-Produkte grundsätzlich vordefinierte Datenstrukturen verwenden, um Einträge für Aufgaben abzubilden; Im Gegensatz dazu beinhaltet α-*Flow* ein zur Laufzeit durch den Nutzer anpassbares Attributmodell für Inhaltseinheiten (vgl. [NSWL11]).

Ein α-*Doc* beinhaltet im Kern eine regelbasierte Inferenzmaschine („rule engine“), die Statusübergänge überwacht und Aktionen auslöst. Zurzeit werden u. a. vorgefertigte Regeln für die Versionierung (vgl. [NWL12]) und die verteilte Synchronisation (vgl.

[NHL12]) unterstützt. Der Workflow-bezogene Nutzen ist die Prozessplanung, Teilnehmerverwaltung, Prozesshistorien-Erfassung und Prozessschablonen-Erstellung.

Das α-*Flow*-Modell ist in [Neu12] formalisiert; es repräsentiert alle im α-*Doc* enthaltenen Inhaltseinheiten als mathematische Faktenmenge. Dies erlaubt die Anwendung der Inferenzmaschine für Anfragen bzw. Auslösung regelbasierter Aktionen. Die Implementierung umfasst über 100.000 Zeilen Code, die auf elf Hauptmodule aufgeteilt sind. Eine technische Evaluierung hat stattgefunden; in [Neu12] werden Code-Metriken analyisiert und die Leistung der eingebetteten Versionsverwaltung mit Subversion und git verglichen.

Eine konzeptionelle Evaluierung erfolgte durch einen Vergleich mit inhaltsorientierten Workflow-Ansätzen sowie mit Ansätzen aus dem Umfeld aktiver Dokumente. Zusätzlich wurden drei weitere Ansätze identifiziert, die kombinierte Merkmale mit α-*Flow* teilen. Die Anforderungen an das Prozessmodell aus der Analysephase wurden zum Zweck der Evaluation wiederverwendet. Derzeit gibt es keinen vergleichbaren Ansatz und kein System, das in der Lage ist institutionsübergreifende Ad-hoc-Prozesse hinreichend zu unterstützen. Derzeit ist α-*Flow* der einzige Ansatz, der eine ausreichend allgemeine und gleichzeitig praktikable Lösung für verteilte Fallakten bereitstellt, über regionale Grenzen hinweg, ohne vorangegangene Systemintegration.

Nachdem die funktionale Machbarkeit eines solchen Systems durch meine Arbeit demonstriert wurde, ergeben sich weiterführende Forschungsfragen. Ungelöste Aufgaben betreffen (1) die Datensicherheit des Replikattransports und der lokalen Speicherung, (2) Möglichkeiten zur Rekonfiguration des Verhaltens der aktiven Dokumente zur Laufzeit und (3) die Ausführungssicherheit und Zugangskontrolle für aktive Dokumente sowie (4) Workflow-Mechanismen für die Teamarbeit zwischen Ärzten und Pflegepersonal.

Literatur

[BAN03] J. Becker, L. Algermissen, and B. Niehaves. Processes in e-government focus: a procedure model for process oriented reorganisation in public administrations on the local level. *Electronic Government*, pages 1062–1062, 2003.

[Ber97] Roland Berger. Telematik im Gesundheitswesen – Perspektiven der Telemedizin in Deutschland. *Studie im Auftrag des Bundesministeriums für Bildung, Wissenschaft, Forschung und Technologie in Zusammenarbeit mit dem Bundesministerium für Gesundheit, München*, 1997.

[DEL+00] P. Dourish, W. K. Edwards, A. LaMarca, J. Lamping, K. Petersen, M. Salisbury, D. B. Terry, and J. Thornton. Extending document management systems with user-specific active properties. *ACM Transactions on Information Systems (TOIS)*, 18(2):140–170, 2000.

[DMC+10] P. R. Dexter, D. K. Miller, D. O. Clark, M. Weiner, L. E. Harris, L. Livin, I. Myers, D. Shaw, L. A. Blue, J. Kunzer, et al. Preparing for an Aging Population and Improving Chronic Disease Management. In *Proc of the AMIA Annual Symposium*, volume 2010, page 162. American Medical Informatics Association, 2010.

[GHS95] D. Georgakopoulos, M. Hornick, and A. Sheth. An overview of workflow management: From process modeling to workflow automation infrastructure. *Distributed and parallel Databases*, 3(2):119–153, 1995.

[Len09] R. Lenz. Information Systems in Healthcare – State and Steps towards Sustainability. *IMIA Yearbook 2009 – Yearbook of Medical Informatics as a supplement of Methods of Information in Medicine*, pages 63–70, 2009.

[McC92] S. McCready. There is more than one kind of workflow software. *Computerworld*, 2:86–90, 1992.

[MMWFF92] R. Medina-Mora, T. Winograd, R. Flores, and F. Flores. The action workflow approach to workflow management technology. In *Proc of the 1992 ACM conference on Computer-supported cooperative work*, pages 281–288. ACM, 1992.

[Neu12] Christoph P. Neumann. Distributed Document-Oriented Process Management in Healthcare. Dissertation, Friedrich-Alexander-Universität Erlangen-Nürnberg, November 2012.

[NHL12] Christoph P. Neumann, Scott A. Hady, and Richard Lenz. Hydra Version Control System. In *Proc of the 10th IEEE Int'l Symposium on Parallel and Distributed Processing with Applications (ISPA-12)*, Madrid, Spain, July 2012.

[NL12] Christoph P. Neumann and Richard Lenz. The alpha-Flow Approach to Inter-Institutional Process Support in Healthcare. *International Journal of Knowledge-Based Organizations (IJKBO)*, 2(4):52–68, 2012.

[NSWL11] Christoph P. Neumann, Peter K. Schwab, Andreas M. Wahl, and Richard Lenz. alpha-Adaptive: Evolutionary Workflow Metadata in Distributed Document-Oriented Process Management. In *Proc of the 4th Int'l Workshop on Process-oriented Information Systems in Healthcare (ProHealth'11)*, Clermont-Ferrand, FR, August 2011.

[NWL12] Christoph P. Neumann, Andreas M. Wahl, and Richard Lenz. Adaptive Version Clocks and the OffSync Protocol. In *Proc of the 10th IEEE Int'l Symposium on Parallel and Distributed Processing with Applications (ISPA-12)*, Madrid, Spain, July 2012.

[RS94] M. Rusinkiewicz and A. Sheth. Specification and execution of transactional workflows. In Won Kim, editor, *Modern Database Systems: The Object Model, Interoperability, and Beyond*, pages 592–620. Addison-Wesley, 1994.

[TOG10] K. E. Thorpe, L. L. Ogden, and K. Galactionova. Chronic conditions account for rise in Medicare spending from 1987 to 2006. *Health Affairs*, 29(4):718, 2010.

[Wee68] Lawrence L. Weed. Medical records that guide and teach. *New England Journal of Medicine*, 278(12):652–657, 1968.



Christoph P. Neumann, geboren am 4. Mai 1980 in Emmendingen, erwarb sein Diplom im Studiengang Informatik an der Friedrich-Alexander-Universität Erlangen-Nürnberg im Juni 2005 mit Auszeichnung. Dann arbeitete er für zwei Jahre als Software-Ingenieur bei der Capgemini sd&m AG in München. Im Anschluss war er wissenschaftlicher Mitarbeiter von Prof. Dr. Richard Lenz an der Friedrich-Alexander-Universität. Dort unterrichtete er Übungsveranstaltungen und Vorlesungen und erhielt zwei Auszeichnungen für herausragende Lehre. Im November 2012 promovierte er in der Informatik mit Auszeichnung. Seine Forschungsinteressen beinhalten datengetriebene Prozesse, verteilte Datenverwaltung, Systemintegration und adaptiv-evolutionäre Informationssysteme.

Effiziente Systemevaluation mit stochastischen Modellen*

Philipp Reinecke

Hewlett-Packard Laboratories, Bristol, UK
und
Freie Universität Berlin
philipp.reinecke@{hp.com, fu-berlin.de}

Abstract: Stochastische Modelle werden zur Evaluation von Computersystemen benötigt. Diese Arbeit betrachtet Fragen der Effizienz von Evaluationsansätzen unter besonderer Berücksichtigung stochastischer Fehlermodelle. Sie bietet einen Überblick über stochastische Fehlermodelle und wendet sich anschließend dem effizienten Einsatz von Phasentypverteilungen zu. Es werden Methoden zur effizienten Zufallszahlengenerierung in Simulationen entwickelt und eine Aussage zur optimalen Repräsentation hergeleitet. Des weiteren wird ein neuer Algorithmus für die Anpassung von Phasentypverteilungen an Daten und seine Implementierung im Werkzeug HyperStar vorgestellt. Drei Fallstudien illustrieren den Einsatz stochastischer Modelle an Beispielen aus der Praxis.

Einleitung

In der modellbasierten Untersuchung und Bewertung der Leistungsfähigkeit, Zuverlässigkeit und Sicherheit von Computersystemen werden relevante Maße des zu untersuchenden Systems anhand eines Systemmodells dieses Systems bestimmt. Bei den Untersuchungsmethoden unterscheidet man drei Abstraktionsstufen: In *Testbetten* wird das System realitätsnah implementiert und mit Mechanismen zur Lasterzeugung und zur Erfassung von Meßwerten ausgestattet. Derartige experimentelle Studien liefern sehr realistische Ergebnisse, sind jedoch zeitaufwendig und teuer. Die Ergebnisse sind oft spezifisch für den jeweiligen Aufbau und schwer verallgemeinerbar. In *Simulationen* wird das System in seiner relevanten Struktur und seinem Verhalten nachgebildet. Gegenüber Testbetten bieten Simulationen den Vorteil geringeren Aufwandes und, aufgrund der größeren Abstraktion, allgemeinerer Aussagen. Allerdings sind Simulationen oft ebenfalls zeitaufwendig und erfassen nicht alle Merkmale der Realität. *Analytische Ansätze* schließlich nutzen ein mathematisches Modell des Systems. Analytische Modelle liefern allgemeingültige Aussagen und können oft effizient gelöst werden; aufgrund der hohen Abstraktionsstufe können jedoch unrealistische Annahmen die Ergebnisse verfälschen. Im Idealfall werden bei der Beantwortung einer Fragestellung alle drei Abstraktionsstufen kombiniert, so daß sinnvolle und allgemeingültige Ergebnisse erzielt werden.

*Englischer Titel der Dissertation: „Efficient System Evaluation Using Stochastic Models“.

Modelle zur Systemevaluation müssen neben dem funktionalen Verhalten des Systems auch Fehler, die das Systemverhalten beeinflussen, widerspiegeln. Hierbei bietet sich die Unterteilung in das *Systemmodell*, das die funktionalen Eigenschaften des Systems abbildet, und *Fehlermodellen*, die Störungen des Systems aufgrund von Fehlern in Komponenten beschreiben, an. Stochastische Fehlermodelle sind besonders geeignet, um das oft unvorhersagbare Verhalten von Fehlern zu erfassen. Fehlermodelle dienen also als Parameter für das Systemmodell, die es erlauben, den Einfluß solcher Störungen auf das reale System nachzubilden. Durch die Wahl verschiedener Fehlermodelle kann das System unter unterschiedlichen Bedingungen untersucht werden.

Gute Modelle müssen realistisch sein und effiziente Evaluierungsverfahren ermöglichen. Aus diesen Anforderungen ergeben sich grundlegende Fragestellungen dieser Arbeit: Welche Fehlermodelle sind geeignet für die Evaluation? Wie können Modelle effizient eingesetzt werden? Wie können Modelle aus Beobachtungen gewonnen werden? Der erste Teil der Arbeit schafft einen Überblick über stochastische Fehlermodelle in der Literatur. Im zweiten Teil wird speziell auf Phasentypverteilungen eingegangen. Der effiziente Einsatz von Phasentypverteilungen in Simulationen wird ebenso untersucht wie die Anpassung von Phasentypverteilungen an Meßwerte. Im dritten Teil wird der Einsatz stochastischer Modelle anhand von Beispielen aus der Praxis illustriert.

1 Stochastische Fehlermodelle in der Literatur

Fehlermodelle dienen in der Systemevaluation zur Wiedergabe des Verhaltens von Subsystemen unter dem Einfluß typischer Fehler. Hierzu sind oft umfangreiche Messungen an realen Systemen nötig, die der eigentlichen Modellierungsarbeit vorausgehen und diese erschweren können. Es wird daher zunächst ein Überblick über in der Literatur vorhandene Fehlermodelle gegeben. Der Überblick ist so angelegt, daß, ausgehend von einer Klassifikation von Fehlern, schnell geeignete Modelle ausgewählt werden können. Sämtliche erfaßten Modelle beruhen auf Messungen, so daß die Fehlermodelle zu einem realitätsnahen Verhalten des Modells führen.

Die erfaßten Fehlermodelle werden zunächst nach der Art des Modells unterschieden: Bernoulli-Modelle geben lediglich die Eintrittswahrscheinlichkeit des Fehlers, beispielsweise eines Paketverlustes, wieder. Allgemeinere Zufallsvariablen beschreiben den Fehler durch eine Verteilung, wie zum Beispiel die Verteilung von Verzögerungen bei der Paketübertragung. Stochastische Prozesse im allgemeinen schließlich erfassen weitere Aspekte des Fehlers. Sie können beispielsweise abwechselnde Perioden von Paketverlusten und -übertragungen mit einer zeitkontinuierlichen Markovkette modellieren. Die Fehlermodelle werden zusätzlich nach der Ebene, auf der das modellierte Subsystem angesiedelt ist, gegliedert. Dies führt zu einem rekursiven Ansatz, der sowohl der Auswahl der Modelle in der Übersicht als auch der Entscheidung für ein Modell in der Anwendung dient: Ausgehend von einer abstrakten Sicht auf das System kann dieses solange weiter in seine Subsysteme zerlegt werden, bis geeignete Fehlermodelle vorliegen.

Als Anwendungsbeispiel dient der *SUN Java Adventure Builder* [Sun06], eine Referenz-

implementierung für Service-Orientierte Systeme (SOA-Systeme). Diese Anwendung illustriert die typische Architektur eines SOA-Systems mit einem Nutzer, der über eine Web-Schnittstelle Dienste unterschiedlicher Anbieter nutzt. Da viele Komponenten dieses Systems allgemein Anwendung finden, ist weder die Suche nach geeigneten Modellen noch die Anwendbarkeit der Modelle auf spezielle Untersuchungen zum Thema SOA beschränkt.

Im ersten Schritt wird zunächst nur die Interaktion zwischen einem Nutzer und dem Adventure Builder als abgeschlossenem System betrachtet. Dies bedeutet, daß Fehlermodelle, die das Verhalten des Adventure Builder unter typischen Fehlern so erfassen, wie es sich aus der Sicht der Nutzers darstellen würde, gesucht werden. In den nächsten Schritten wird dann stetig verfeinert, indem Kommunikation und System und verschiedene Ebenen dieser beiden betrachtet werden. In jedem Schritt werden jeweils die existierenden Modelle zusammengefaßt und diskutiert.

Anschließend werden Fehlerklassifikationsschemata für SOA-Systeme aus der Literatur vorgestellt und zur Strukturierung der beschriebenen Fehlermodelle genutzt. Dies dient zum einen der Bewertung der Unterscheidungskraft der Taxonomien. Es zeigt sich, daß viele Kategorien nur sehr unscharf oder aber unzutreffend gewählt sind, da es bei der Klassifizierung oftmals zu Überschneidungen zwischen Kategorien kommt, während andererseits auch Kategorien leer bleiben. Zum anderen wird es durch diesen Schritt möglich, Fehlermodelle bei Bedarf aufgrund dieser Taxonomien auszuwählen.

Im Ergebnis des ersten Teils der Arbeit liegt ein umfangreicher Überblick über vorhandene Fehlermodelle vor, der für eine Vielzahl von Untersuchungen die schnelle Auswahl geeigneter Fehlermodelle zur Parametrisierung der Systemmodelle erheblich erleichtert. Des weiteren werden Bereiche identifiziert, die bislang nicht ausreichend durch stochastische Fehlermodelle abgedeckt werden.

2 Phasentypverteilungen

Im zweiten Teil konzentriert sich die Arbeit auf Phasentypverteilungen. Phasentypverteilungen werden in der stochastischen Modellierung vielfältig eingesetzt und insbesondere auch als Fehlermodelle verwendet. Phasentypverteilungen dienen der Modellierung von Phänomenen, die durch eine Verteilung gut beschrieben werden können, und zeichnen sich dadurch aus, daß sie bei sehr guter Modellqualität auf allen drei Abstraktionsebenen gleich gut eingesetzt werden können. Sie bieten damit die Möglichkeit, ein gemessenes Systemverhalten mit einem Modell zu erfassen und dieses Modell in der Analyse, Simulation und im Testbett einzusetzen und damit die Qualität der erzielten Aussagen zu verbessern.

2.1 Grundlagen

Phasentypverteilungen (PH-Verteilungen) sind definiert als die Verteilung der Zeit, die in einer zeitkontinuierlichen Markov-Kette (*Continuous-Time Markov Chain, CTMC*) mit

einem absorbierenden Zustand vom Eintritt in die Kette bis zum Erreichen des absorbierenden Zustandes vergeht [Neu81]. In der Klasse der allgemeinen PH-Verteilungen (PH) unterscheidet man als Unterklassen insbesondere die azyklischen Phasentypverteilungen (APH) und die Hyper-Erlang-Verteilungen (HErD). Azyklische Phasentypverteilungen werden durch zyklusfreie Markovketten definiert. Hyper-Erlang-Verteilungen als eine Unterklasse von APH sind Mischungen von Erlang-Verteilungen.

Jede Phasentypverteilung kann mit einem Tupel $(\boldsymbol{\alpha}, \mathbf{Q})$ aus einem Zeilenvektor $\boldsymbol{\alpha} \in \mathbb{R}^n$ und einer quadratischen Matrix $\mathbf{Q} \in \mathbb{R}^n$ beschrieben werden. Das Tupel $(\boldsymbol{\alpha}, \mathbf{Q})$ definiert die Dichtefunktion $f(t) = \boldsymbol{\alpha}\, \mathrm{e}^{\mathbf{Q}t}(-\mathbf{Q}\mathbb{1})$ sowie die Verteilungsfunktion $F(t) = 1 - \boldsymbol{\alpha}\, \mathrm{e}^{\mathbf{Q}t}\, \mathbb{1}$. Die Repräsentation $(\boldsymbol{\alpha}, \mathbf{Q})$ ist im allgemeinen nicht eindeutig, unterschiedliche Tupel können also die selbe Verteilung definieren. Insbesondere sind die Markovschen Repräsentationen von Bedeutung:

Definition 1 (Markovsche Repräsentation) *Das Tupel* $(\boldsymbol{\alpha}, \mathbf{Q})$ *mit*

$$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \quad \textit{und} \quad \mathbf{Q} = \begin{pmatrix} -\lambda_{11} & \lambda_{12} & \ldots & \lambda_{1n} \\ \lambda_{21} & \ddots & & \\ \vdots & & & \\ \lambda_{n1} & & \ldots & -\lambda_{nn} \end{pmatrix} \tag{1}$$

ist eine Markovsche Repräsentation *einer Phasentypverteilung der Größe* n *genau dann wenn*

$$\alpha_i \geq 0 \ \textit{für}\ i = 1, \ldots, n, \ \textit{und}\ \boldsymbol{\alpha}\mathbb{1} \leq 1 \tag{2}$$

$$\lambda_{ij} \geq 0 \ \textit{und}\ \lambda_{ii} > 0 \ \textit{für}\ i, j = 1, \ldots, n \tag{3}$$

$$\mathbf{Q}\mathbb{1} \geq_{el} \mathbf{0} \ \textit{und}\ \mathbf{Q}\mathbb{1} \neq \mathbf{0} \tag{4}$$

gilt. In diesem Fall beschreibt $\boldsymbol{\alpha}$ *den Initialisierungsvektor und* $\mathbf{Q}$ *die Subgeneratormatrix einer CTMC mit absorbierendem Zustand* $n + 1$.

Für die Klassen PH und APH existieren kanonische Formen, in die jede Verteilung aus der jeweiligen Klasse transformiert werden kann. Diese Repräsentationen zeichnen sich durch die einfache Struktur ihrer Generatormatrix aus. Es werden die monozyklische [MC99] und die CF-1-Form [Cum82] betrachtet. Die monozyklische Form ermöglicht eine kanonische Darstellung allgemeiner Phasentypverteilungen in einer blockdiagonalen Form, wobei die Blöcke jeweils eine einfache Struktur aufweisen und aufsteigend nach dem Betrag ihrer dominanten Eigenwerte sortiert sind [MC99]. Die CF-1-Form ist ein Spezialfall der monozyklischen Form für APH, bei der die Blöcke die Größe 1 haben, und nur die Haupt- und die obere Nebendiagonale besetzt sind. Jede allgemeine Phasentypverteilung hat eine Markovsche Repräsentation in monozyklischer Form [MC99]; ebenso besitzt jede azyklische Phasentypverteilung eine Markovsche Repräsentation in CF-1-Form [Cum82]. Die allgemeine Struktur der Markovketten der kanonischen Formen ist in Abbildung 1 dargestellt. Eine wichtige Eigenschaft dieser kanonischen Formen besteht darin, daß die

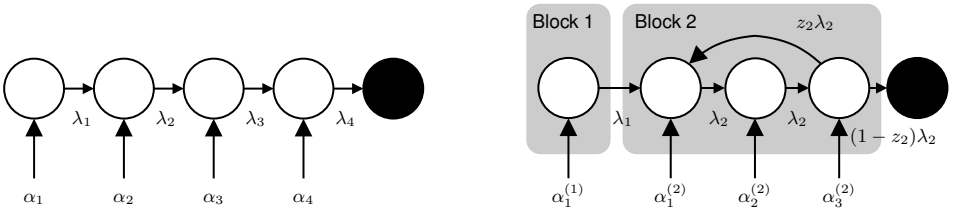


Abbildung 1: CF-1-Form (links) und monozyklische Form (rechts) im Vergleich.

Blöcke eine Kette bilden und der Wechsel in den absorbierenden Zustand nur vom letzten Block der Kette erfolgen kann.

Um die Umwandlung einer Repräsentation einer Phasentypverteilung in eine andere zu beschreiben, werden Ähnlichkeitstransformationen verwendet:

Definition 2 (Ähnlichkeitstransformation (vgl. [Ber09])) *Seien* $(\boldsymbol{\alpha}, \mathbf{Q})$ *und* $(\boldsymbol{\alpha}', \mathbf{Q}')$ *der Größe* n *zwei Repräsentationen der selben PH-Verteilung. Sei* $\mathbf{S} \in \mathbb{R}^{n \times n}$ *die Lösung des Systems* $\left\{\boldsymbol{\alpha}' = \boldsymbol{\alpha}\mathbf{S}, \mathbf{Q}' = \mathbf{S}^{-1}\mathbf{Q}\mathbf{S}, \mathbf{S}\mathbb{1} = \mathbb{1}\right\}$. *Dann ist* $\mathbf{S}$ *die* Ähnlichkeitstransformation *zwischen* $(\boldsymbol{\alpha}, \mathbf{Q})$ *und* $(\boldsymbol{\alpha}', \mathbf{Q}')$.

Insbesondere beschreiben Ähnlichkeitstransformationen, wie ein neuer Vektor $\boldsymbol{\alpha}'$ berechnet werden kann, wenn eine neue Matrix $\mathbf{Q}'$ konstruiert wurde.

2.2 Effiziente Erzeugung phasentypverteilter Zufallszahlen

Der Einsatz von Phasentypverteilungen in Simulationen und Testbetten erfordert die Erzeugung phasentypverteilter Zufallszahlen. Hierzu bietet die Literatur eine Reihe von Algorithmen. Der Fokus der Arbeit liegt auf Methoden, die die Markovkette vom Einstieg bis zur Absorption durchspielen. Es wird gezeigt, daß die Effizienz solcher Algorithmen von der Zahl der benötigten Berechnungen des Logarithmus und gleichverteilter Zufallszahlen auf $(0, 1)$ abhängt und daß auf aktuellen Systemen deutliche Unterschiede in den Kosten der Operationen existieren. Die Kosten für die Zufallszahlenerzeugung werden mittels dieser Operationen explizit hergeleitet.

Anschließend werden zwei neue Algorithmen zur Erzeugung von Zufallszahlen aus APH- und PH-Verteilungen entwickelt. Die Algorithmen nutzen die kanonischen Formen für die jeweilige Klasse. Sie bieten eine Reihe von Vorteilen: Durch Ausnutzung der die diagonalen Struktur der kanonischen Formen reduziert sich die Zahl der benötigten gleichverteilten Zufallszahlen und der zu berechnenden Logarithmen. Des weiteren ergeben sich aus der Struktur elegante Ausdrücke für die Kosten der Algorithmen, die die Grundlage von Optimierungsverfahren bilden. Überdies unterstützen die Algorithmen alle APH- beziehungsweise PH-Verteilungen, da jede Verteilung aus einer dieser Klassen in der jeweiligen kanonischen Form dargestellt werden kann.

Anhand der neuen Algorithmen wird nach einer für die effiziente Zufallszahlenerzeugung

optimalen Repräsentation von PH-Verteilungen gesucht. Unter Verwendung des neuen Algorithmus ist für eine APH-Verteilung der Größe n in CF-1-Form

$$n^* := \boldsymbol{\alpha}(n, n-1, \ldots, 1)^{\mathsf{T}} \tag{5}$$

die mittlere Zahl der besuchten Zustände. Die Ziehung einer Zufallszahl erfordert dann im Mittel $1 + n^*$ gleichverteilte Zufallszahlen und n^* Logarithmen. (5) zeigt, daß n^* von der initialen Verteilung der Zustandswahrscheinlichkeiten abhängt. Die Kosten können reduziert werden, wenn es gelingt, die Wahrscheinlichkeitsmasse innerhalb des Vektors $\boldsymbol{\alpha}$ nach rechts (hin zum absorbierenden Zustand) zu verschieben.

In der Generatormatrix für die CF-1-Form sind die Diagonale und die obere Nebendiagonale mit betragsgleichen Einträgen gefüllt und alle anderen Einträge gleich null. Aus dieser bi-diagonalen Struktur ergibt sich die Idee, die Kosten für verschiedene Anordnungen der Einträge zu betrachten. Die folgende Ähnlichkeitstransformation beschreibt die Vertauschung zweier zweier aufeinanderfolgender Einträge λ_i, λ_{i+1} $(i = 1, \ldots, n-1)$:

$$\mathbf{S} = \begin{pmatrix} \ddots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & s_{i+1,i} & s_{i+1,i+1} & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \ddots \end{pmatrix} \in \mathbb{R}^{n \times n}, \tag{6}$$

wobei

$$s_{i+1,i} = \frac{\lambda_i - \lambda_{i+1}}{\lambda_i} \quad \text{und} \quad s_{i+1,i+1} = \frac{\lambda_{i+1}}{\lambda_i}. \tag{7}$$

Wenn die Generatormatrix $\mathbf{Q}'$ aus $\mathbf{Q}$ durch Vertauschen des $i$ten und $(i+1)$ten Eintrages hervorgeht, dann ist $\boldsymbol{\alpha}' = \boldsymbol{\alpha}\mathbf{S}$ der neue Initialisierungsvektor. Da die Umordnung durch eine Ähnlichkeitstransformation erfolgt, repräsentiert $(\boldsymbol{\alpha}', \mathbf{Q}')$ die selbe Verteilung wie $(\boldsymbol{\alpha}, \mathbf{Q})$. Im allgemeinen gilt $\boldsymbol{\alpha}' \neq \boldsymbol{\alpha}$, $\boldsymbol{\alpha}'$ kann also andere Kosten $n^{*\prime} \neq n^*$ bedeuten. Da nach dem Satz von Steinhaus-Johnson-Trotter [Joh63] mittels wiederholter paarweiser Vertauschungen von Einträgen einer Liste jede beliebige Permutation erreicht wird, kann anhand dieser Operation die Entwicklung der Kosten für alle bi-diagonalen Repräsentation einer gegebenen PH-Verteilung untersucht werden.

Aus (6) und $\boldsymbol{\alpha}' = \boldsymbol{\alpha}\mathbf{S}$ folgt

$$n^*(\boldsymbol{\alpha}', \mathbf{Q}') = n^*(\boldsymbol{\alpha}, \mathbf{Q}) + \alpha_{i+1}\left(1 - \frac{\lambda_{i+1}}{\lambda_i}\right). \tag{8}$$

Dies bedeutet, daß die Kosten für die Zufallszahlenerzeugung reduziert werden können, wenn $\lambda_{i+1} > \lambda_i$ gilt. Durch wiederholte Anwendung ergibt sich

Satz 1 (Optimalität der umgekehrten CF-1-Form) *Sei $(\boldsymbol{\alpha}, \mathbf{Q})$ eine Markovsche Repräsentation in CF-1-Form. Dann ist die Repräsentation $(\boldsymbol{\alpha}^*, \mathbf{Q}^*)$, in der die Raten absteigend sortiert sind, optimal hinsichtlich der Kosten für die Zufallszahlenerzeugung,*

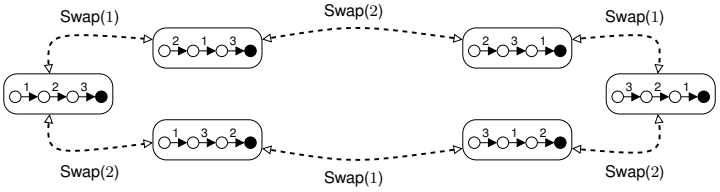


Abbildung 2: Beispiel für den Suchraum bei der Optimierung einer APH-Verteilung der Größe $n = 3$. Swap(i) bezeichnet die Vertauschung des $i$ten und $(i+1)$ten Elementes der Diagonale.

wenn alle Einträge von $\boldsymbol{\alpha}^*$ nicht-negativ sind. In diesem Falle sind alle bi-diagonalen Repräsentationen Markovsch.

Satz 1 beschreibt zum einen die optimale Repräsentation. Zum anderen folgt, daß in Fällen, in denen die umgekehrte CF-1-Form nicht Markovsch ist, die Kosten durch Annäherung an diese Form reduziert werden können. Es werden zwei Algorithmen entwickelt, die, ausgehend von der CF-1-Form beziehungsweise der umgekehrten CF-1-Form, in dem in Abbildung 2 dargestellten Suchraum nach einem Optimum suchen. Wenn die umgekehrte CF-1-Form Markovsch ist, finden beide Algorithmen das durch Satz 1 beschriebene Optimum. Andernfalls können sie das globale Optimum verfehlen. Die Algorithmen sind jedoch schneller als eine vollständige Enumeration aller $n!$ Permutationen. Die Effizienzsteigerung durch Umsortieren ist abhängig von der Verteilung und dem Algorithmus. In Beispielen sind die neuen Repräsentationen um bis zu 20% effizienter als die CF-1-Form.

Die Existenz einer zu Satz 1 äquivalenten Aussage für allgemeine PH-Verteilungen in monozyklischer Form wird widerlegt. Geeignete Heuristiken ermöglichen jedoch auch für allgemeine PH-Verteilungen eine Kostenreduktion durch Umsortieren.

2.3 Anpassung von Phasentypverteilungen

Für den Einsatz von Phasentypverteilungen müssen aus Messungen gewonnene Datensätze angepaßt werden. Dabei wird ein Tupel $(\boldsymbol{\alpha}, \mathbf{Q})$ gesucht, so daß die dadurch beschriebene Verteilung die statistischen Eigenschaften des Datensatzes gut wiedergibt. Neben einer guten Anpassungsqualität ist es für die Praxis vorteilhaft, wenn die angepaßte Verteilung effizient eingesetzt werden kann und wenn die Algorithmen zur Anpassung intuitiv konfigurierbar sind.

In der Arbeit wird ein neuer Algorithmus sowie ein Werkzeug zur Anpassung entwickelt. Der Algorithmus beruht auf der Aufspaltung des Datensatzes durch Clustering. Die einzelnen Teile werden mit PH-Verteilungen angepaßt und die Verteilung für den gesamten Datensatz ist die gewichtete Summe der Einzelverteilungen. Gegenüber existierenden Verfahren bieten sich folgende Vorteile: Erstens können für die Einzelverteilungen beliebige Klassen von PH-Verteilungen gewählt werden. In Experimenten zeigt sich, daß insbesondere Erlang-Verteilungen gut geeignet sind; mit diesen liefert der Algorithmus eine Hyper-Erlang-Verteilung als Ergebnis. Hyper-Erlang-Verteilungen haben kompakte

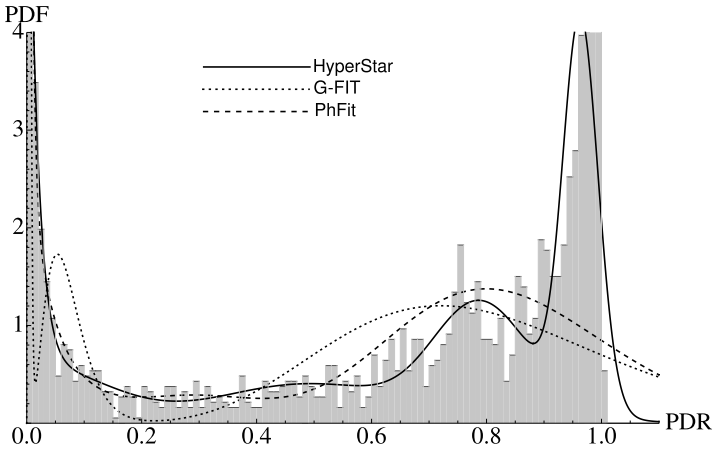


Abbildung 3: Histogramm eines Datensatzes aus dem DES-Testbett [BGJ+11] und Dichten angepaßter PH-Verteilungen. PDR bezeichnet die Paketübertragungswahrscheinlichkeit (Packet Delivery Ratio).

Repräsentationen und sind für die effiziente Zufallszahlenerzeugung nutzbar. Zweitens werden durch das Clustering-Verfahren vor allem Abschnitte mit ähnlichen Werten im Datensatz identifiziert. Derartige Häufungen zeigen sich in der Dichte als Hügel. Oszillierende Dichten werden in der Praxis häufig beobachtet (siehe z.B. [RW08]). Der Algorithmus ist daher besonders gut für die Anpassung empirischer Dichten geeignet. Drittens wird der Clustering-Algorithmus durch Vorgabe von Cluster-Mittelpunkten konfiguriert. Dies erlaubt eine intuitive Bedienung, da der Nutzer die Clustermittelpunkte in einer graphischen Benutzeroberfläche durch Auswahl und Markierung der Hügel der Dichte setzen kann. Der Algorithmus bildet den Kern des neuen PH-Anpassungswerkzeugs HyperStar.

Abbildung 3 illustriert beispielhaft die erzielbare Anpassungsqualität. Der hier verwendete Datensatz enthält die Paketübertragungswahrscheinlichkeiten für Links innerhalb des DES-Testbetts, eines Testbettes zur Untersuchung drahtloser Mesh-Netzwerke [BGJ+11]. In diesem Datensatz sind insbesondere die Hügel nahe bei 0, bei 0.75 und bei 1 wichtig. Im direkten Vergleich zu zwei anderen gebräuchlichen Werkzeugen (G-FIT [TBT06] und PhFit [HT02]) wird deutlich, daß HyperStar die Form der Dichte wesentlich besser erfaßt.

HyperStar ist so ausgelegt, daß das Programm auch als graphische Benutzeroberfläche für Mathematica-Programme dienen kann. Dies erleichtert die Entwicklung und Erprobung von Approximationsalgorithmen, wie anhand eines in der Arbeit entwickelten Algorithmus zur Anpassung von PH-Verteilungen in monozyklischer Form demonstriert wird.

Als Ergebnis des zweiten Teils der Arbeit stehen effiziente Algorithmen zur Erzeugung von Zufallszahlen aus PH-Verteilungen, theoretische Optimalitätsaussagen und Optimierungsalgorithmen für die Zufallszahlenerzeugung sowie ein leistungsfähiges und nutzerfreundliches Werkzeug zur Anpassung von Phasentypverteilungen an Datensätze zur Verfügung. Damit wird der Einsatz von Phasentypverteilungen insbesondere in der Simulation

und in Experimenten erheblich erleichtert.

3 Anwendung

Im dritten Teil werden die Ergebnisse anhand von Beispielen für die Systemevaluation mit stochastischen Modellen illustriert. Zunächst zeigt eine Fallstudie die Bedeutung der Wahl eines geeigneten Fehlermodells. Dazu werden die Auswirkungen einer zeitdiskreten und einer zeitkontinuierlichen Implementierung von Fehlermodellen für IP-Paketverluste auf verschiedene Klassen von Netzwerkprotokollen verglichen. Beide Implementierungen erzeugen alternierende Perioden von Paketverlusten und Paketübertragungen, wobei die Periodenlängen in der zeitdiskreten Implementierung in ankommenden Paketen gemessen werden und daher vom Ankunftsstrom abhängen. Im zeitkontinuierlichen Fall sind die Periodenlängen unabhängig. Es zeigt sich, daß ein Ankunftsprozeß, der auf Verluste mit einer Reduzierung der Senderate reagiert (wie das TCP-Protokoll) eine starke Verlängerung der Verlustperioden zur Folge hat. Damit werden die Auswirkungen von Paketverlusten auf höhere Ebenen stark überschätzt.

Anschließend wird die Libphprng-Bibliothek zur Erzeugung phasentypverteilter Zufallszahlen vorgestellt. Libphprng implementiert die effizienten Algorithmen aus dem zweiten Teil der Arbeit. Die Bibliothek kann mit minimalen Veränderungen an existierendem Quelltext zu vorhandenen Simulationsumgebungen hinzugebunden werden. Die Verwendung von Libphprng sowie der Vorteil der Nutzung von PH-Verteilungen gegenüber bekannten statistischen Verteilungen wird in einer Fallstudie illustriert.

Im letzten Abschnitt werden PH-Verteilungen zur Effizienzsteigerung in einem hybriden Simulationsansatz genutzt. Es wird gezeigt, wie die simulationsbasierte Untersuchung von PTP effizient durchgeführt werden kann. PTP ist ein Protokoll zur Frequenzsynchronisation zwischen den Basisstationen von Mobilfunknetzen, das nur sehr geringe Schwankungen der Übertragungszeiten aufeinanderfolgender Pakete toleriert. Die Laufzeiten der nötigen detaillierten Simulationen sind bei größeren Netzen sehr lang. Im hier beschriebenen Ansatz wird das Verhalten einzelner Switches mit PH-Verteilungen angepaßt und anschließend Netze aus diesen Modellen aufgebaut. Diese Modelle reduzieren die Simulationszeiten von Tagen auf Minuten bei nur sehr geringen Genauigkeitseinbußen.

Zusammenfassung

Die Beiträge der Dissertation erleichtern die Systemevaluation erheblich. Anhand der entwickelten Übersicht können geeignete Fehlermodelle für Studien schnell ausgewählt und eingesetzt werden. Das Werkzeug HyperStar erlaubt einem breiten Anwenderkreis die Anpassung von Phasentypverteilungen an Meßwerte, und die Bibliothek Libphprng ermöglicht die Verwendung der gewonnenen Verteilungen in Simulationsstudien. Die Optimalitätsaussagen und die Optimierungsalgorithmen garantieren die Effizienz der Zufallszahlenerzeugung.

Literatur

[Ber09] D.S. Bernstein. *Matrix Mathematics: Theory, Facts, and Formulas*. Princeton University Press, 2. Auflage, 2009.

[BGJ+11] Bastian Blywis, Mesut Günes, Felix Juraschek, Oliver Hahm und Nicolai Schmittberger. Properties and Topology of the DES-Testbed (2nd Extended Revision). Bericht TR-B-11-04, Freie Universität Berlin, July 2011.

[Cum82] A. Cumani. On the Canonical Representation of Homogeneous Markov Processes Modelling Failure-time Distributions. *Microelectronics and Reliability*, 22:583–602, 1982.

[HT02] András Horváth und Miklós Telek. PhFit: A General Phase-Type Fitting Tool. In *TOOLS '02: Proceedings of the 12th International Conference on Computer Performance Evaluation, Modelling Techniques and Tools*, Seiten 82–91, London, UK, 2002. Springer-Verlag.

[Joh63] Selmer M. Johnson. Generation of Permutations by Adjacent Transposition. *Mathematics of Computation*, 17(83):282–285, July 1963.

[MC99] Stefanita Mocanu und Christian Commault. Sparse Representations of Phase-type Distributions. *Commun. Stat., Stochastic Models*, 15(4):759 – 778, 1999.

[Neu81] Marcel F. Neuts. *Matrix-Geometric Solutions in Stochastic Models. An Algorithmic Approach*. Dover Publications, Inc., New York, 1981.

[Rei13] Philipp Reinecke. *Efficient System Evaluation Using Stochastic Models*. Dissertation, Freie Universität Berlin, 2012/2013.

[RW08] Philipp Reinecke und Katinka Wolter. Phase-Type Approximations for Message Transmission Times in Web Services Reliable Messaging. In Samuel Kounev, Ian Gorton und Kai Sachs, Hrsg., *Performance Evaluation – Metrics, Models and Benchmarks*, Jgg. 5119 of *Lecture Notes in Computer Science*, Seiten 191–207. Springer, June 2008.

[Sun06] Sun Microsystems. SUN Java Adventure Builder Reference Application. https://adventurebuilder.dev.java.net/, 2006. Last seen April 28th, 2009.

[TBT06] Axel Thümmler, Peter Buchholz und Miklos Telek. A Novel Approach for Phase-Type Fitting with the EM Algorithm. *IEEE Trans. Dependable Secur. Comput.*, 3(3):245–258, 2006.

Philipp Reinecke schloß sein Studium der Informatik und Politikwissenschaft an der Humboldt-Universität zu Berlin im Jahr 2007 ab und promovierte im Jahr 2012 an der Freien Universität Berlin.

Er befaßt sich seit fast zehn Jahren mit der Modellierung, Messung und Bewertung der Leistungsfähigkeit und Zuverlässigkeit von Systemen und setzt dabei gleichermaßen experimentelle, simulative und analytische Verfahren ein. Die betrachteten Anwendungsgebiete umfassen drahtlose Netzwerke ebenso wie service-orientierte Systeme, wo er insbesondere der Einsatz von Restart-Verfahren untersucht.

Derzeit arbeitet er im Trust-Domains-Projekt in den Hewlett-Packard-Laboratories in Bristol. Hier liegt der Schwerpunkt auf der modellbasierten Untersuchung des Spannungsfeldes zwischen Sicherheit, Leistungsfähigkeit und Zuverlässigkeit hochkomplexer Systeme, deren Verhalten von der Interaktion zwischen Individuen, Organisationen und technischer Infrastruktur bestimmt wird.

Der Asynchrone Graz Brain Switch*

Teodoro Solis-Escalante

Institut für Semantische Datenanalyse
Inffeldgasse 13/IV, 8010, Graz, Österreich
teodoro.solisescalante@tugraz.at

Abstract: Diese Dissertation führt den asynchronen Graz Brain Switch ein, ein nicht-invasives asynchrones Brain-Computer Interface basierend auf dem Beta Rebound Phänomen. Der Beta Rebound ist ein transientes Reaktionsphänomen im Elektroenzephalogramm, mit dem man Bewegungsvorstellungen detektieren kann. Der Graz Brain Switch verwendet das Beta Rebound Phänomen, um eine schnelle und einfache Anwendung sowie eine optimale Leistung mit möglichst wenigen falschen Aktivierungen zu ermöglichen. Diese Zusammenfassung präsentiert die Machbarkeitsstudien eines Beta Rebound basierenden Brain Switch und die online Evaluierung des Graz Brain Switches. Zusätzlich beschreibt diese Arbeit eines der ersten hybriden BCIs.

1 Einführung

Eine Gehirn-Computer Schnittstelle (Brain-Computer Interface, BCI) ist ein Kommunikationssystem, das eine direkte Verbindung zwischen dem menschlichen Gehirn und einem Computer herstellt [WBH+00] (siehe Abb. 1). Der hauptsächliche Zweck eines BCIs ist es, Menschen zu helfen, die aufgrund schwerer motorischer Einschränkungen sonst nicht mehr kommunizieren können. Für Personen ohne Einschränkungen eröffnen BCIs neuartige Mensch-Maschine Interaktionsmöglichkeiten.

Wesentliche offene Punkte, um BCI-Systeme außerhalb kontrollierter Bedingungen anzuwenden, sind praktische Verwendbarkeit und Zuverlässigkeit. Praktisch verwendbare BCI-Systeme sollten kostengünstig und einfach verwendbar sein. Zuverlässige BCI-Systeme sollten eine konstant hohe Leistung mit einer geringen Anzahl an Fehlern bieten. Eine Möglichkeit, ein einfaches BCI-System mit stabiler Leistung zu implementieren, ist ein sogenannter Brain Switch.

Ein Brain Switch [MB00] ist ein BCI, das zwei Zustände annehmen kann: einerseits einen sehr spezifischen mentalen Zustand und andererseits jeden anderen mentalen Zustand (siehe Abb. 1). Im asynchronen Modus bleibt der Brain Switch während Ruheperioden (nicht-beabsichtigte Kontrolle) inaktiv und reagiert nur wenn der Benutzer eine spezifische mentale Aufgabe ausführt (beabsichtigte Kontrolle). Der Benutzer kann so jederzeit frei entscheiden, wann er den Brain Switch aktivieren möchte. Damit ein derartiges System prak-

*Englischer Titel der Dissertation: “The Asynchronous Graz Brain Switch”

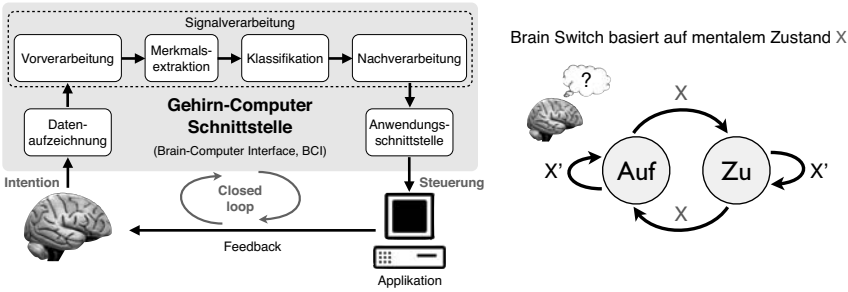


Abbildung 1: Blockdiagramm von einem BCI (links) und Konzept von einem Brain Switch (rechts).

tikabel ist, dürfen unbeabsichtigte Aktivierungen nicht vorkommen.

Diese Dissertation führt den asynchronen Graz Brain Switch ein [SE12], ein nicht-invasives asynchrones BCI basierend auf dem Beta Rebound Phänomen, welches auf eine Fußbewegung oder Fußbewegungsvorstellung folgt. Der Beta Rebound ist ein transientes Reaktionsphänomen im Elektroenzephalogramm (EEG), mit dem man Fußbewegungsvorstellungen detektieren kann. Der Graz Brain Switch verwendet das Beta Rebound Phänomen, um eine schnelle und einfache Anwendung sowie eine optimale Leistung mit möglichst wenigen falschen Aktivierungen zu ermöglichen. Die Kapitel in dieser Dissertation beschreiben die Entwicklungsstadien sowie die komplette Evaluierung des Graz Brain Switches. Die folgenden Abschnitte fassen die Arbeit dieser Dissertation zusammen.

2 Der Beta Rebound

Der Beta Rebound ist eine transiente nicht-phasengebundene Antwort des Gehirns, die als eine plötzliche Leistungszunahme im Beta-Frequenzband (13 bis 35 Hz) im EEG und anderen Aufnahmetechniken sichtbar wird. Vorübergehende Änderungen der spektralen Komponenten im EEG werden Ereigniskorrelierte Desynchronisation (Event-Related Desynchronization, ERD; Leistungsabnahme) und Ereigniskorrelierte Synchronisation (Event-Related Synchronization, ERS; Leistungszunahme) genannt [PL99]. Der Beta Rebound erscheint typischerweise am motorischen Kortex, dem somatosensorischen Kortex und dem supplementärmotorischen Areal (SMA). Nach einer Fußbewegung erscheint der Beta Rebound an der Vertexposition, nahe dem SMA und dem kortikalen Areal, in dem Fußbewegungen repräsentiert werden [NP96]. Zieht man die Nähe dieser beiden Areale und mögliches Übersprechen zwischen dem primärmotorischen Kortex und dem SMA in Betracht, erscheint es nachvollziehbar, dass ein Beta Rebound mit hoher Amplitude nach Fußbewegung oder Fußbewegungsvorstellung auftritt. Der Beta Rebound nach einer Fußbewegung hat ein sehr hohes Signal-Rausch-Verhältnis, wodurch sich dieses Phänomen besonders gut für die Detektion von Fußbewegungsvorstellung in einzelnen EEG-Epochen eignet.

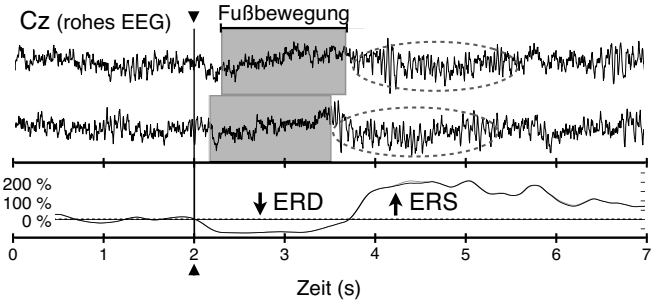


Abbildung 2: EEG vor, wahrend und nach einer Fubewegung. Oben: der Beta Rebound ist mit strichlierten roten Kreisen markiert. Unten: Relative Leistungsabnahme (ERD) und Leistungszunahme (ERS) im Beta-Frequenzband.

3 Machbarkeitsstudie eines Beta Rebound basierenden Brain Switch

Die Ergebnisse zu den Machbarkeitsstudien eines Brain Switch, der auf dem Beta Rebound basiert, wurden in zwei Artikeln publiziert [SEMPP08, PSE09]. Zunächst wurden EEG-Datensätze von zehn gesunden Teilnehmern analysiert. Das EEG wurde aufgezeichnet, während die Teilnehmer mehrere Durchläufe absolvierten, in denen sie motorische Aufgaben nach Erscheinen entsprechender Instruktionen durchführen mussten. Diese Aufgaben umfassten passive Bewegung, motorische Ausführung und motorische Vorstellung. Nur die drei Durchläufe, in denen die Teilnehmer kurze Fußbewegungen ausführen mussten, wurden für die Analyse verwendet.

EEG-Epochen (1 s lang) von einer Laplace-Ableitung wurden in spektrale Merkmale über die logarithmische Bandleistung zerlegt. Diese Merkmale entsprechen den spektralen Komponenten zwischen 6 und 36 Hz. Merkmalsvektoren wurden separat für ERD (während Bewegung) und ERS (nach Bewegung) Merkmale gegen die restliche Gehirnaktivität klassifiziert. Dadurch, dass ERD und ERS in unterschiedlichen Frequenzbändern und zu unterschiedlichen Zeitpunkten auftreten, kann angenommen werden dass sie sich gegenseitig ausschliessen.

Zur Klassifikation der Merkmalsvektoren wurden Support Vector Maschinen (SVM) mit Gauss'schen Kernels verwendet (libSVM, [CL01]). Kernelparameter der SVM wie z. B. der Regularisierungsfaktor C und die Kernelbreite σ wurden durch eine erschöpfende Suche in einem festgelegten Raster bestimmt. Vor der Parameterauswahl wurden die drei Durchläufe zufällig permutiert, und einer der Durchläufe wurde zu Evaluierungszwecken ausgewählt. Von den restlichen zwei Durchläufen wurde einer zum Trainieren und einer zum Testen verwendet. Eine 10-fache Kreuzvalidierung wurde für jedes Parameterpaar (C_i, σ_j) durchgeführt. Das Resultat für jeden Kreuzvalidierungsschritt wurde als Differenz zwischen der Rate der korrekten Aktivierungen (true positive rate, TPR) und der falschen Aktivierungen (false positive rate, FPR) zusammengefasst: $Y = \mathrm{TPR} - \mathrm{FPR}$. Nach dem Testen aller Parameterkombinationen wurde das Paar mit dem höchsten Wert

für Y selektiert.

Abschließend wurde ein SVM-Klassifikator mit den Trainings- und Testdurchläufen und dem zuvor gewählten Parameterpaar trainiert. Die SVM wurde trainiert, um eine Schätzung für die a-posteriori Klassenwahrscheinlichkeit jedes Merkmalsvektors zu bekommen. Mit einem Schwellwert (Threshold, TH), einer Verweildauer (Dwell Time, $\mathrm{DT} = 250\,\mathrm{ms}$) über dem Schwellwert und einer Refraktärperiode ($\mathrm{RP} = 2\,\mathrm{s}$) wurden Aktivierungen in der Ausgabe des Klassifikators detektiert. Der Parameter TH wurde dabei mittels Beobachterkennlinie (Receiver-Operator-Characteristc, ROC) ermittelt.

Die Kommandos eines asynchronen Brain Switches können zu jedem Zeitpunkt, abhängig von der Intention des Benutzers, ausgelöst werden. Eine Simulation eines asynchronen Brain Switches auf Daten, bei denen der Benutzer zu fixierten Zeitpunkten instruiert wurde, Aktivierungen auszulösen, können nützlich sein, um die Genauigkeit eines Brain Switches zu evaluieren, sowie absichliche Kontrolle und Ruhe voneinander zu differenzieren. Das Wissen, wann eine Brain Switch Aktivierung ausgelöst werden sollte, erlaubt es, TP, FP und falsche Nicht-Aktivierungen (False Negatives, FN) zu berechnen. Nachdem außerdem die Ruheperioden in der Trialstruktur bekannt sind, können weiters auch korrekte Nicht-Aktivierungen (True Negatives, TN) identifiziert werden.

Detektionen von kurzen Fußbewegungen basierend auf ERD erreichten eine durchschnittliche TPR von $0{,}21 \pm 0{,}12$. Die auf ERS basierende Detektion erreichte eine durchschnittliche TPR von $0{,}74 \pm 0{,}21$. Dies sind die bestmöglichen Ergebnisse laut der ROC, bei der die TPR maximal ist, während gleichzeitig die FPR maximal $0{,}1$ ist. Die Leistung des Klassifikators könnte noch weiter optimiert werden um die FPR noch weiter abzusenken. Dabei muss jedoch beachtet werden, dass TH-Änderungen, die zu einem weiteren Sinken der FPR führen, auch zu einer niedrigeren TPR führen.

Um das Beta ERS Phänomen weiter für die Verwendung in einem Brain Switch zu evaluieren, wurde in einer weiteren Analyse Bewegungsvorstellung detektiert. Dabei wurde EEG von fünf Teilnehmern in einem Paradigma ohne visuelles Feedback aufgezeichnet. In dem Paradigma führten die Teilnehmer motorische Vorstellung nach visuellen Instruktionen aus. Die Aufgabe bestand in kinästhetischer Vorstellung einer kurzen Fußbewegung. Merkmalsextraktion, Klassifikatortraining, sowie Nachverarbeitung und Erfassung der Leistung waren gleich wie oben beschrieben.

Die FPR wurde auch hier unter $0{,}1$ gehalten. Die durchschnittliche TPR für die Detektion von ERD war $0{,}28 \pm 0{,}13$ und die TPR für Detektionen von ERS war $0{,}59 \pm 0{,}20$. In Übereinstimmung mit vorherigen Analysen zu motorischer Ausführung waren die Ergebnisse des ERS-basierten Klassifikator besser als die des ERD-basierte Klassifikators.

Diese beiden Analysen zeigten, dass der Beta Rebound (ERS) für die Detektion von tatsächlichen und vorgestellten Fußbewegungen ein besseres Merkmal darstellt als ERD (siehe Abb. 3). Die relative Stabilität des Beta Rebound und seine Ähnlichkeit während ausgeführten und vorgestellten Fußbewegungen und die Aktivierungen ähnlicher kortikaler Areale während tatsächlicher oder vorgestellter Bewegungen könnten es erlauben, einen Brain Switch mit Bewegungsausführung aufzusetzen, der dann mit Bewegungsvorstellung kontrolliert werden kann.

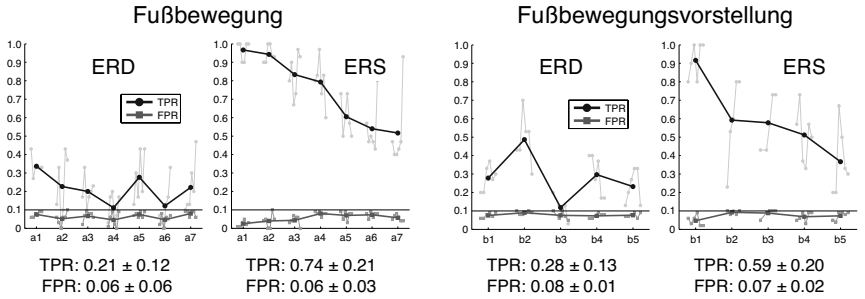


Abbildung 3: ERD- und ERS-basierte Detektion von Fußbewegung (links) und Fußbewegungsvorstellung (rechts).

4 Ein Brain Switch für gesunde Nutzer

Die Idee, einen Klassifikator mit Bewegungsausführung zu trainieren, wurde in einer weiteren Studie untersucht [SEMPB+10]. EEG-Signale von neun gesunden Personen wurden analysiert. Das EEG wurde während Durchgängen mit Bewegungsausführung und Bewegungsvorstellung ohne Feedback von fünf Ag/AgCl Elektroden, die auf der Kopfhaut um die Elektrodenposition Cz platziert waren, aufgenommen. Eine einzelne Laplace-Ableitung wurde aus den Mehrkanaldaten berechnet. Jeder Teilnehmer führte drei Durchgänge von Bewegungsausführung und weitere drei Durchgänge von Bewegungsvorstellung aus. Alle Durchgänge wurden am selben Tag durchgeführt, mit einigen Minuten Pause dazwischen.

Die Analyse der Daten wurde unterteilt in synchrone und asynchrone Verarbeitung. In der synchronen Phase wurden zwei SVMs auf den Daten aus den Durchgängen mit Bewegungsausführung trainiert, mit den zuvor beschriebenen Methoden. Die Kennzeichnung der Merkmalsvektoren wurde für jeden Teilnehmer über die Informationen aus den ERD/ERS Maps angepasst, die aus den Durchgängen mit der Bewegunsausführung berechnet wurden. Über die ERD/ERS Maps kann der Zeitverlauf der relativen spektralen Veränderungen (also ERD und ERS) in einem bestimmten Experiment visualisiert werden. Im Gegensatz zur vorherigen Analyse war die FPR während des Trainings nicht beschränkt auf 0,10. Stattdessen wurden die SVM-Parameter, die zur größten TPR und kleinsten FPR führten, ausgewählt. Danach wurde die Leistung so eingestellt, welche die FPR reduzierte und eine maximale TPR erzielte.

In der asynchronen Phase wurde eine kurze Kalibrierungsphase eingefügt, um die Parameter für die Nachverarbeitung DT, TH und RP aus den Durchgängen mit der Bewegungsvorstellung (der erste aufgezeichnete Durchgang) auszuwählen. Diese Parameter wurden über eine ROC-Analyse auf TH und DT ausgewählt, in der die Leistung für die Simulation eines asynchronen Brain Switches abgeschätzt wurde. Der Wert von RP unterlag der Bedingung $\mathrm{DT} + \mathrm{RP} = 2\,\mathrm{s}$. Die Parameter TH und DT, die zur höchsten TPR mit einer $\mathrm{FPR} \leq 0{,}10$ führten, wurden ausgewählt. Die Evaluation wurde mit der Simulation eines

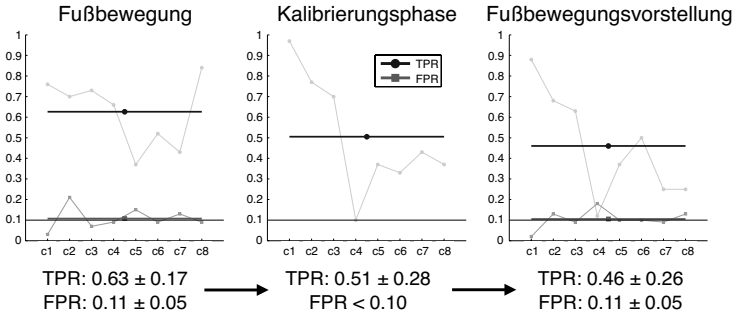


Abbildung 4: ERS-basierte Ergebnisse aus den Trainings-, Kalibrierungs- und Evaluationsphasen. ERD war das wichtigste Merkmal für Teilnehmer c4 und c5.

asynchronen Brain Switches abgeschlossen, die über die zwei verbleibenden Durchgänge der Bewegunsvorstellung ausgeführt wurde.

Die durchschnittliche TPR in der Evaluierungsphase war $0{,}52 \pm 0{,}20$ und $0{,}63 \pm 0{,}17$ für ERD- und ERS-basierte Klassifikation. Das Mittel der FPR war $0{,}11 \pm 0{,}03$ und $0{,}11 \pm 0{,}05$ für ERD- und ERS-basierte Klassifikation. Es gab keine signifikanten Unterschiede zwischen ERD- und ERS-basierten Klassifikationsschemas. ERS war das wichtigste Merkmal für sechs von acht Teilnehmern in der Trainingsphase (mit Bewegungsausführung). Diese Präferenzen blieben über die Kalibrierungs- und Evaluationsphasen (mit Bewegungsvorstellung) erhalten, wo ERD nur für zwei Teilnehmer eindeutig das wichtigste Merkmal war (Abb. 4).

Diese Ergebnisse zeigen, dass ein Brain Switch implementiert werden kann mit einem Klassifikator, der auf Bewegungsausführungsdaten trainiert wird und dann auf Bewegunsvorstellungsdaten mit einer geringen Kalibrierung angewendet werden kann. Dieser Ansatz war erfolgreich, da beide motorischen Aufgaben (Ausführung und Vorstellung) in ähnlichen ERD/ERS-Mustern resultieren. Obwohl es keine signifikanten Unterschiede zwischen ERD- und ERS-basierter Klassifikation gab, war ERS das wichtigste Merkmal für den Großteil der Teilnehmer.

Für die Implementierung eines Online Brain Switches wurde die Methodik angepasst: ein Schritt zur Merkmalsauswahl wurde integriert, der auf der Distinction Sensitive Learning Vector Quantization (DSLVQ) basiert, und als Klassifikator wurde Fisher's Lineare Diskriminanzanalyse (LDA) anstatt SVM benutzt. Diese beiden Methoden werden als Standard im Graz ERD-basierten BCI verwendet. ERS-Merkmale werden bevorzugt, aber ERD-Merkmale werden als Backup beibehalten. Es wurde gezeigt, dass beide Ansätze (SVM-basierte Klassifikation ohne Merkmalsauswahl und LDA-basierte Klassifikation mit DSLVQ-Merkmalsauswahl) äquivalent sind. Die Methode basierend auf LDA wird bevorzugt, da sie einfacher ist und einen geringeren Rechenaufwand während des Trainings mit sich bringt.

5 Online-Evaluierung

Die Online-Evaluierung des Graz Brain Switches wurde in einer weiteren Studie durchgeführt [PSEO+10]. Eine Möglichkeit, um die online Leistung eines asynchronen Brain Switches zu evaluieren, besteht darin, die Kontrolle des Users über eine einfache Benchmark-Anwendung zu erfassen. Eine Benchmark-Anwendung beinhaltet eine bestimmte Aufgabe und eine Menge an Regeln, die die Teilnehmer befolgen müssen, während sie den Brain Switch verwenden.

In einer neuartigen Benchmark-Anwendung konnten Bewegungsvorstellung und fokussierte visuelle Aufmerksamkeit in einem einzigen Experiment integriert werden, das von einem hybriden BCI kontrolliert wird. Hybride BCIs entstehen aus der Kombination aus einem BCI (z. B. ein Brain Switch), und einem anderen System. Das zweite System kann ein zweites BCI sein oder eine andere Art von unterstützender Technologie. In dieser Arbeit wurde ein hybrides BCI durch die Kombination eines Brain Switches mit einem BCI basierend auf Steady State Visual Evoked Potentials (SSVEP) realisiert. Um das hybride BCI zu bedienen, werden Bewegungsvorstellung und visuelle Aufmerksamkeit sequentiell vom Nutzer ausgeführt.

Die Experimente wurden in drei Hauptteile gegliedert. Der erste Teil beinhaltete das Training eines Brain Switches basierend auf dem Beta Rebound, der nach der Bewegungsvborstellung auftritt, und der Kalibrierung eines SSVEP-basierten BCIs. Der zweite Teil bestand in der selbstinitiierten Bedienung eines hybriden BCIs bestehend aus dem Brain Switch und dem SSVEP-basierten BCI. Zum Schluss, wiederholten die Teilnehmer das Paradigma unter selbstinitiierter Kontrolle mit dem SSVEP-basierten BCI als Kontrollbedingung.

Um Daten für das Training des Brain Switches zu erhalten, führte jeder Teilnehmer zwei Durchgänge der Bewegungsvorstellung ohne Feedback aus. Der Brain Switch wurde implementiert, indem das reaktive Band des Beta Rebounds und ein spezifisches Zeitfenster ausgewählt wurden, das die beste Klassifikation zwischen Beta Rebound nach Bewegungsvorstellung und einem Referenzintervall vor dem Stimulusbeginn boten. Um die Einstellungszeit zu reduzieren, wurden die Nachverarbeitungsparameter TH und DT manuell für jeden Teilnehmer während eines Testdurchgangs angepasst. Die Refraktärperiode (RP) wurde auf zwei Sekunden festgelegt.

Die Teilnehmer verwendeten ein SSVEP-basiertes BCI, um eine vierstufige elektrische Hand-Orthese zu steuern (Otto Bock GmbH, Wien, Österreich). Zwei an die Orthese angebrachte LEDs lieferten die visuelle Stimulation für das SSVEP-basierte BCI. Eine LED, die mit 8 Hz flackert, wird für die Handgelenksbeugung verwendet, die andere LED, die mit 13 Hz flackert, wird für die Handgelenksstreckung verwendet. Die Bedienung des SSVEP-basierten BCIs stützt sich auf die Harmonic Sum Decision (HSD) [MPP08]. Das SSVEP-basierte BCI implementiert die HSD-Methode mit Hilfe der diskreten Fourier Transformation, die über die letzte Sekunde der EEG-Aufzeichnung berechnet wird (bipolare Ableitung über O1). Der Output des SSVEP-basierten BCIs wurde weiter verarbeitet mit einer DT (1,56 s) und RP (4 s).

Das hybride BCI wurde realisiert, indem der ERS-basierte Brain Switch und das SSVEP-

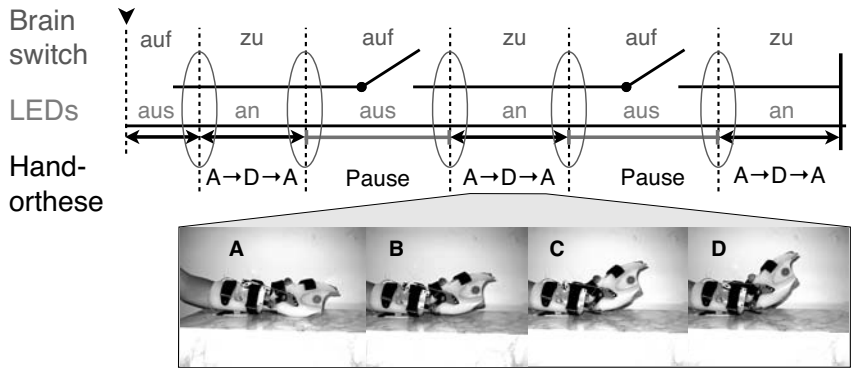


Abbildung 5: Paradigma für das hybride BCI Experiment. Am Anfang des Durchgangs mit selbstinitierter Kontrolle aktivierten die Teilnehmer den Brain Switch, um die visuelle Stimulation (d. h. die LEDs auf der Orthese) anzuschalten. Als nächstes bedienten die Teilnehmer das SSVEP-basierte BCI, um die Position der Handorthese zu verandern (A $\rightarrow$ D $\rightarrow$ A). Nach Beendigung dieser Aufgabe war es erforderlich, dass die Teilnehmer den Brain Switch aktivieren, um die visuelle Stimulation abzuschalten und das SSVEP-basierte BCI zu deaktivieren. Eine Ruhephase von einer Minute folgte. Diese Phase wird als nicht beabsichtigte Kontrolle betrachtet, und die Teilnehmer wurden instruiert, sich zu entspannen und die Aktivierung beider BCIs zu vermeiden. Die Teilnehmer wiederholten die SSVEP-basierte Kontrolle drei mal, mit zwei Ruhephasen dazwischen. Die maximal erlaubte Dauer eines Durchgangs betrug zehn Minuten. Ein perfekter Brain Switch Durchgang hŁtte fnf richtige Aktivierungen (rote Kreise) und keine falsche Aktivierung.

basierte BCI kombiniert wurden. Der ERS-basierte Brain Switch aktiviert/deaktiviert die flackernden Elemente des SSVEP-basierten BCIs während der SSVEP-basierten Kontrolle der Hand-Orthese. Das Paradigma mit selbstinitiierter Kontrolle erfordert, dass die Teilnehmer die beiden BCIs sequentiell bedienen (siehe Abb. 5). Die Teilnehmer wurden angewiesen, falsche Aktivierungen des Brain Switches und des SSVEP-basierten BCIs während der Phasen mit bewusster Kontrolle zu korrigieren. Als Kontroll-Experiment wiederholte jeder Teilnehmer das Paradigma mit selbstinitiierter Kontrolle mit dem SSVEP-basierten BCI alleine, d. h. der Brain Switch wurde als Kontrolle entfernt und die LEDs waren immer angeschaltet.

Das Mittel der Klassifikationsgenauigkeit während der Brain Switch Einrichtung war $85{,}0\pm$ $6{,}6$ %. Da die Nachverarbeitungsparameter manuell ausgewählt wurden, gab es keine Beschränkungen der FPR. Im Mittel resultierte die Brain Switch Leistung in $0{,}47 \pm 0{,}37$ FP/min (siehe Abb. 6). Zusätzlich traten $7{,}58 \pm 2{,}35$ TPs und $3{,}50 \pm 3{,}35$ FPs auf. Daraus ergibt sich ein Mittel des Positive Predictive Value (PPV) von $0{,}74 \pm 0{,}14$. Das heißt, dass 74 % aller Brain Switch Aktivierungen beabsichtigt waren. Der PPV betrug über 0,70 bei vier von sechs Teilnehmern.

Wenn man das hybride BCI betrachtet (siehe Abb. 6), war das Mittel der TP/min $3{,}96 \pm$ $1{,}34$ und der FP/min $0{,}84 \pm 0{,}98$ während der beabsichtigten Kontrolle. Zusätzlich traten $1{,}46 \pm 1{,}18$ FP/min während der nicht-beabsichtigten Kontrolle auf. Unter Berücksichtigung des SSVEP-basierten BCIs alleine betrug das Mittel des TP/min $6{,}87 \pm 2{,}48$ und

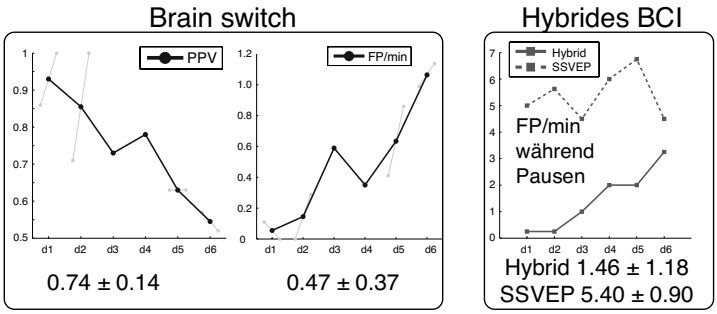


Abbildung 6: Leistung des Brain Switches und von des Hybriden BCIs.

das FP/min $0{,}94 \pm 0{,}76$ während der beabsichtigten Kontrolle. Zusätzlich traten $5{,}40 \pm 0{,}90$ FP/min während der nicht-beabsichtigten Kontrolle auf. Beachtenswert ist, dass die FP/min während nicht-beabsichtigter Kontrolle signifikant reduziert waren für das hybride BCI. Obwohl die TP/min (beabsichtigte Kontrolle) auch signifikant reduziert war, trat nur eine leichte Reduktion der FP/min und der PPV auf.

Die Ergebnisse zeigen die Online-Bedienung des Graz Brain Switch, und seine Rolle als Teil eines hybriden BCIs. Das hybride BCI-System bietet die Kontrolle einer Handorthese und reduziert gleichzeitig die FP/min während der Ruhephasen. Es wurde also gezeigt, dass die Einbeziehung des Brain Switches die Anzahl der falschen Aktivierungen reduziert. Dies wird durch die Deaktivierung des SSVEP-basierten BCIs während Phasen nicht-beabsichtigter Kontrolle erreicht. Das online Paradigma mit selbstiniitiierter Kontrolle kann als Benchmark-Anwendung betrachtet werden, und ist geeignet um verschiedene Brain Switch Designs in Echtzeitanwendungen mit Feedback zu untersuchen, zu testen und zu entwickeln. Es sollte erwähnt werden, dass die Anzahl der falsch positiven Erkennungen pro Minute (FP/min) 0,47 betrug. Im Vergleich betragen bei anderen Brain Switch Designs (diese wurden in den ersten Kapiteln dieser Dissertation diskutiert), die FP/min 0,7 in offline Analysen und 1,4 in online Experimenten.

6 Ausblick

Zukünftige Arbeit wird darauf ausgerichtet sein, die Leistung des Graz Brain Switch zu verbessern, zum Beispiel durch die Einbeziehung von zusätzlichen Merkmalen neben dem Beta Rebound, der nach der Bewegung auftritt. Aus praktischen Gründen wurden in den Analysen dieser Arbeit Laplace-Ableitungen um die Elektrodenposition Cz benutzt, d. h. ein Set aus fünf EEG-Kanälen. Obwohl der Beta Rebound eine spezifische somatotopische Organisation hat, variiert die Lokalisation der Quellen von Beta-Oszillationen über die Personen. Es wäre interessant, die verschiedenen bipolaren Ableitungen zu analysieren, die aus dem Set dieser Elektroden, oder aus zusätzlichen EEG-Kanälen berechnet werden können. Dies könnte genutzt werden, um Merkmale zu extrahieren, die relevant

für die Klassifikation sein könnten.

Literatur

[CL01] C. C. Chang und C. J. Lin. *LIBSVM: a library for support vector machines*, 2001. Software available at `http://www.csie.ntu.edu.tw/~cjlin/libsvm`.

[MB00] S. G. Mason und G. E. Birch. A brain-controlled switch for asynchronous control applications. *IEEE Transactions on Biomedical Engineering*, 47:1297–1307, 2000.

[MPP08] G. R. Müller-Putz und G. Pfurtscheller. Control of an electrical prosthesis with an SSVEP-based BCI. *IEEE Transactions on Biomedical Engineering*, 55:361–364, 2008.

[NP96] C. Neuper und G. Pfurtscheller. Post movement synchronization of beta rhythms in the EEG over the cortical foot area in man. *Neuroscience Letters*, 216:17–20, 1996.

[PL99] G. Pfurtscheller und F. H. Lopes da Silva. Event-related EEG/MEG synchronization and desynchronization: basic principles. *Clinical Neurophysiology*, 110:1842–1857, 1999.

[PSE09] G. Pfurtscheller und T. Solis-Escalante. Could the beta rebound in the EEG be suitable to realize a "brain switch"? *Clinical Neurophysiology*, 120:24–29, 2009.

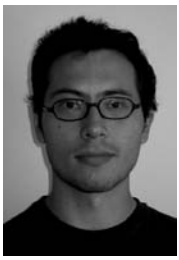
[PSEO$^+$10] G. Pfurtscheller, T. Solis-Escalante, R. Ortner, P. Linortner und G. R. Müller-Putz. Self-paced operation of an SSVEP-based orthosis with and without an imagery-based "brain switch": a feasibility study towards a hybrid BCIs. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, 18:409–414, 2010.

[SE12] T. Solis-Escalante. *The Asyncrhonous Graz Brain Switch*. Dissertation, Graz University of Technology, 2012.

[SEMPB$^+$10] T. Solis-Escalante, G. R. Müller-Putz, C. Brunner, V. Kaiser und G. Pfurtscheller. Analysis of sensorimotor rhythms for the implementation of a brain switch for healthy subjects. *Biomedical Signal Processing and Control*, 5:15–20, 2010.

[SEMPP08] T. Solis-Escalante, G. R. Müller-Putz und G. Pfurtscheller. Overt foot movement detection in one single Laplacian EEG derivation. *Journal of Neuroscience Methods*, 175:148–153, 2008.

[WBH$^+$00] J. R. Wolpaw, N. Birbaumer, W. J. Heetderks, D. J. McFarland, P. Hunter Peckham, G. Schalk, E. Donchin, L. A. Quatrano, C. J. Robinson und T. M. Vaughan. Brain-computer interface technology: a review of the first international meeting. *IEEE Transactions on Rehabilitation Engineering*, 8:164–173, 2000.



Teodoro Solis-Escalante wurde am 29. Jänner 1983 in Mexiko geboren. Er erhielt die akademischen Grade des M.Sc. (2007) in Biomedizinischer Technik von der Universidad Autónoma Metropolitana-Iztapalapa, Mexiko, und den Grad des Dr.techn. (2012) von der Technischen Universität Graz, Österreich. Seine Forschungsinteressen sind Gehirn-Computer-Kommunikationssysteme, Rehabilitationstechnik und somatosensorische und motorische Systeme des Menschen.

Schadsoftwareerkennung auf Netzwerkebene ohne Einzelpaketanalyse

Florian Tegeler
Institut für Informatik
Universität Göttingen
tegeler@cs.uni-goettingen.de

Abstract: Eines der größten Sicherheitsprobleme im Internet sind Bots – gekaperte Rechner, die in großer Zahl Schäden durch SPAM, Denial-of-Service-Angriffe oder Informationsdiebstahl anrichten. Entsprechend aktiv ist die Forschungsgemeinde bei der Entwicklung von Detektionsmechanismen, insbesondere auch im Feld der netzwerbasierten Erkennung. Da dazu jedoch typischerweise Paketinhalte analysiert werden müssen, stößt diese klassische netzwerkbasierte Detektion bei verschlüsselter Kommunikation an ihre Grenzen.

Als Antwort auf dieses Problem präsentieren wir BOTFINDER – ein neuartiges System, dass Bots anhand ihrer verbindungsorientierten Kommunikationsstruktur mit dem Botmaster erkennt und vollständig auf eine Analyse von Paketinhalten verzichtet. Hierzu beobachtet es das Kommunikationsverhalten der Schadsoftware in einer kontrollierten Umgebung und errechnet hieraus aussagekräftige Modelle. Diese Modelle werden dann im Praxisbetrieb mit dem Netzwerkverkehr der einzelnen Rechner im Netz verglichen.

Unsere Ergebnisse mit einer repräsentativen Auswahl verschiedener Bots auf realen Netzwerkmitschnitten zeigen, dass BOTFINDER in der Lage ist, Bots mit hoher Trefferquote bei gleichzeitig wenigen Falsch-Positiven zu erkennen.

1 Einleitung

Eine Vielzahl von Sicherheitsproblemen im heutigen Internet lässt sich auf Bots zurückführen, also Schadsoftware, die ohne das Wissen des Nutzers den Rechner infiziert und so in ein großes Netzwerk, dem Botnet [RZMT06], einbindet. Diese Netzwerke stehen typischerweise unter zentraler Kontrolle eines kriminellen Botmasters, der mit dem Netzwerk dem Versand von SPAM, Angriffen durch Distributed-Denial-of-Service (DDoS) oder Identitätsdiebstahl nachgehen kann. Entsprechend groß sind die Bemühungen bei der Entwicklung von Gegenmaßnahmen, um bereits einzelne Infektionen zu vermeiden bzw. aufzuspüren.

Der klassische Weg zur Schadsoftwarebekämpfung ist die Installation von Anti-Virus-Software auf den Rechnern der Endnutzer. Hierbei gibt es jedoch Probleme, wie z.B. den hohen Wartungsaufwand, die Erfordernis aktualisierter Virensignaturen und die lokale Sicht des Scanners. Als Konsequenz wird angestrebt, die lokalen Anti-Virus-Scanner durch netzwerkbasierte Lösungen zu ergänzen, die es erlauben, eine Vielzahl an Rechnern gleichzeitig zu untersuchen und miteinander in Beziehung zu setzen.

Da immer mehr Bots ihre Kommunikation verschleiern und verschlüsseln, um so einer netzwerkbasierten Erkennung zu entgehen, sollte eine erfolgreiche Lösung folgende Grundanforderungen erfüllen:

(a) individuelle Bot-Infektionen im Netzwerk erkennen,

(b) nur auf Verbindungsdaten basieren, um gegenüber verschlüsseltem Netzwerkverkehr immun zu sein und

(c) auch für Bots funktionieren, die sich nicht durch aussergewöhnliches Kommunikationsverhalten wie z.B. bei DDoS oder SPAM-Versand auszeichnen.

Als eine solche Lösung stellen wir BOTFINDER [TFVK12] vor – ein System, das individuelle Bot-Infektionen durch Beobachtung des Netzwerkverkehrs erkennt. BOTFINDER nutzt aus, dass die Kommunikation zwischen infiziertem Rechner und dem Botmaster, der sogenannte *Command-and-Control (C&C)*-Verkehr, oftmals regelmäßigen Mustern unterliegt die dann zur Erkennung verwendet werden können. Diese Muster erlernt BOTFINDER durch die Beobachtung des Netzwerkverkehrs von Schadsoftware, die in kontrollierter Umgebung ausgeführt wird. Aus diesen Mustern wird dann ein Modell des Bots erstellt, mit dem unbekannter Netzwerkverkehr verglichen und Bots darin erkannt werden können.

Aufgrund seines Designs arbeitet BOTFINDER anders als bisher veröffentlichte netzwerkbasierte Ansätze und ist in der Lage, einzelne Botinfektionen im Netzwerk zu erkennen. Zudem benötigt es keine Aktivitätskorrelationen der Netzwerkkommunikation wie beispielsweise BotSniffer [GZL08] oder BotMiner [GPZL08]. Die erwähnten Systeme erfordern zudem oft auffällige Aktivitäten wie SPAM oder DDoS Netzwerkverkehr, was die Erkennung von besonders getarnten Bots erschwert. Natürlich gibt es einige Systeme [WBH+09, GH07, GPY+07], die die Erkennung von individuellen Botinfektionen erlauben; diese arbeiten jedoch auf Basis der *deep packet inspection*, also der Analyse jedes einzelnen Paketinhaltes. Demgegenüber verwendet BOTFINDER nur NetFlow-ähnliche [Cla04] Informationen über die Netzwerkverbindungen und ist somit auch in der Lage, auf verschüsseltem Netzwerkverkehr zu arbeiten.

Um unseren Ansatz zu evaluieren, wurden Erkennungsmodelle für einige, zurzeit aktive, Schadsoftwarefamilien erzeugt, die eine Mischung verschiedener Infektions- und *C&C*-Strategien anwenden. Unsere Ergebnisse zeigen, dass BOTFINDER Netzkommunikation von Schadsoftware mit hoher Genauigkeit erkennt. Die erzeugten Modelle wurden zudem auf zwei Datensätzen – dem Mitschnitt der Netzkommunikation eines akademischen Forschungslabors und den Verbindungsdaten eines großen Internetanbieteres (mit mehreren Milliarden Verbindungen) – angewandt. BOTFINDER erzeugte dabei vielversprechende Erkennungsergebnisse bei niedriger Falsch-Positiv-Rate.

Insgesamt stellen wir folgende Ergebnisse vor:

- Die Beobachtung, dass der Netzwerkverkehr von Bots gewisse Periodizitäten aufweist, die genutzt werden können, um eine Unterscheidung zu normalem, unbedenklichem Netzwerkverkehr vorzunehmen. Durch die Unabhängigkeit von Paketinhalten kann unser Ansatz auch verschlüsselte bzw. verschleierte Kommunikation verarbeiten und Bots erkennen.

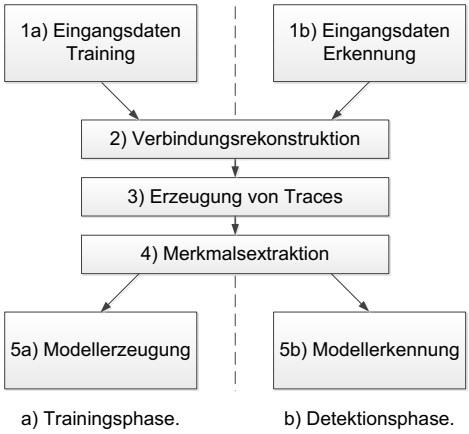


Abbildung 1: BOTFINDER-Architektur.

- BOTFINDER, ein System, das durch Beobachtung des Netzwerkverkehrs von Schadsoftware in kontrollierter Umgebung Modelle erzeugt, die dann zur Erkennung eingesetzt werden können.
- Ein Prototyp von BOTFINDER, der in der Lage ist, auf hochperformanten Netzwerken zu arbeiten und dort individuelle Schadsoftwareinfektionen zu erkennen, wie die Evaluation auf Basis verschiedener Netzwerkmitschnitte zeigt.

2 BotFinder

BOTFINDER erkennt Schadsoftware auf Netzwerkebene durch den Vergleich statistischer Merkmale des Netzwerkverkehrs mit vorab erlerntemn Modellen, die das Bot-Verhalten widerspiegeln. Dementsprechend arbeitet BOTFINDER in zwei Phasen: der *Trainingsphase* und der *Detektionsphase*. Während der Trainingsphase analysiert BOTFINDER die charakteristischen Merkmale des *C&C*-Verkehrs verschiedener Botfamilien und erzeugt statistische Modelle, die das Verhalten der Bots möglichst genau abbilden. In der Detektionsphase werden die Modelle auf den zu analysierenden Netzwerkverkehr angewandt und potentielle Botinfektionen identifiziert.

Wie Abbildung 1 zeigt, unterteilen sich beide Phasen in die fünf im Folgenden dargestellten Schritte.

2.1 Eingangsdatenverarbeitung

Im ersten Schritt wird Schadsoftware in kontrollierter Umgebung – wie z.B. Anubis [BKK08], BitBlaze [SBY+08], CWSandbox [WHF07] oder Ether [DRSL08] – ausgeführt und aller Netzwerkverkehr mitgeschnitten. Eine besondere Herausforderung hierbei ist die korrekte Klassifikation der binären Schadsoftwareprogramme zu Familien, wobei unsere Klassifikation auf Ergebnissen verschiedener Anti-Viren-Scanner, die über VirusTotal[1] abgefragt wurden, und Verhaltensanalysen in Anubis [BCH+09] beruhen. Nichtsdestotrotz können fehlerhafte Zuordnungen auftreten, was jedoch als statistische Schwankung die grundlegende Modellierung der Botfamilie nicht zu stark einschränkt.

2.2 Verbindungsrekonstruktion

In einem zweiten Schritt wird, wenn kein NetFlow direkt verwendet wird, der Paketdatenstrom logisch zu Verbindungen zusammengefasst. Wird ein normaler Netzwerkmitschnitt verwendet, erzeugt BOTFINDER Daten ähnlichen Formats zu NetFlow, dem Industriestandard für die Sammlung und Auswertung von Netzwerkinformationen.

2.3 Erzeugung von Traces

Im dritten Schritt werden Verbindungen zwischen zwei Netzwerkendpunkten zu chronologisch geordneten Folgen, sogenannten *Traces*, zusammengefasst. Die Traces bilden den wesentlichen Baustein von BOTFINDER, da auf Ihnen die gesamte statistische Auswertung erfolgt. Wie in Abbildung 2 im Beispiel dargestellt, zeigen einige Traces, wie $\mathcal{T}_2$ von A zu C auf Port 80, deutliche Regularitäten. Diese Regelmäßigkeit, erlaubt es BOTFINDER die Kommunikation durch das statistische Merkmal der nahezu konstanten Abstände zwischen zwei Verbindungen zu charakterisieren.

Um statistisch aussagekräftige Daten zu gewinnen, ist es notwendig, eine Mindestanzahl (typischerweise 10-50) von Verbindungen $|\mathcal{T}|_{min}$ zu beobachten. Eine weitere Herausforderung bei der Ermittlung der Traces ist die Unterscheidung zwischen echtem *C&C*-Verkehr und Störverbindungen, die teilweise bewusst von der Schadsoftware erzeugt werden [FSP+06] um den eigentlichen Kontrollverkehr zu tarnen. Um nicht-relevante Anteile des Netzwerkverkehrs zu ermitteln, verwenden wir zum Einen eine kurze Whitelist mit oft aufgerufenen Diensten wie Microsoft oder Google und zum Anderen eine Blacklist um Verbindungen zu bekannten Schadsoftwareservern zu erkennen und auszuwerten. Interessanterweise zeigt sich, dass fehlerhaft zum Kontrollverkehr gerechnete Netzwerkkommunikation oder der Verzicht auf die Blacklistauswertung die Modellergebnisse nur unwesentlich verschlechtert.

[1] `http://www.virustotal.com`

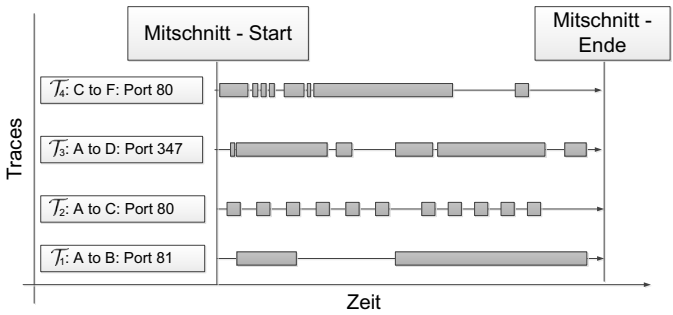


Abbildung 2: Verbindungssequenzen mit unterschiedlichen Verhaltensmustern..

2.4 Merkmalsextraktion

BOTFINDER erzeugt dann im vierten Schritt die grundlegenden statistischen Merkmale:

1. Das **durchschnittliche Intervall zwischen zwei Verbindungen** zwischen Quell- und Ziel-IP-Addresse auf einem festen Port. Dieses Zeitintervall ist oft periodisch, da die Bots regelmäßig den *C&C*-Server kontaktieren, um neue Befehle zu erhalten. Eine Kommunikation, bei der der Server ein neues Kommando des Botmasters an alle Bots weiterleitet, ist aufgrund der weiten Verbreitung von NATs und Firewalls oft nicht möglich, so dass die Bots selbstständig regelmäßig um neue Befehle bitten müssen. Interessanterweise ist es nicht einfach, zufällig erscheinenden Netzwerkverkehr, der trotzdem eine regelmäßige Kommunikation ermöglicht, zu erzeugen [TFVK12].
2. Die **durchschnittliche Zeit dieser Verbindungen**. Da bei den wiederholten Kommandoabfragen oftmals keine neuen Kommandos bereitstehen, ist die Kommunikation häufig gleich lang und von gleichem Transfervolumen. Selbst wenn neue Kommandos oder bspw. eine neue SPAM-Liste zur Verfügung steht, ist die Anfrage immer noch von festem Format.
3. Die **durchschnittliche Menge an Daten**, die in Quell- und Zielrichtung übertragen wurden.
4. Eine **Fouriertransformation der Folge an Startzeiten** in der Trace. Durch diese Frequenzanalyse können kleinere Unregelmäßigkeiten in der Kommunikation besser ausgeglichen werden und die grundlegende Periodizität wird besser erfasst.

2.5 Modellerzeugung

Im letzten Schritt clustered BOTFINDER die jeweiligen Merkmale und erzeugt so statistisch aussagekräftige Modelle. Jedes Merkmal wird hierbei für sich genommen verarbeitet,

Name	Daten-menge	Interne Rechner	Parallele Verbind.	Start-zeit	Länge	Verb.
LabCapture	$\approx$ 3.6 TB	$\approx$80	$\approx$60	2011-05-04	84 days	$\approx 64.3 \cdot 10^6$
ISPNetFlow	$\approx$ 540 TB	$\approx$1M	$\approx$250k	2011-05-28	37 days	$\approx 2.5 \cdot 10^{10}$

Tabelle 1: Datensätze

da wir oft keine Korrelation zwischen den verschiedenen Merkmalen beobachten konnten. Als Beispiel seien zwei Versionen des gleichen Bots angeführt, die sich zu zwei verschiedenen *C&C*-Servern C_1 und C_2 verbinden und je nach Version unterschiedliche Datenmengen übertragen. Nichtsdestotrotz können die beiden Versionen das gleiche Verbindungsintervall verwenden.

Nach dem Clustern werden die kleineren Cluster als nicht-repräsentativ verworfen und aus den großen Clustern die Modellbeschreibung abgeleitet. Ein Modell kann daher beispielsweise verstanden werden als:

> *Ein durchschnittliches Intervall von 850 oder 2.100 Sekunden, ein Transfer von 51kB zur Quelle und 140 Bytes zur Destination, eine Verbindungsdauer von 0,2 oder 10 Sekunden und eine Kommunikationsfrequenz von 0,0012Hz oder 0,04Hz deuten auf eine Dedler-Infektion hin.*

2.6 Modellerkennung

In der Detektionsphase wird der zu untersuchende Netzwerkverkehr genau wie der Trainingsverkehr statistisch analysiert und die Merkmale extrahiert. Diese Merkmale werden nun mit den vorliegenden Bot-Modellen verglichen und für jeden "Treffer" im Modell M wird eine Bewertungsvariable γ_M erhöht. Wie stark die Erhöhung ausfällt, hängt von der Qualität des Clusters und der vergleichenden Trace ab; je regelmäßiger der Netzwerkverkehr ist, desto stärker wird der Treffer gewichtet. Ist γ_M größer als ein – vom BOTFINDER-Administrator zur setzender – Wert a, gilt das Modell als akzeptiert. Der Administrator kann zudem verlangen, dass mindestens h verschiedene Merkmale des Modells getroffen werden, um Zufallstreffer so weit wie möglich zu reduzieren.

Für das Modell M mit dem größten γ_M wird, sofern $\gamma_M > a$, durch BOTFINDER ein Alarm ausgelöst.

3 Evaluation

Bei der Evaluation kamen sechs repräsentative Schadsoftwarefamilien mit durchschnittlich 32 verschiedenen Varianten zum Einsatz: **Banbra**, ein Spyware-Trojaner, die **Bifrose** (oder Bifrost) Familie, der DDoS Bot **Blackenergy** der bereits Polymorphismus und verschlüsselte Kommunikation beherrscht, der Spambot **Dedler**, **Pushdo**, ein stark verbrei-

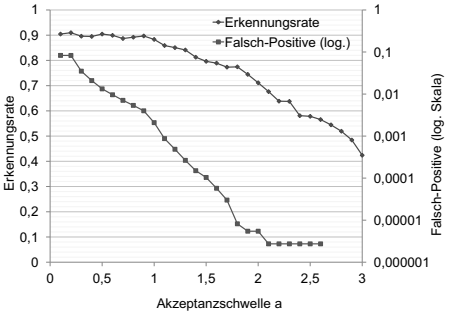


Abbildung 3: Detektions- und Falsch-Positiv-Rate von BOTFINDER im Kreuzvalidierungsexperiment.

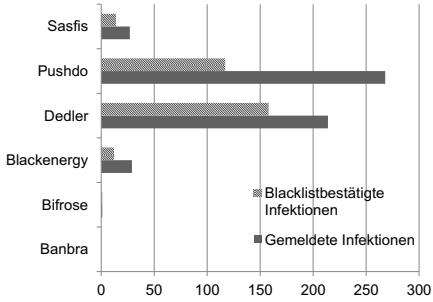


Abbildung 4: Infektionen nach Botfamilien aufgeschlüsselt. 56% der Verbindungen wurden zu bekannten Schadsoftwareservern aufgebaut.

teter SPAM-Bot, der auch unter den Namen *Pandex* oder *Cutwail* bekannt ist, und **Sasfis**, ein klassischen Trojaner.

Insgesamt wurden drei Experimente zur BOTFINDER-Evaluation durchgeführt: Ersten, ein Kreuzvalidierungsexperiment auf Basis von vollständigen Netzwerkmitschnitten aus einem Forschungslabor, zweitens ein Vergleich mit *Bothunter*, obwohl *Bothunter* Paketinhalte analysiert, jedoch kein direkt vergleichbares Produkt existiert, und drittens der Analyse eines Netzwerkmitschnittes eines großen Internetanbieters. Als Datensätze wurden die beiden in Tabelle 1 dargestellten Datensätze *LabCapture* und *ISPNetFlow* verwendet, wobei *LabCapture* ein vollständiger Mitschnitt ist, so dass potentielle Infektionen manuell überprüft werden können, und *ISPNetFlow* ein reiner NetFlow-Datensatz ohne Paketinhalte ist.

3.1 Kreuzvalidierung

Um die Erkennungsrate von BOTFINDER zu ermitteln, wurden die in kontrollierter Umgebung erhobenen Trainingsdaten mit dem *LabCapture* Datensatz vermischt und für verschiedene Erkennungsgrenzwerte α jeweils 50 Durchläufe folgender Art gemacht:

1. Die Schadsoftwaretraces wurden in ein Trainingsset $\mathcal{W}$ (70%) und ein Erkennungsset $\mathcal{D}$ (30%) geteilt.

2. $\mathcal{D}$ wurde mit dem *LabCapture* Datensatz vermengt und diente unter der Annahme, dass *LabCapture* infektionsfrei ist, als Grundlage zur Bestimmung der Falsch-Positiven.

3. BOTFINDER wurde auf $\mathcal{W}$ trainiert.

4. Die so erzeugten Modelle wurden auf die aus $\mathcal{D}$ und *LabCapture* erzeugten Daten angewandt.

Schadsoftware-Familie	BOTFINDER Erkennungsrate	BOTFINDER Falsch-Positive	*Bothunter* Erkennungsrate
Banbra	100%	0	24%
Bifrose	49%	0	0%
Blackenergy	85%	2	21%
Dedler	63%	0	n/a
Pushdo	81%	0	11%
Sasfis	87%	1	0%

Tabelle 2: Erkennungsrate und Falsch-Positive bei $a = 1.8$ im Kreuzvalidierungsexperiment und im Vergleich zu *Bothunter*.

Sehr niedrige Grenzwerte führen erwartungsgemäß zu hohen Erkennungsraten von mehr als 90%, aber auch hohen Fehlerquoten. Jedoch wird auf Abbildung 3 deutlich, dass die Erkennungsrate linear, die Fehlerrate dagegen exponentiell abfällt. Ein Optimum liegt für $a \in [0, 3]$ und $h = 3$ vor, wo z.B. für $a = 1.8$ 77% Erkennungsrate bei $5 \cdot 10^{-6}$ Falsch-Positiven erreicht wird. Wie Tabelle 2 zeigt, variieren die Erkennungsraten jedoch für die verschiedenen Bot-Familien.

3.2 Vergleich mit BotHunter

Bei einem direkten Vergleich mit *Bothunter* [GPY+07], einem paketinhaltbasierten, weiterentwickelten Snort[2], fällt auf, dass die Erkennungsrate von BOTFINDER deutlich über der von *Bothunter* liegt. *Bothunter* versucht den gesamten Infektionsprozess nachzuvollziehen und arbeitet stark mit Blacklists und fertigen Signaturen. Bei unserer Untersuchung konnten wir feststellen, dass *Bothunter* zudem stark auf Downloads von Binaries reagiert und dort auch viele Falsch-Positive (37 von 41 Alarmen) hervorruft, jedoch einige echte Infektionen übersieht. Interessanterweise hat *Bothunter* noch einige Infektionen im Forschungsnetz (*LabCapture*) aufdecken können, die von BOTFINDER nicht entdeckt wurden, da es auf diese Bots nicht trainiert worden war.

3.3 *ISPNetFlow*-Analyse

Da der *ISPNetFlow*-Datensatz nur Verbindungsdaten beinhaltet, können keine absoluten Aussagen über die Richtigkeit einer gemeldeten Bot-Infektion gemacht werden, jedoch können die Ziel-IPs der identifizierten Schadsoftwareverbindungen mit bekannten Blacklists verglichen werden um so eine Abschätzung der Erkennungsqualität zu erhalten. Die Daten wurden in 24-Stunden-Zeitschlitze unterteilt und durch BOTFINDER, das vorher mit allen erhobenen Schadsoftwaretraces trainiert wurde, ausgewertet. Insgesamt wurden im Durchschnitt 14.6 Traces als verdächtig markiert (542 insgesamt) – eine Menge, die

[2] `http://www.snort.org`

problemlos von einem Administrator im Tagesgeschäft genauer analysiert werden kann. Abbildung 4 zeigt die Gesamtzahl von Infektionen der verschiedenen Familien, wobei insbesondere die beiden SPAM-Bots Pushdo und Dedler mit 268 bzw. 214 Infektionen dominieren.

Ein Vergleich der Zieladdressen von als infiziert eingeschätzten Traces mit Informationen öffentlich verfügbarer Blacklists[3] ergab, dass es sich bei mindestens *56% davon um Verbindungen zu bekannten Schadsoftwareservern* handelt. Interessanterweise finden sich von den nicht in den Blacklists geführten 238 IP-Addressen 85 in 5 großen Clustern. Der größte Cluster zeigt zwar auf Apple Inc., die vier weiteren Cluster jedoch zu Firmen, die Dedicated-Server in Russland und auf den Seychellen vermieten. Fügt man Apple zur Whitelist, hinzu ergibt sich eine Trefferquote von 61% der identifizierten Zieladdressen in Blacklists.

4 Abschlussbetrachtung

In dieser Arbeit haben wir BOTFINDER vorgestellt, ein neues netzwerkbasiertes System zur Erkennung von einzelnen Schadsoftwareinfektionen im Netzwerk. BOTFINDER lernt aus der Beobachtung von Schadsoftware, die in kontrollierter Umgebung ausgeführt wird, erzeugt daraus Modelle und nutzt diese, um Bots ohne Analyse von Paketinhalten zu identifizieren. Hierbei erreicht es Erkennungsraten von nahezu 80% bei niedriger Falsch-Positiv-Rate.

Die hier sehr kurz vorgestellten Ergebnisse sind auf der ACM CoNEXT 2012 im Paper "BotFinder: Finding Bots in Network Traffic Without Deep Packet Inspection" [TFVK12] ausführlicher präsentiert worden und basieren auf der Dissertation "Content Agnostic Malware Detection in Networks" [Teg12].

Literatur

[BCH+09] Ulrich Bayer, Paolo M. Comparetti, Clemens Hlauschek, Christopher Kruegel und Engin Kirda. Scalable, Behavior-Based Malware Clustering. 2009.

[BKK08] Ulrich Bayer, Christopher Kruegel und Engin Kirda. Anubis: Analyzing Unknown Binaries. In *http://anubis.iseclab.org/*, 2008.

[Cla04] B. Claise. Cisco Systems NetFlow Services Export Version 9. RFC 3954", Internet Engineering Task Force, 2004.

[DRSL08] Artem Dinaburg, Paul Royal, Monirul Sharif und Wenke Lee. Ether: malware analysis via hardware virtualization extensions. In *Proceedings of the 15th ACM conference on Computer and communications security*, CCS '08, Seiten 51–62, New York, NY, USA, 2008. ACM.

[3] RBLS: `http://rbls.org/`

[FSP+06] Prahlad Fogla, Monirul Sharif, Roberto Perdisci, Oleg Kolesnikov und Wenke Lee. Polymorphic blending attacks. In *Proceedings of the 15th conference on USENIX Security Symposium - Volume 15*, Berkeley, CA, USA, 2006. USENIX Association.

[GH07] Jan Goebel und Thorsten Holz. Rishi: Identify Bot Contaminated Hosts by IRC Nickname Evaluation. In *HotBots'07: Proceedings of the First Workshop on Hot Topics in Understanding Botnets*, Seiten 8–8, Berkeley, CA, USA, 2007. USENIX Association.

[GPY+07] Guofei Gu, Phillip Porras, Vinod Yegneswaran, Martin Fong und Wenke Lee. BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation. In *Proceedings of the 16th USENIX Security Symposium (Security'07)*, August 2007.

[GPZL08] Guofei Gu, Roberto Perdisci, Junjie Zhang und Wenke Lee. BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection. In *Proceedings of the 17th USENIX Security Symposium (Security'08)*, 2008.

[GZL08] Guofei Gu, Junjie Zhang und Wenke Lee. BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic. In *Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08)*, February 2008.

[RZMT06] Moheeb A. Rajab, Jay Zarfoss, Fabian Monrose und Andreas Terzis. A Multifaceted Approach to Understanding the Botnet Phenomenon. In *IMC '06: Proceedings of the 6th ACM SIGCOMM on Internet measurement*, Seiten 41–52. ACM Press, 2006.

[SBY+08] Dawn Song, David Brumley, Heng Yin, Juan Caballero, Ivan Jager, Min Kang, Zhenkai Liang, James Newsome, Pongsin Poosankam und Prateek Saxena. BitBlaze: A New Approach to Computer Security via Binary Analysis. In R. Sekar und Arun Pujari, Hrsg., *Information Systems Security*, Jgg. 5352 of *Lecture Notes in Computer Science*, Seiten 1–25. Springer Berlin / Heidelberg, 2008.

[Teg12] Florian Tegeler. *Content Agnostic Malware Detection in Networks*. Dissertation, University of Gttingen, Germany, `http://ediss.uni-goettingen.de/handle/11858/00-1735-0000-000D-F068-1`, 2012.

[TFVK12] Florian Tegeler, Xiaoming Fu, Giovanni Vigna und Christopher Kruegel. BotFinder: Finding Bots in Network Traffic without Deep Packet Inspection. In *Proceedings of the 8th international conference on Emerging networking experiments and technologies*, CoNEXT '12, Seiten 349–360, New York, NY, USA, 2012. ACM.

[WBH+09] Peter Wurzinger, Leyla Bilge, Thorsten Holz, Jan Goebel, Christopher Kruegel und Engin Kirda. Automatically Generating Models for Botnet Detection. In *14th European Symposium on Research in Computer Security (ESORICS), Lecture Notes in Computer Science, Springer Verlag*, September 2009.

[WHF07] Carsten Willems, Thorsten Holz und Felix Freiling. Toward Automated Dynamic Malware Analysis Using CWSandbox. *IEEE Security and Privacy*, 5:32–39, 2007.



Florian Tegeler studierte Informatik (BSc/MSc) und Physik (Diplom) in Göttingen und promovierte von 2008 bis 2012 am dortigen Institut für Informatik. Über längere Auslandsaufenthalte an der University of Cambridge, der Columbia University in New York und der University of California in Santa Barbara konnte er seine verschiedenen Interessen von Internet Security über Netzwerktechnik zu Social Network Analysis verfolgen.

Irisbiometrie in der Überwachung: Innovationen zu Segmentierung und Komparatoren*

Peter Wild

Fachbereich Computerwissenschaften, Universität Salzburg
Jakob Haringer Str. 2, 5020 Salzburg, Austria
pwild@cosy.sbg.ac.at

Abstract: Die Iris des menschlichen Auges zählt zu den eindeutigsten Merkmalen zur Personenidentifikation ohne Erfordernis von Token oder Wissen. Irisbiometrie-Systeme erfordern aber traditionell die Kooperation der Person dessen Merkmal extrahiert werden soll. Um aus Sicherheitsgründen die automatische Identitätsfeststellung aus Beobachtungsdaten zu ermöglichen, müssen neue Lösungen entwickelt und untersucht werden, um Eingabebeispiele niedriger Qualität (defokussierte, bewegungsunscharfe, ausserhalb der optischen Achse aufgenommene Bilder verschiedener Spektren) in Echtzeit verarbeiten zu können. Diese Arbeit präsentiert neue Modelle zur homogenen Segmentierung von Bildern sichtbarer Wellenlänge sowie nahinfrarot und neue Komparatoren, welche die Wechselbeziehung zwischen Genauigkeit und Geschwindigkeit ausnutzen.

1 Einführung

Um die unbeaufsichtigte, unkooperative, automatisierte Identitätsfeststellung von Personen basierend auf der menschlichen Iris aus Gesichtsaufnahmen in nichtstandardisierten Umgebungen in Echtzeit und mit für die Anwendung hinreichender Genauigkeit zu ermöglichen, weist das Daugman'sche Referenzmodell [Dau04] für Iris-Erkennung (siehe Abbildung 1) an einigen Punkten Schwachstellen auf: (1) Segmentierungsmodelle verwenden unzureichend flexible kreisförmige Randmodelle oder sind nicht echtzeitfähig aufgrund eines zu komplexen Parameterraums des Segmentierungsmodells; (2) Segmentierungsalgorithmen sind auf bestimmte Datenquellen geeicht, insbesondere ist eine Anwendung desselben Augendetektions bzw. Lokalisationsalgorithmus für in Irissystemen typische Nahinfrarot (NIR) Bilder und Überwachungsaufnahmen im sichtbaren (VW) Spektrum generell nicht möglich; (3) die Hamming-Distanz (HD) als Standard-Komparator zum Vergleich zweier Muster bei der Authentifikation wurde bislang nicht im Hinblick auf die erzielbare Wechselwirkung zwischen Genauigkeit und Geschwindigkeit optimiert, und; (4) Segmentierungsungenauigkeiten im Rahmen der Komparator-Anwendung zu behandeln sowie Fusion von Komparatoren bieten neue Möglichkeiten erhöhter Performanz.

*Englischer Titel der Dissertation: "Advanced Segmentation and Comparators for Iris Biometric Surveillance" [Wil12]; enthält Inhalte aus Monographie [RUW12b], Journal und internat. Konferenzbeiträgen des Autors.

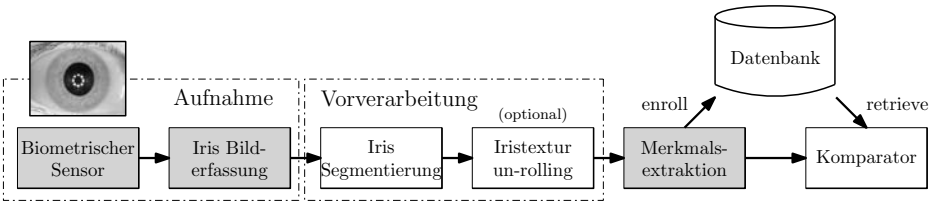


Abbildung 1: Verarbeitungskette für Irisbiometrie-Systeme [RUW12b].

Im Rahmen der kumulativen Dissertation [Wil12] wurden verschiedene Lösungsansätze zu Segmentierung und Komparatoren in der Irisbiometrie entwickelt. In Sektion 2 werden vorgeschlagene Segmentierungsverfahren vorgestellt, Sektion 3 fokussiert auf neue Komparatoren. Algorithmen werden in Sektion 4 mittels öffentlicher Bilddatenbanken evaluiert und Resultate diskutiert. Sektion 5 beschließt diese Zusammenfassung.

2 Segmentierung

Segmentierung in der Biometrie beschäftigt sich mit Lokalisierung und Normalisierung des Merkmals und gehört aufgrund ungleicher Ausleuchtung, Bewegungsunschärfe und Fehlfokussierung zu den schwierigsten, aber aufgrund zahlreicher öffentlicher Wettbewerbe (MBGC, NICE) meistuntersuchten Problemen in biometrischer Überwachung [Pro10]. Im Folgenden werden ein allgemeines Framework zur modellgesteuerten Objekterkennung sowie ein robuster Irissegmentierungsalgorithmus mit dem Ziel einer Verschmelzung von VW Gesichts- und NIR Irisbiometriesystemen vorgestellt.

2.1 Gauss'sche modellgesteuerte Gesichts- und Gesichtsteil-Fusion

Zur Detektion von Gesicht und Augen lassen sich existierende (und potentiell verbesserbare) individuelle Klassifizierer auf generische Art und Weise kombinieren. Dazu werden Normalverteilungen (N_x, N_y, N_s zu Lokation x, y und Größe s für jeden Typ t) zu einzelnen Detektor-Antworten gelernt [UW12a], aber nicht kaskadierend wie in AdaBoost [VJ01] sondern parallel ausgeführt und kombiniert. Zu jeder Teilmenge von $i \in \{1, \ldots, m\}$ Klassifizierern wird die Position $O = (a, b)$ und Augenabstand u des Gesichts sowie zugehörige Streuungen geschätzt, basierend auf N_x, N_y, N_s, siehe Abb. 2:

$$a := x - \mu_x s; \quad b := y - \mu_y s; \quad u := \frac{s}{\mu_s}; \quad \alpha := \sigma_x u; \quad \beta := \sigma_y u; \quad \gamma := \sigma_s u. \tag{1}$$

Zu jeder Menge $L := \{L_1, \ldots, L_m\}$, $L_i = (a_i, b_i, u_i, \alpha_i, \beta_i, \gamma_i)$ von Modellokationen wird das Durchschnittsmodell $\overline{L} = (\overline{a}, \overline{y}, \overline{u})$ berechnet, sowie eine Energiefunktion $E(L)$ ermittelt, welche die Konformität der Individualdetektionen mit dem Modell evaluiert.

$$\overline{a} := (\sum_{i=1}^{m} \frac{1}{\alpha_i}) \cdot (\sum_{i=1}^{m} a_i \cdot \frac{1}{\alpha_i}); \quad \overline{b} := (\sum_{i=1}^{m} \frac{1}{\beta_i}) \cdot (\sum_{i=1}^{m} b_i \cdot \frac{1}{\beta_i}); \quad \overline{u} := (\sum_{i=1}^{m} \frac{1}{\gamma_i}) \cdot (\sum_{i=1}^{m} u_i \cdot \frac{1}{\gamma_i}). \tag{2}$$

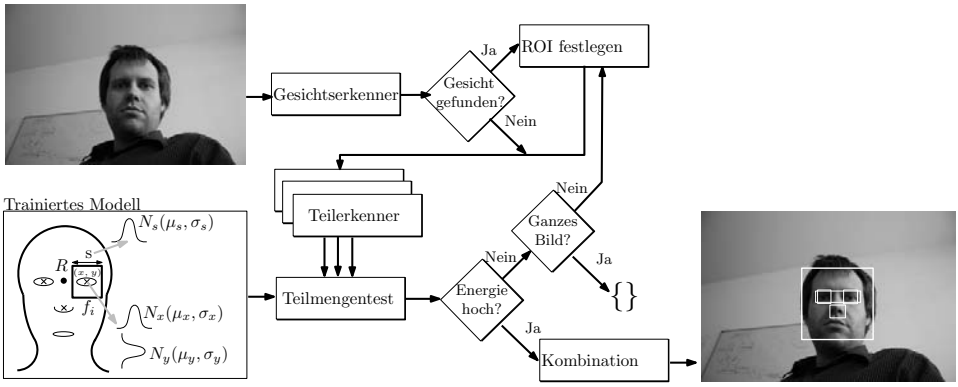


Abbildung 2: Gauss'sche modellgesteuerte Gesichts- und Gesichtsteil-Fusion [UW12a].

$$E(L) := \frac{1}{m} \sqrt{1 + \sum_{i=1}^{m} \max\left(\frac{|a_i - \overline{a}|}{\alpha_i}, \frac{|b_i - \overline{b}|}{\beta_i}, \frac{|u_i - \overline{u}|}{\gamma_i}\right)}. \tag{3}$$

Individuelle Detektionen werden anhand des bzgl. Energiefunktion optimalen Modells rekonstruiert.

2.2 Gewichtete adaptive Hough und Ellipsopolar-Transformation

Bevor Merkmale aus der Iristextur extraiert werden, empfiehlt sich die Anwendung von Daugman's "Rubbersheet Transform" [Dau04], welche ein $m \times n$ Irisbild anhand der parametrisierten inneren und äußeren Randkurven P, L aufrollend in einen Raum abbildet, der invariant gegenüber Pupillendilation ist:

$$R : [0, 2\pi) \times [0, 1] \to [0, m] \times [0, n]. \quad R(\theta, r) := (1 - r) \cdot P(\theta) + r \cdot L(\theta). \tag{4}$$

Um eine effizientere und tolerantere Ermittlung der Randkurven als die traditionelle zirkulare Hough Transformation bzw. der integrodifferentiale Operator [Dau04] zu erreichen wurde ein neues Framework vorgeschlagen, welches folgende Ideen umsetzt: (1) Zweistufige Segmentierung mit separater Zentrums- und Randerkennung; (2) Adaption einer iterativen Hough Transformation nach [CFV08]; (3) Polar- und Ellipsopolartransformation zur Unterstützung der Randfindung basierend auf Zentrum und detektierter Primärrandkurve; (4) Gauss'sche Gewichtungsfunktionen zur Einbeziehung von Vorwissen.

Zur adaptiven Zentrumsfindung wird dabei für eine Zielregion im Bild (ROI) R_i der Größe $m_i \times n_i$ ein $w \times h$ Akkumulator-Zellgitter A_i iterativ inkrementiert, siehe Abb. 3:

1. *Initialisierung*: Aus allen Kantenpixeln E_{i-1} werden alle Punkte $P_j \in E_{i-1}$ bestimmt, deren Gradientenlinien g_j sich mit der ROI R_i schneiden als E_i.

2. *Wahlphase*: Alle Zellen in A_i, welche nach Bresenham von Gradientenlinien g_j aus Punkten in E_i geschnitten werden, inkrementiert man um den absoluten Gradienten.

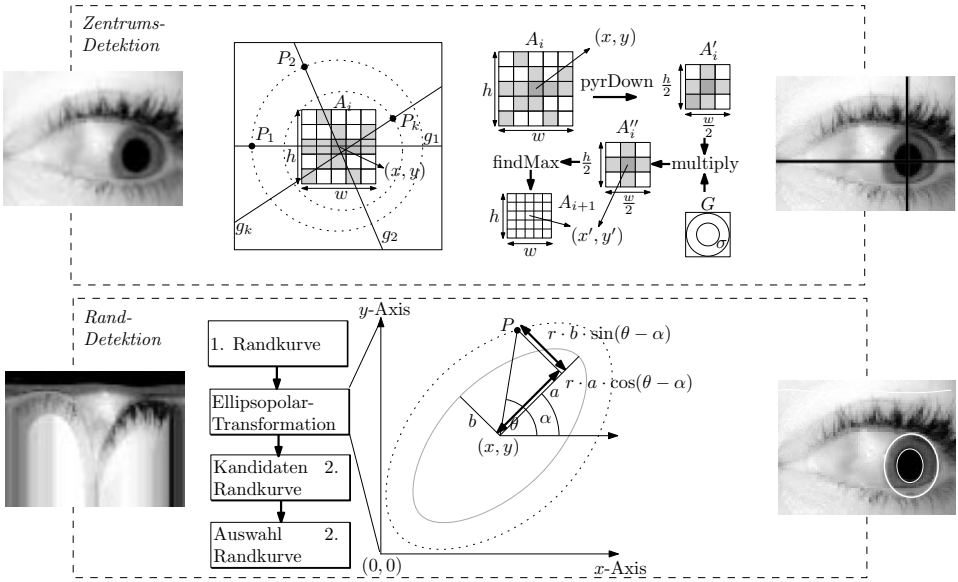


Abbildung 3: Adaptive Hough Transformation und Ellipsopolartransformation der vorgeschlagenen WAHET Segmentierung [UW12c].

3. *Gewichtung*: Der Accumulator A_i wird skaliert, mit einem Gauss'schen Kernel G multipliziert, die Zelle mit Maximalwert gefunden und mit der verfeinerten Region R_{i+1} halber Größe zentriert im Zellenkern fortgefahren, solange die geforderte Genauigkeit nicht erreicht ist bzw. der Regionsmittelpunkt ausgegeben.

Mit vorgeschlagener Technik lassen sich verschiedene Implementierungen realisieren und mit Randfindungsalgorithmen kombinieren (WAHET [UW12c], IFPP [UW12b]). Zur homogenen Verarbeitung von NIR und VW-Daten wurde in WAHET eine ellipsopolare Transformation vorgeschlagen, welche die Randfindung basierend auf der ersten gefunden ellipsoiden Randkurve unterstützt, indem konzentrische Ellipsen auf achsenparallele Geraden abgebildet werden, siehe Abb. 3. Sei B die polar gesampelte Repräsentation einer orientierten Ellipse mit Zentrum (x, y), Halbachsen a, b und Auslenkungswinkel α, dann ist die zugehörige Ellipsopolartransformation definiert als:

$$T_E : [0, 2\pi) \times \mathbb{R}_0^+ \to \mathbb{R}^2.\ T_E \begin{pmatrix} \theta \\ r \end{pmatrix} := \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} * \begin{pmatrix} ra\cos(\theta - \alpha) \\ rb\sin(\theta - \alpha) \end{pmatrix} \quad (5)$$

3 Komparatoren

Traditionelle Irisbiometriesysteme verwenden die minimale fraktionale HD an mehreren Versatzstellen (*shifts*) um zu zwei gegebenen Merkmalsvektoren (*Iriscode*) die Ähnlichkeit unabhängig von Augenrotation zu bestimmen [RUW12b]. Folgende alternative Komparator-Klassen wurden vorgeschlagen:

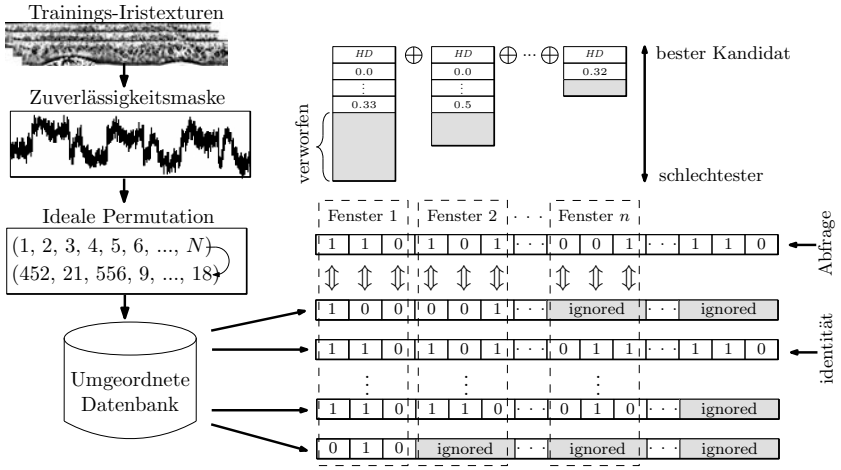


Abbildung 4: IIR-Komparator: HD wird inkrementell berechnet und unwahrscheinliche Kandidaten schnell verworfen [RUW10].

1. *Alignment-optimierte Komparatoren*: nutzen Information bei der Codeausrichtung und tolerieren zusätzliche nicht-lineare Verzerrungen bzw. Segmentierungsfehler;

2. *Zuverlässigkeits-basierte Komparatoren*: nutzen die Zuverlässigkeits individueller Codebits um schnell Nicht-Übereinstimmungen zu verwerfen;

3. *Fusions-Komparatoren*: kombinieren verschiedene Merkmale (und untersuchen u.a. Bildmetriken für Vergleiche).

Der CLD-Komparator (Constrained Levenshtein Distance) [UW10] verwendet dynamische Programmierung [MR81] sowie Optimierungen bezüglich maximalem Versatz (Berechnungen werden auf eine Region $S := \{(x, y) : |x - y| \leq s\}$ beschränkt), um eine Subsequenz $a[1..i]$ in $b[1..j]$ in minimal $D[i, j]$ Operationen $(c_{del}, c_{ins}, c_{sub})$ zu transformieren und besseres Alignment zu erzielen. Dabei liegt die optimierte Version in derselben Komplexitätsklasse wie HD ($O(n \cdot s)$ Zeit und $O(n + s)$ Speicherplatz bei n Bits und s Versatz).

$$D[0,0] = 0;\ \ \forall i > 0 : D[i,0] = D[i-1,0] + c_{del};\ \ \forall j > 0 : D[0,j] = D[0,j-1] + c_{ins};$$
$$\forall i,j > 0 : D[i,j] = \min(D[i-1,j] + c_{del}, D[i,j-1] + c_{ins}, D[i-1,j-1] + c_{sub}(a[i], b[j])). \quad (6)$$

Weitere Komparatoren aus der Alignment-optimierten Klasse umfassen SSF (Shifting Score Fusion) [RUW11c] als Verfahren, welches minimale und maximale HD kombiniert, sowie GSF (Gauss'sches Score Fitting) [RUW12a], welches neben der minimalen HD die Ähnlichkeit der Verteilung der HD-Werte mit einer gelernten Gauss-Verteilung berechnet und ausnutzt, dass sich echte Codepaare im Bereich des optimalen Alignments verbessern.

Um speziell im Überwachungseinsatz schnelle Negativ-Vergleiche durchführen zu können wurde der IIR-Komparator (Incremental Iris Recognition) entwickelt [RUW10]. Unter

Tabelle 1: Augendetektion: Rate und Zeit [UW12a].

Algo.	Erfolgsrate		Zeit	
	Casia-D	Yale-B	Casia-D	Yale-B
Eye-only	65.8%	87.3%	0.60 s	0.61 s
Nested	14.6%	97.6%	0.65 s	0.28 s
FFF	96.4%	99.2%	1.28 s	0.28 s

Tabelle 2: Komparatoren: relative Verbesserung der EER (CASIA.v3-I).

Komp.	Shifts	Masek	Ma
SSF	7	17%	10%
GSF	8	27%	18%
CLD	20	9%	24%

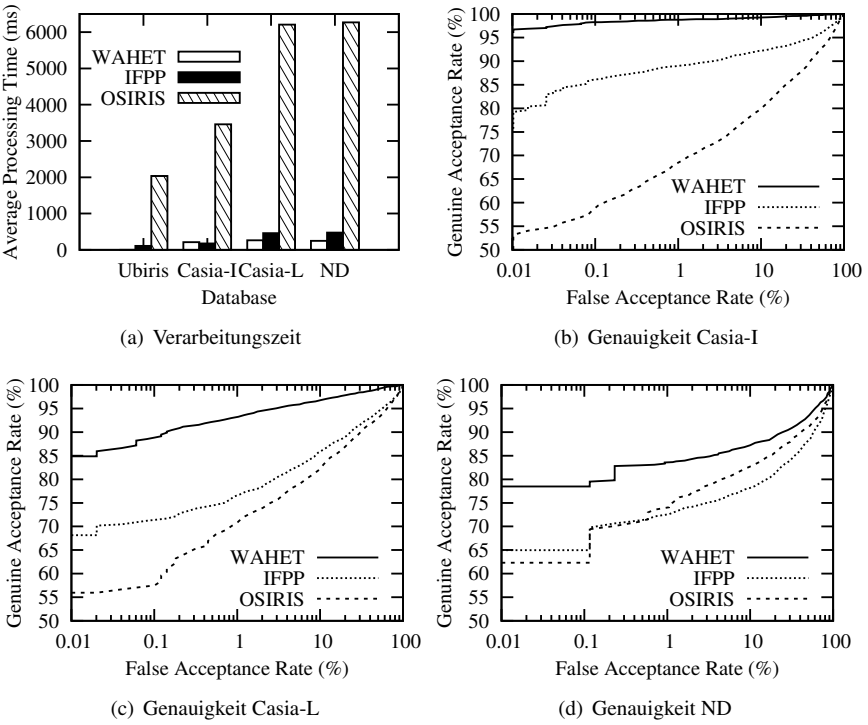
Ausnutzung der Eigenschaft, dass die Zuverlässigkeit von Iriscode-Bits nicht gleichverteilt ist [HBF09] wird in einer Trainingphase eine globale Zuverlässigkeitsmaske gelernt, welche zu jeder Bitposition der ausgerichteten Intra- und Inter-Vergleichspaare die Wahrscheinlichkeiten eines Bit-Wechsels (0-1 bzw. 1-0) P_{Intra} and P_{Inter} berechnet und nach *Reliability* $R = P_{Intra}$ - P_{Inter} geordnet. Basierend auf der erhaltenen Permutation von Iriscode-Bits kann nun ein partieller Vergleich durchgeführt werden. Dabei wird im Identifikationsmodus für alle gespeicherten Codes die minimale HD für ein Fenster fixer Größe (i Prozent) berechnet und nur jene Kandidaten x weiter verglichen, die eine Maximalabweichung η_i (trainierbar) vom besten Vergleichscode b aufweisen, siehe Abb. 4:

$$EC_i(x) := \begin{cases} keep & if\ HD_i(x,s) - HD_i(b,s) < \eta_i, \\ reject & otherwise. \end{cases} \tag{7}$$

Bit-Zuverlässigkeit kann auch verwendet werden, um im Rahmen von *Fuzzy Commitment Schemata* Iriscodes zweier Merkmale so anzuordnen, dass Fehlerkorrektur effizienter möglich ist [RUW11b]. Als letzte Gruppe von fusionsbasierten Komparatoren wurden sowohl Bildmetriken mit herkömmlicher HD [HRUW12b, HRUW12a] kombiniert als auch individuelle Komparatoren fusioniert: SSF mit zuverlässigkeits-basierten Techniken [RUW11a] oder schnelle rotationsinvariante mit kompensierenden klassischen Komparatoren [KSUW10]. Mittels generischer serieller Fusions-Techniken [UW09] kann ähnlich zu IIR eine Erhöhung von Genauigkeit und Geschwindigkeit bei der Kombination mehrerer biometrischer Merkmale erzielt werden. Generell ist anzumerken, dass die Grenze zu fusionsbasierten Techniken nicht scharf ist, insbesondere beinhalten auch [HRUW12a, RUW11b, RUW11c, RUW12a] fusionsbasierte Elemente.

4 Experimente

Um die Robustheit der Segmentierungsalgorithmen zu testen wurden verschiedene Datenquellen verwendet: (1) *Casia-D* als hochauflösendes (2352x1728) 282 Bilder Subset von NIR Gesichtsaufnahmen der CASIA.v4-Distance Datenbank, (2) *Yale-B* mit 252 VW 640x480 Portraits der Yale-B Datenbank, (3) *Casia-I* als Subset aller 1332 linken 320x280 NIR Augenbilder der offenen CASIA.v4-Interval Datenbank, (4) *Casia-L* bestehend aus einem 1000 Bilder NIR Subset aus CASIA.v4-Lamp, (5) *ND* aus 420 Bildern der NIR 640x480 Datenbank NDIRIS-0405, sowie (6) *UBIRIS* aus 817 Bildern der VW Irisdatenbank UBIRIS-V1, siehe [Wil12].



(a) Verarbeitungszeit

(b) Genauigkeit Casia-I

(c) Genauigkeit Casia-L

(d) Genauigkeit ND

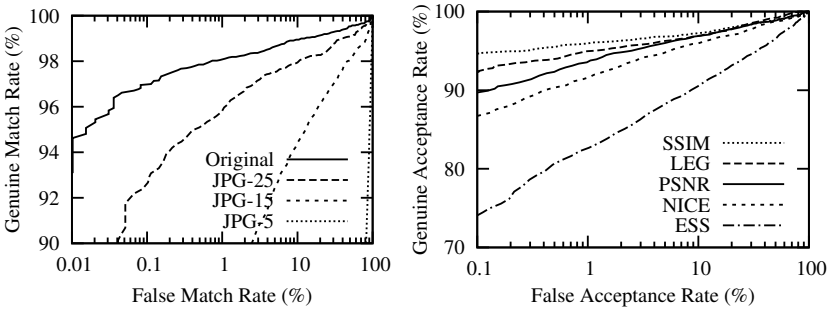
Abbildung 5: Verarbeitungszeit vs. Genauigkeit vorgeschlagener Segmentierung [UW12c, UW12b].

Wie aus Tab. 1 ersichtlich liefert die vorgeschlagene Gaussian Face-part Classifier Fusion (FFF) mit 96.4% Augen-Detektionsrate auf Casia-D und 99.2% auf YaleB beste Ergebnisse im Vergleich zu geschachtelter (Nested) bzw. individueller (Eye-only) Detektion. Auch wird nur dann signifikant mehr Verarbeitungszeit (1.28 s vs. 0.65 s) erfordert, wenn ein Neudurchlauf aufgrund zu naher Aufnahme durchgeführt werden muss. Auch die entwickelten Segmentierungsmethoden WAHET und IFPP weisen bessere Ergebnisse als die verbreitete Open Source Software OSIRIS auf (WAHET: 1.2% EER vs. 16.4% EER auf Casia-I, 4.36% EER vs. 14.89% EER auf Casia-L, 12.9% EER vs. 15.45% EER auf ND) und benötigen nur einen Bruchteil der Verarbeitungszeit (WAHET: 0.21–0.26 s vs. 3.46–6.27 s). Tabelle 3 listet Einzelergebnisse, Abbildung 5 die Grenzwertoptimierungskurven und Durchlaufzeiten. Eine Analyse der Auswirkung von Kompression auf Segmentierungsgenauigkeit ergab deutliche Beeinflussung (siehe Abb. 6).

Mit alignment-optimierten Komparatoren lässt sich die Gleichfehlerrate (EER) um 9-27% je nach Komparator und Merkmal verbessern, siehe Tab. 2. Während die Performance bei GSF und SSF im Bereich der HD liegt, wird der Performance-Vorteil von CLD mit im Schnitt 4-5 mal höheren Vergleichszeiten erkauft. Allerdings lässt sich durch die Wahl des Shifts die Genauigkeit bzw. Geschwindigkeit steuern, siehe Abb. 7. Mittels IIR lassen sich im Identifikationsmodus die Vergleiche auf 5% (!) ohne Einbußen an Genauigkeit reduzieren. Bildmetriken liefern Genauigkeiten von 3-10% EER und können erfolgreich mit Komparatoren fusioniert werden.

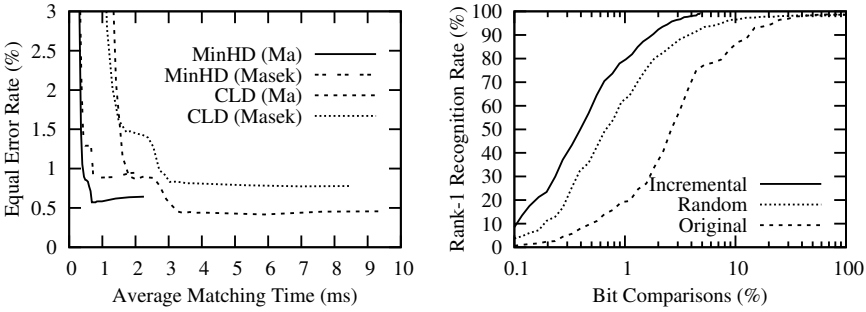
Tabelle 3: Segmentierung: EER und Segmentierungszeit (in Sekunden pro Bild) [UW12c, UW12b].

Algo.	Gleichfehlerrate (EER)				Zeit			
	Casia-I	Casia-L	ND	Ubiris	Casia-I	Casia-L	ND	Ubiris
OSIRIS	16.40%	14.89%	15.45%	33.51%	3.46 s	6.21 s	6.27 s	2.03 s
IFPP	8.07%	12.90%	19.04%	34.56%	0.18 s	0.46 s	0.48 s	0.11 s
WAHET	1.20%	4.36%	12.90%	-	0.21 s	0.26 s	0.25 s	-



(a) Kompression (b) Metriken

Abbildung 6: (a) Auswirkung von Kompression auf Segmentierung, (b) Genauigkeit von Irismetriken [RUW12b, HRUW12b].



(a) CLD-Operator (b) IIR-Operator

Abbildung 7: Verarbeitungszeit vs. Genauigkeit für vorgeschlagene Komparatoren [RUW10, UW10].

5 Zusammenfassung

Irisbiometrie-Technologien konnten sich erfolgreich in wohldefinierten kooperativen Umgebungen etablieren und werden im weltgrößten Biometriesystem Aadhaar zur Identifikation der indischen Bevölkerung eingesetzt. In Überwachungsumgebungen stellen sich jedoch neue Herausforderungen an Segmentierungsgenauigkeit sowie Echtzeitfähigkeit, welche das effiziente Zusammenspiel aller involvierten Module erfordern. Diese Arbeit

widmete sich neuen Lokalisationsalgorithmen unter Berücksichtigung der Kriterien Genauigkeit, Unabhängigkeit von Sensoren und Geschwindigkeit. Ebenso wurden zahlreiche neue Iris-Komparatoren vorgestellt mit dem Ziel eine höhere Bandbreite an Flexibilität für die anwendungsbezogene Auswahl unter Abwägung von Geschwindigkeit und Genauigkeit zur Verfügung zu stellen.

Literatur

[CFV08] J. Cauchie, V. Fiolet und D. Villers. Optimization of an Hough transform algorithm for the search of a center. *Pattern Recognition*, 41(2):567–574, 2008.

[Dau04] J. Daugman. How iris recognition works. *IEEE Trans. on Circuits and Systems for Video Technology*, 14(1):21–30, 2004.

[HBF09] K. P. Hollingsworth, K. W. Bowyer und P. J. Flynn. The Best Bits in an Iris Code. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 31(6):964–973, 2009.

[HRUW12a] H. Hofbauer, C. Rathgeb, A. Uhl und P. Wild. Image Metric-based Biometric Comparators: A Supplement to Feature Vector-based Hamming Distance? In *Proc. IEEE Int'l Conf. of the Biometrics Special Interest Group (BIOSIG'12)*, Jgg. 196 of *LNI*, 5 pages, Darmstadt, Germany, September 6–7, 2012. GI.

[HRUW12b] H. Hofbauer, C. Rathgeb, A. Uhl und P. Wild. Iris Recognition in Image Domain: Quality-metric based Comparators. In G. Bebis et al., Hrsg., *Proc. 8th Int'l Symposium on Visual Computing (ISVC'12)*, Jgg. 7432 of *LNCS*, Seiten 1–10, Crete, Greece, July 16–18, 2012. Springer.

[KSUW10] M. Konrad, H. Stögner, A. Uhl und P. Wild. Computationally efficient serial combination of rotation-invariant and rotation compensating iris recognition algorithms. In *Proc. 5th Int'l Conf. on Computer Vision Theory and Applications (VISAPP'10)*, Jgg. 1, Seiten 85–90, Angers, France, May 17–21, 2010. SciTePress.

[MR81] C. S. Myers und L. R. Rabiner. A comparative study of several dynamic time-warping algorithms for connected word recognition. *The Bell System Technical Journal*, 60(7):1389–1409, 1981. Bell Labs.

[Pro10] H. Proença. Iris Recognition: On the Segmentation of Degraded Images Acquired in the Visible Wavelength. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 32(8):1502–1516, 2010.

[RUW10] C. Rathgeb, A. Uhl und P. Wild. Incremental Iris Recognition: A Single-algorithm Serial Fusion Strategy to Optimize Time Complexity. In *Proc. IEEE 4th Int'l Conf. on Biometrics: Theory, Applications, and Systems (BTAS'10)*, 6 pages, Washington, DC, USA, September 27–29, 2010. IEEE.

[RUW11a] C. Rathgeb, A. Uhl und P. Wild. Iris-Biometric Comparators: Minimizing Trade-Offs Costs between Computational Performance and Recognition Accuracy. In *Proc. 4th Int'l Conf. on Imaging for Crime Detection and Prevention (ICDP'11)*, 6 pages, London, UK, November 3–4, 2011. IET.

[RUW11b] C. Rathgeb, A. Uhl und P. Wild. Reliability-balanced Feature Level Fusion for Fuzzy Commitment Scheme. In *Proc. 1st Int'l Joint Conf. on Biometrics (IJCB'11)*, 7 pages, Washington, DC, USA, October 10–13, 2011. IEEE.

[RUW11c] C. Rathgeb, A. Uhl und P. Wild. Shifting Score Fusion: On Exploiting Shifting Variation in Iris Recognition. In *Proc. 26th ACM Symposium On Applied Computing (SAC'11)*, Seiten 3–7, TaiChung, Taiwan, March 21–24, 2011. ACM.

[RUW12a] C. Rathgeb, A. Uhl und P. Wild. Iris-Biometric Comparators: Exploiting Comparison Scores towards an Optimal Alignment under Gaussian Assumption. In *Proc. 5th Int'l Conf. on Biometrics (ICB'12)*, 6 pages, New Delhi, India, March 29–April 1, 2012. IEEE.

[RUW12b] C. Rathgeb, A. Uhl und P. Wild. *Iris Recognition: From Segmentation to Template Security*, Jgg. 59 of *Advances in Information Security*. Springer, New York, 2012. ISBN 978-1-4614-5570-7.

[UW09] A. Uhl und P. Wild. Single-sensor multi-instance fingerprint and eigenfinger recognition using (weighted) score combination methods. *Int'l Journal on Biometrics*, 1(4):442–462, 2009.

[UW10] A. Uhl und P. Wild. Enhancing Iris Matching Using Levenshtein Distance with Alignment Constraints. In George Bebis et al., Hrsg., *Proc. 6th Int'l Symposium on Advances in Visual Computing (ISVC'10)*, Jgg. 6453 of *LNCS*, Seiten 469–479, Las Vegas, NV, USA, November 29–December 1, 2010. Springer.

[UW12a] A. Uhl und P. Wild. Combining Face with Face-Part Detectors under Gaussian Assumption. In A. Campilho und M. Kamel, Hrsg., *Proc. 9th Int'l Conf. on Image Analysis and Recognition (ICIAR'12)*, Jgg. 7325 of *LNCS*, Seiten 80–89, Aveiro, Portugal, June 25–27, 2012. Springer.

[UW12b] A. Uhl und P. Wild. Multi-stage Visible Wavelength and Near Infrared Iris Segmentation Framework. In A. Campilho und M. Kamel, Hrsg., *Proc. 9th Int'l Conf. on Image Analysis and Recognition (ICIAR'12)*, Jgg. 7325 of *LNCS*, Seiten 1–10, Aveiro, Portugal, June 25–27, 2012. Springer.

[UW12c] A. Uhl und P. Wild. Weighted Adaptive Hough and Ellipsopolar Transforms for Real-time Iris Segmentation. In *Proc. 5th Int'l Conf. on Biometrics (ICB'12)*, 8 pages, New Delhi, India, March 29–April 1, 2012. IEEE.

[VJ01] P. Viola und M. Jones. Rapid Object Detection Using a Boosted Cascade of Simple Features. In *Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR'01)*, Seiten 511–518, Kauai, HI, USA, December 8–14, 2001. IEEE.

[Wil12] P. Wild. *Advanced Segmentation and Comparators for Iris Biometric Surveillance*. Dissertation, University of Salzburg, 2012.



Peter Wild ist Postdoc am Fachbereich Computerwissenschaften der Universität Salzburg, Österreich. Er erhielt den Diplom-Ingenieur in Angewandter Informatik von der Universität Salzburg, wo er auch seine Dissertation zu "Advanced Segmentation and Comparators for Iris Biometric Surveillance" verfasste. Er ist Autor der Monografie "Iris Recognition: From Segmentation to Template Security", Springer 2012 und fungiert als Lehrbeauftragter an der Universität Salzburg, Fachhochschule Salzburg, sowie Pädagogischen Hochschule Salzburg. Seine Forschungsinteressen umfassen Bildverarbeitung (mit Fokus Objekterkennung), Biometrie (mit Fokus Iriserkennung) und Mediensicherheit.

Analyse molekularbiologischer Daten mittels Self-organizing Maps

Dr. rer. nat. Henry Wirth

Interdisziplinäres Zentrum für Bioinformatik, Universität Leipzig
LIFE Forschungszentrum für Zivilisationserkrankungen, Universität Leipzig
Helmholtz-Zentrum für Umweltforschung, Leipzig
wirth@izbi.uni-leipzig.de

Abstract: Die Molekularbiologie sieht sich gegenwärtig mit enormen Datenmengen konfrontiert, welche durch moderne Hochdurchsatzmessungen wie Microarrays oder Sequenzierung erzeugt werden. Etablierte Methoden zur Datenanalyse erweisen sich zumeist als ungeeignet für solch hochdimensionale, komplexe und meist verrauschte Daten.
Wir stellen hier kurz unsere Analysestrategie vor, welche essenzielle Methoden wie Dimensionsreduzierung, Clustering, multidimensionales Skalieren und Visualisierung vereint und zudem eine in hohem Maße intuitive Sicht auf die Daten erlaubt.

1 Einführung

Die moderne Molekularbiologie sieht sich gegenwärtig mit enormen Datenmengen konfrontiert. Immer geringer werdende Kosten für Hochdurchsatz-Analysen wie Microarrays, Sequenzierung oder Massenspektrometrie führten in den letzten Jahren zu einer Explosion der Menge an produzierten und in Datenbanken verfügbaren molekularbiologischen Daten. Die erhobenen Datensätze umfassen dabei oft mehrere hundert Proben mit mehreren zehntausend, teilweise millionen gemessenen Merkmalen (sog. Features) je Probe. Für die bioinformatische Auswertung sind solche Datenfluten eine große Herausforderung und erfordern optimale Analysestrategien.
Besonders wichtige aber auch komplizierte Aufgabenstellungen wie die Vorverarbeitung der Rohdaten, ihre passende Evaluierung und Wichtung entsprechend ihres Einflusses auf die Biologie und geeignete Methoden zur Auswahl und Interpretation relevanter Features beschäftigen die moderne Bioanalytik. Viele weit verbreitete Methoden wie Cluster-Heatmaps, Balken- oder Streu-Diagramme geben schnell und intuitiv Überblick über die Daten. Andererseits repräsentieren viele der etablierten und einfachen Ansätze den multivariaten Charakter der Daten nur ungenügend, sodass für das Verständnis des untersuchten Systems wichtige Informationen verborgen bleiben können. Mehr noch, die moderne Medizin und Zellbiologie verlangt die individuelle Analyse jeder Probe. Dies erfordert ein Portraitieren der Datenlandschaft jedes einzelnen Patienten oder jeder einzelnen Zelle und das Ausarbeiten individueller Unterschiede beispielsweise in Folge verschiedener Behandlungen oder von Entwicklungsprozessen.

Geeignete Analysestrategien umfassen in diesem Zusammenhang aufeinander abgestimmte Visualisierungen der Messwerte und der Ergebnisse. Die beiden Sichten auf die Daten, entweder Proben- oder Feature-basiert, sollten in geeigneter Weise kombiniert werden und so die Besonderheiten jeder einzelnen Probe in ihrem multivariaten Kontext zugänglich machen. Diese Selektion sogenannter Biomarker erfordert die Anwendung passender Statistiken zur Schätzung der Signifikanz sowie folgender Analysemethoden um den funktionellen Zusammenhang zu erschließen.
Einen besonderen Ansatz für die genannten Aufgaben stellen die Methoden des maschinellen Lernens dar. Besonders neuronale Netze wie die selbstorganisierenden Karten (engl. self-organizing maps, SOMs) kombinieren effektive Verarbeitung und Reduktion großer Datenmengen mit einzigartigen Visualisierungsmöglichkeiten. SOMs bieten daher ein passendes Herzstück um große und komplexe Datensätze detailliert zu untersuchen. Die vorliegende Arbeit soll nun unsere Analysestrategie auf Basis SOM-verarbeiteter molekularbiologischer Daten kurz zusammenfassen und ihre Anwendung auf verschiedene experimentelle Systeme sowie Messmethoden illustrieren.

2 SOM Portraitierung und Datenkompression

Das von uns entworfene und implementierte Softwarepaket umfasst zehn Module, welche jeweils individuell angepasste und integrierte Methoden enthalten. Die Module können grob in drei Abschnitte eingeteilt werden (siehe Abbildung 1, rechte Seite): Verarbeitung der Einzel-Features, Analysen auf Basis der Meta-Features und Analysen der Fleckenmuster der Proben-Portraits. Die Vorverarbeitung wandelt die Rohdaten in Trainingsdaten für das maschinelle Lernen um. Dabei sollen technisch bedingte Verzerrungen und Artefakte entfernt und die Vergleichbarkeit der Proben gewährleistet werden. Je nach Messmethode werden dabei unterschiedliche Kalibrierungs- und Normalisierungsalgorithmen angewendet.
Die vorverarbeiteten Daten liegen dann als Feature-Matrix der Dimension N x M vor (siehe Abbildung 1a), wobei N die Anzahl der Features bezeichnet, die je Probe gemessen werden, und M die Anzahl der Proben (z.B. Patienten, unterschiedliche Behandlungen oder verschiedene Zeitpunkte) im Datensatz. Dabei ist N typischerweise um Größenordnungen größer als M. Die Zeilen der Datenmatrix werden als Profile der Features bezeichnet, die Spalten als Zustder Proben. Ziel des SOM Lernens ist nun die Reduktion der Zahl der relevanten Features. Dies wird durch eine Sortierung und Gruppierung ähnlicher Feature-Profile erreicht. Dabei wir die Eingangs-Datenmatrix in eine sogenannte Meta-Datenmatrix überführt welche eine wesentlich geringere Anzahl an Meta-Features enthält (Abbildung 1b). Anders ausgedrückt projiziert die SOM den hochdimensionalen Eingangsdatenraum auf einen Meta-Datenraum geringerer Dimension. Dadurch wird der Datenraum in Gruppen ähnlicher Feature-Profile segmentiert, welche zu je einem Meta-Feature gehören. Dieses Feature-Mapping ist in Abbildung 1a und b durch rote Linien dargestellt. Die von uns verwendete Standard-SOM verwendet dazu K in einem zweidimensionalen Raster angeordnete Knoten, hinter jedem sich ein Meta-Feature repräsentiert durch ein Profil der Länge M verbirgt.

Die Spalten der Meta-Datenmatrix, die Meta-Zustände der Proben, können durch geeignete Färbung der entsprechenden Werte (rot=hohe Werte, grün=mittlere Werte, blau=niedrige Werte) als intuitive Mosaikbilder mit charakteristischen Fleckenmustern visualisiert werden (siehe auch Abbildungen 2-4). Dabei ist besonders bemerkenswert, dass diese zweidimensionalen Portraits die multivariate Datenlandschaft detailgetreu widergeben und daher alternative Visualisierungsmethoden wie die beliebten, jedoch univariaten Heatmaps ausstechen. Der SOM Algorithmus assoziiert ähnliche Feature-Profile, welche zum gleichen Hauptmodul der Variabilität gehören, zum gleichen beziehungsweise zu benachbarten Meta-Features, wogegen unabhängige Features zu entfernteren Meta-Features assoziiert werden. Durch diese Eigenschaft des SOM Algorithmus ergeben sich intuitive Fleckenmuster mit gleichmäßigen Farbverläufen und roten bzw. blauen fleckenartigen Regionen, welche jeweils Gruppen von Features mit besonders hohen bzw. niedrigen Werten repräsentieren (Abbildung 1c). Meta-Features, und damit auch alle assoziierte Einzelfeatures, können als koreguliert betrachtet werden, wogegen separierte Flecken verschiedene regulatorische Moden repräsentieren. Dieser globale Blick auf die Feature-Landschaft spiegelt die multivariate Kovarianzstruktur der Daten wieder und ist wesentlich intuitiver als das Suchen nach Unterschieden zwischen den Proben in sortierten Listen hunderter Einzelfeatures, wie sie Standardanalysen produzieren. Daher können die Flecken-Module als natürliche Wahl angesehen werden wenn es darum geht, kontextbezogene Muster in komplexen Datensätzen zu identifizieren.
Es ist wichtig zu erwähnen, dass dieses Zerlegen der Meta-Features in koregulierte Module neben dem SOM Lernen eine zweite Ebene der Datenkompression darstellt. Beispielsweise werden die mehr als 20,000 Gene eines Transkriptom-Datensatzes mit knapp 70 Proben menschlicher Gewebe durch den SOM Algorithmus auf 60 x 60 = 3,600 Meta-Gene reduziert [WLvBB11]. In den entsprechenden Portraits ließen sich ein Dutzend unterschiedliche Flecken-Module identifizieren. Somit wurde die Datenmenge um etwa drei Größenordnungen reduziert, ohne dabei in irgendeiner Weise Primärinformationen zu verlieren. Denn anders als bei Filter-Methoden wird dies durch eine Wichtung und Aggregation der gesamten Information erreicht. Sie ist auch nach der Transformation noch vollständig in den Meta-Daten enthalten und kann in nachgeschalteten Analysen wieder abgerufen werden.

3 Information Mining

Die Erste der Analysen auf Basis der Meta-Daten zielt auf das Identifizieren der Module potentiell koregulierter Features ab (Abbildung 1c). Wir verwenden dazu verschiedene Metriken: Erstens können Regionen mit besonders hohen bzw. niedrigen Werten (also besonders rote bzw. blaue Meta-Features) durch Anwenden eines einfachen Perzentil-Kriteriums identifiziert werden. Zweitens können etablierte Clusterverfahren wie zum Beispiel k-Means angewendet werden, um den durch die SOM aufgespannten Raum zu segmentieren. Zusätzliche Supporting Maps visualisieren verschiedene wichtige Eigenschaften der SOM und der Meta-Datenlandschaft, wie etwa Überblickskarten welche sämtliche identifizierten Flecken enthalten, eine Populationskarte welche die Anzahl der assoziier-

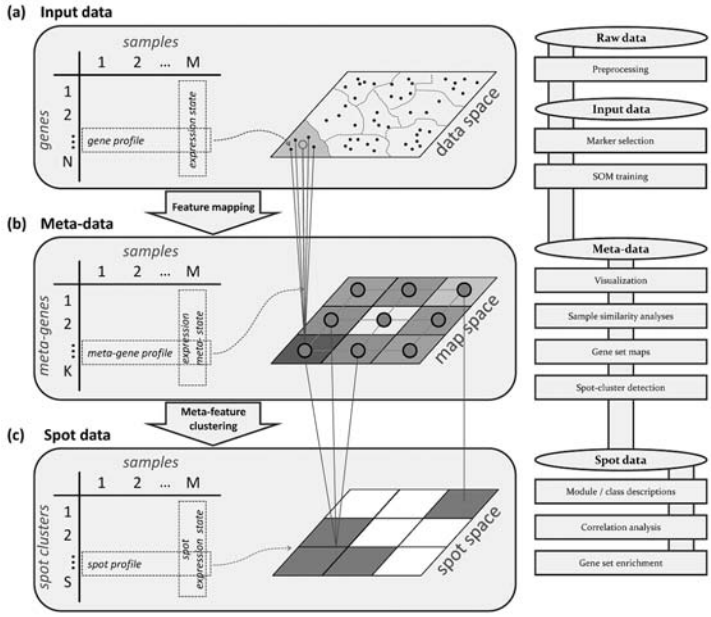


Abbildung 1: Zweistufige Datenkompression bei Anwendung des SOM Lernens: Zunächst werden die Eingangsdaten in Meta-Daten transformiert, danach werden die Meta-Daten anhand der charakteristischen Fleckenmuster gruppiert. Auf der rechten Seite ist der Ablaufplan der gesamten Analyse illustriert.

ten Einzelfeatures pro Meta-Feature aufzeigt, oder Varianz- und Entropiekarten der Meta-Feature Profile. Information Mining im engeren Sinne beinhaltet Fragestellungen wie Biomarker Selektion, das Klassifizieren der Proben und das Einbeziehen funktioneller Analysen. Die SOM Methodik erlaubt es uns nun solche Aufgaben auf den komprimierten Daten auszuführen. Wir konnten zeigen, dass dies im Vergleich zu Analysen auf Basis der unkomprimierten Daten nicht nur Vorteile bei Rechenzeit- und Speicherplatzbedarf bietet, sondern auch die Ergebnisse in Bezug auf Sensitivität und Spezifität verbessert [WLvBB11]. Daher wurde eine Reihe etablierter statistischer Methoden für die Anwendung auf die Meta-Daten angepasst und implementiert um Aufgaben wie Marker Selektion, Ähnlichkeits-und Klassenanalysen der Proben oder funktionelle Analysen der differentiellen Muster zu realisieren [WvBB12].

4 Anwendungsbeispiele

In diesem Abschnitt soll die SOM Analyse anhand dreier ausgewählter Anwendungsbeispiele illustriert werden. Diese wurden stellvertretend für verschiedene 'OMe' (Transkriptom, Genom, Proteom) und verschiedene experimentelle Designs (Entwicklungsserien,

weltweite Populationskohorte und Proben unterschiedlicher Taxa) ausgewählt.

4.1 Transkriptomdynamik des Hefezyklus aus Sicht der SOM Expressionsportraits

Der Stoffwechselzyklus der Backhefe (engl. 'yeast metabolic cycle', YMC) ist eines der am besten untersuchten Modelle der molekularbiologischen Forschung. Wir nutzen dieses Wissen um unsere SOM Methodik in Bezug auf Dynamiken der Genexpression zu evaluieren. Während des etwa 45minütigen Zyklus' wurden die Expressionslevel von knapp 6,000 Genen der Hefe in Zeitintervallen von 4 Minuten gemessen [LK06]. Jede der 11 Proben (t1 - t11) wurde in ein Expressionsportrait transformiert, welches rote und blaue Flecken entsprechend über- und unterexprimierten (Meta-)Genen enthält (siehe Abbildung 2a). Diese Flecken scheinen gegen den Uhrzeigersinn entlang der Ränder der Portraits zu rotieren und spiegeln somit den gleitenden Übergang der transkriptionellen Zustände zwischen den jeweiligen Zeitpunkten wieder. Die Heatmap in Abbildung 2b zeigt den Expressionsverlauf sechs identifizierter Flecken der Portraits (siehe die Bilder auf der linken Seite). Jeder der Flecken enthält konzertierte Meta-Gene, bzw. mit ihnen assoziierte Einzelgene, welche mit größer werdender Phasenverschiebung oszillieren. Die Analyse angereicherter Gensets erlaubt es uns nun jedem dieser regulatorischen Modulen sein transkriptionelles Programm im Kontext der Zellfunktionen zuzuordnen (Abbildung 2c). Interessanterweise liefert die SOM Portraitierung nicht nur mit den drei Hauptphasen des Zyklus' konsistente Ergebnisse [TKRM05]. Sie bietet auch eine verfeinerte Sichtweise auf die Dynamik des Transkriptoms. Die Expressionsprofile ausgewählter funktioneller Gensets sind in Abbildung 2d zu sehen. Auch auf dieser funktionellen Ebene ist das zyklisch oszillierende Verhalten sowie die phasenverschobene Zeitabhängigkeit der Genexpression detailliert analysierbar.

4.2 Genomportraits enthüllen Fußspuren der frühmenschlichen Völkerwanderung

Die genetische Diversität der Menschheit wird durch biologische als auch durch demografische Faktoren geformt und ihr Verständnis ist fundamental für die detaillierte Untersuchung der genetischen Grundlagen verschiedenster Krankheiten. In dieser Anwendung haben wir die SNP (= 'single nucleotide polymorphism') Landschaften von über 1,000 Menschen aus 57 ethnischen Gruppierungen und 7 geographischen Regionen untersucht. Die Daten wurden durch das 'Human Genome Diversity Project' erhoben und beinhalten Informationen über mehr als 650,000 SNPs pro Individuum [LAT$^+$08]. Unser SOM Ansatz komprimiert diesen riesigen Datensatz mit erstaunlich hoher Auslösung auf 80 x80 = 6,400 'Meta-Allele'. Um den Datensatz für maschinelles Lernen verarbeitbar zu machen wurde ein ternärer Code verwendet: '0' für das häufigere und '2' für das seltenere homozygote Allel (blaue bzw. rote Färbung in den SOM Portraits), '1' für heterozygote Allele (grüne Färbung). Die von der SOM erzeugten Portraits jedes Individuums wurden entsprechend der geografischen Zugehörigkeit gemittelt (siehe Abbildung 3). Diese Regionen-Portraits spiegeln den lokalen SNP Mutationsstand in ihren charakteristischen Fleckenmustern wieder. Dabei divergiert die Ähnlichkeit der Portraits mit zunehmender

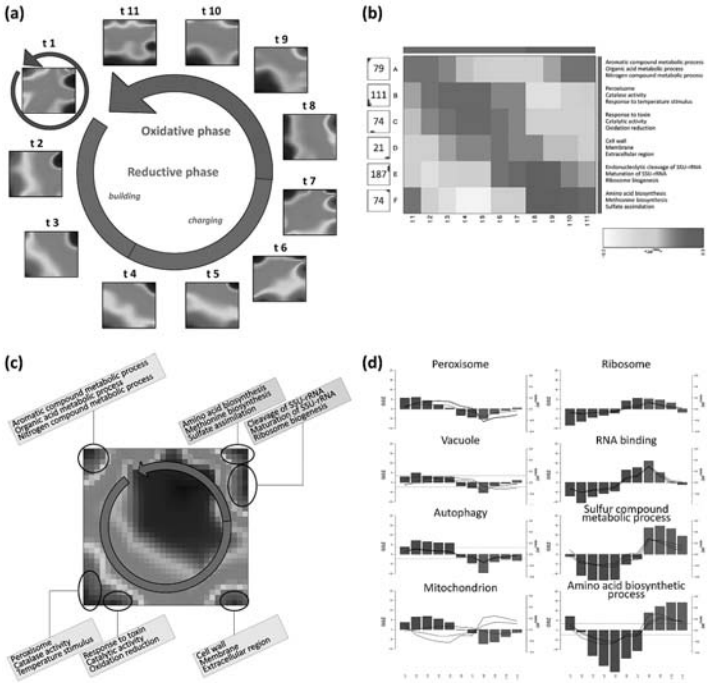


Abbildung 2: Portraits der Expressionsdynamik des Hefezyklus: (a) Die SOM Portraits der Proben spiegeln den zyklischen Charakter der Expressionslandschaften wieder. (b) Sechs verschiedene rote Flecken wurden in den Portraits identifiziert. Die Heatmap stellt deren Profile über die Zeitpunkte dar. Diese oszillieren, weisen jedoch verschiedene Zeitpunkte der maximalen Amplitude auf. (c) Die Überblickskarte sammelt alle überexprimierten (roten) Flecken und ordnet ihnen angereicherte funktionelle Gensets zu. (d) Die Expressionsprofile ausgewählter Gensets zeigen den Zeitverlauf verschiedener transkriptioneller Programme.

geografischer Entfernung der Populationen vom vermuteten Ursprung der Menschheit in Afrika. Diese Divergenz erfolgt jedoch nicht abrupt sondern als gleichmäßiger Übergang, was die zeitliche Veränderung der Mutations-Muster durch Migration einerseits und die genetische Isolation geografisch getrennter Populationen andererseits widerspiegelt. Bemerkenswerterweise durchbricht das Portrait von Ozeanien die Ähnlichkeitsregel benachbarter Regionen. Es zeigt vielmehr ein gesprenkeltes Muster mit vielen kleinen Flecken entlang der Ränder des Portraits. Die Einwohner Ozeaniens teilen sich demnach genetische Charakteristiken mit nahezu allen anderen Regionen. Dieses spezifische Muster deutet auf eine frühere Migrationswelle der Frühmenschen zusätzlich zur 'Out-of-Africa' Wanderung hin. Eine aktuelle Studie zeigte kürzlich, dass Melanesier und Papua im Vergleich zu den anderen nicht-afrikanischen Populationen genetische Ähnlichkeit mit den Neandertalern und den Denisova-Menschen aufweisen [RGK$^+$10]. Die wurde damit erklärt, dass die Frühmenschen möglicherweise in mehreren Wellen migrierten. Um die verschiedenartigen Fleckenmuster der ozeanischen Individuen zu erklären muss man sich verdeut-

lichen, dass die meisten anderen Populationen aus einer gemeinsamen Migrationswelle stammen. Diese große 'Kohorte' mit ihren überlappenden, weil kontinuierlich evolvierten SNP-Landschaften hat auch einen großen Anteil an der Formung des Meta-Datenraumes. Populationen einer anderen Migrationswelle, wie die Papua-Melanesier, passen in diese sequentiellen SNP-Zustände erwartungsgemäß in weit geringerem Maße und erzeugen ein stärker fragmentiertes Fleckenmuster. Andererseits führten Vermischungen mit den Genpools der angrenzenden Populationen Südostasiens dazu, dass einige ozeanische Individuen den asiatischen sehr ähnlich sind. Wir haben für die mehr als eintausend untersuchten Menschen einen Korrelations-Spannbaum erzeugt, in welchem Individuen mit der höchsten Korrelation ihrer SNP-Landschaften paarweise verbunden sind (Abbildung 3). Erstaunlicherweise passt dieser Baum sehr genau auf die heutige geografische Verteilung der Populationen. Doch auch interessante Details sind klar erkennbar. Die Afrikanischen Populationen lassen sich genau in zwei Zeige unterteilen: Jäger und Sammler (z.B. San und Pygmy) und Agrargesellschaften (Bantu, Yoruba). Populationen und Individuen aus dem mittleren Osten, Europa und Zentralasien vermischen sich teilweise entsprechend den komplexen Wanderungen im Laufe der Geschichte. In Ostasien bilden die Jakuten eine 'Brücke' zu den amerikanischen Ureinwohnern während die Kambodschaner zu den Populationen Ozeaniens verbunden sind. Diese Ergebnisse untermauern die Feststellung, dass Ähnlichkeiten zwischen den SNP-Landschaften mit zunehmender zeitlicher und räumlicher 'Entkopplung' der Populationen abnehmen [LAT+08]. Somit offenbaren die SOM Portraits und der Korrelations-Baum Fußspuren der frühmenschlichen Migration in unseren Genomen. Dieses Beispiel zeigt die Fähigkeit des SOM Lernens eine große Anzahl komplexer Genotypen zu verarbeiten und für intuitive und dennoch detaillierte Analysen aufzubereiten.

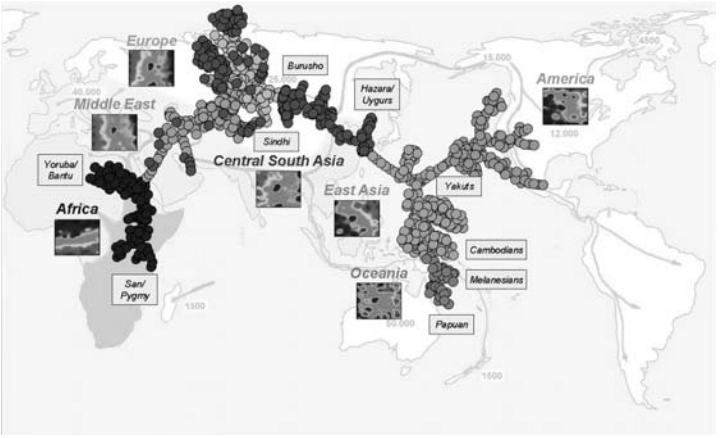


Abbildung 3: SOM Analyse der genetischen Diversität des Menschen: Der Korrelations-Spannbaum visualisiert die Ähnlichkeitsrelationen zwischen den SNP-Landschaften der Individuen. Jeder Kreis entspricht einem Individuum und ist nach geografischer Zugehörigkeit gefärbt. Jede der Regionen ist durch das mittlere SOM Portrait der entsprechenden Individuen repräsentiert und eindeutig charakterisiert. Die Struktur des Baumes spiegelt die gegenwärtige Hypothese der frühmenschlichen Verbreitung von Afrika aus wieder.

4.3 Proteom-Portraits der taxonomischen Verwandtschaftsverhältnisse von Drosophila

Massenspektrometrie (MS) ist neben Microarrays und Sequenzierung eine weitere Technologie, welche im Hochdurchsatzbereich enorme Mengen an Daten produziert und in der Proteomik und Metabolomik weit verbreitet ist. Dabei ist besonders die 'MALDI-ToF MS' Methode zu erwähnen, welche Informationen über Peptide und Proteine einer Probe in einem breiten Massenbereich liefert. Sie wird unter anderem als 'MALDI-typing' angewandt und ermöglicht die Klassifizierung der Proben anhand ihrer gesamten Spektralinformation und ohne die dahinterliegende Proteinzusammensetzung explizit zu kennen. In diesem Beispiel analysierten wir MALDI-ToF-Spektren von 125 Drosophila Exemplaren gehörend zu 13 verschiedenen Spezies [FGK+10]. Sogenannte 'Peak-Listen' von 208 Intensitäts-Amplituden je Probe wurden dafür aus den kontinuierlichen Spektren extrahiert und für das Training einer SOM mit 40 x 40 = 1,600 Meta-Features benutzt. Die meisten der pro Spezies gemittelten SOM Portraits weisen nur einen roten Fleck entsprechend Peaks mit hohen Intensitäten auf (Abbildung 4a). Die Position dieses roten Bereiches in den Portraits ist spezifisch für jede Spezies. Das bedeutet, dass es für jede Spezies charakteristische Bereiche in den Spektren gibt, welche nur in dieser eine hohe Intensitätsamplitude haben. Somit bietet unsere Portraitierung eine einfache und direkte M¨glichkeit diese 'MS-Fingerabdrücke' zu extrahieren. Auf Basis der Meta-Feature Landschaften wurde ein phylogenetischer Clusterbaum generiert (Abbildung 4a). Dieser weist sauber getrennte Äste auf, welche die allgemein anerkannte Phylogenie von Drosophila sehr gut widerspiegelt (vergleiche Abbildung 4b). Im Allgemeinen ist festzuhalten, dass phylogenetische Ähnlichkeit direkt mit Ähnlichkeit der Fleckenmuster in den SOM Portraits einhergeht. Einige der Portraits haben zwei rote Flecken, wobei einer oder beide mit der Charakteristik anderer Spezies Übereinstimmen. Zum Beispiel zeigen die Portraits von D. teissieri zwei Flecken an der Position, welche für D. mauritiana bzw. D. funebris spezifisch sind. Daher sind die D. teissieri Proben im phylogenetischen Baum an den Ästen zu finden, welche hauptsächlich mit letzteren beiden Taxa besetzt sind. Die Ursache dieser Spaltung der Protein-Landschaft ist jedoch unklar. Die Originalpublikation berichtet zwar von Problemen bei der Annotation von Teilen der D. teissieri Proben, geht aber nicht auf Details ein [FGK+10]. Andererseits wird das hohe Auflösungsvermögen der Meta-Feature Landschaften dadurch bestätigt, dass die beiden Spezies mit der geringsten evolutionären Distanz, D. miranda und D. speudoobscura mit weniger als 2 Millionen Jahren, im phylogenetischen Baum klar voneinander getrennt sind. Zu beachten ist, dass die Klassifizierung auf Basis der MS-Spektren als problematisch eingestuft wird [FGK+10]. Wie wir jedoch zeigen konnten erhöht die Transformation der Daten in Meta-Daten das Auflösungsvermögen und die Qualität von Klassifizierungen beim MALDI-Typing [WvBB12]. Somit hat sich unsere SOM Analyse auch in diesem schwierigen Teilgebiet verdient gemacht.

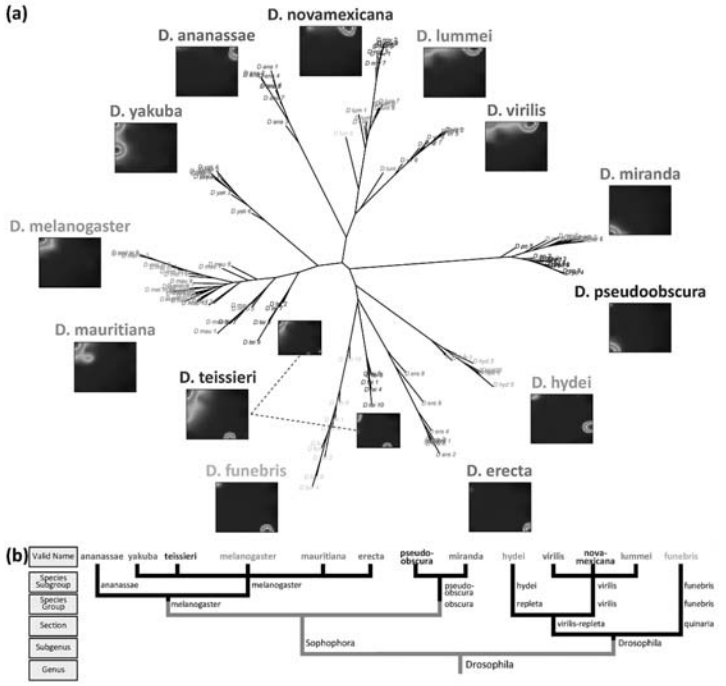


Abbildung 4: Portraitierung des Drosophila-Proteoms: (a) Der Ähnlichkeitsbaum der Drosophila Meta-Feature Landschaften wurde durch den 'Neighbor-Joining-Algorithmus' generiert. Mittlere SOM Portraits sind für jede taxonomische Gruppe aufgezeigt. Dabei beziehen sich rote Regionen auf Bereiche im Spektrum mit hohen Intensitäten. (b) Dendrogramm der Drosophila-Taxonomie (aus [FGK+10], bearbeitet).

5 Quintessenz

Methodische Aspekte der SOM Portraitierung wurden hier kurz vorgestellt. Sie zielen auf die gezielte Extraktion von Informationen aus großen und komplexen molekularbiologischen Datensätzen ab und stellen die Datenlandschaft sowie die Analyseergebnisse in ausgeklügelter Art und Weise dar. Die individuellen Portraits der Proben sind sehr elegant, da sie unverkennbare Fingerabdrücke der darunterliegenden Datenlandschaft darstellen. Dies ermöglicht eine dem Menschen intuitive Bild-basierte Sichtweise und fördert so die datengetriebene Analyse der Daten und die Generierung von Hypothesen. Die Dimension der ursprünglichen Daten wird stark reduziert und komplexe Meta-Daten für nachfolgende Analysen generiert. Dabei wird die Informationsvielfalt bewahrt und so exploratives und multivariates Vergleichen der Proben ermöglicht.

Literatur

[FGK+10] Ralph Feltens, Renate Görner, Stefan Kalkhof, Helke Gröger-Arndt und Martin von Bergen. Discrimination of different species from the genus Drosophila by intact protein profiling using matrix-assisted laser desorption ionization mass spectrometry. *BMC evolutionary biology*, 10:95, Januar 2010.

[LAT+08] Jun Z Li, Devin M Absher, Hua Tang, Audrey M Southwick, Amanda M Casto, Sohini Ramachandran, Howard M Cann, Gregory S Barsh, Marcus Feldman, Luigi L Cavalli-Sforza und Richard M Myers. Worldwide human relationships inferred from genome-wide patterns of variation. *Science (New York, N.Y.)*, 319(5866):1100–4, Februar 2008.

[LK06] Caroline M Li und Robert R Klevecz. A rapid genome-scale response of the transcriptional oscillator to perturbation reveals a period-doubling path to phenotypic change. *Proceedings of the National Academy of Sciences of the United States of America*, 103(44):16254–9, Oktober 2006.

[RGK+10] David Reich, Richard E Green, Martin Kircher, Johannes Krause, Nick Patterson, Eric Y Durand, Bence Viola, Adrian W Briggs, Udo Stenzel, Philip L F Johnson, Tomislav Maricic, Jeffrey M Good, Tomas Marques-Bonet, Can Alkan, Qiaomei Fu, Swapan Mallick, Heng Li, Matthias Meyer, Evan E Eichler, Mark Stoneking, Michael Richards, Sahra Talamo, Michael V Shunkov, Anatoli P Derevianko, Jean-Jacques Hublin, Janet Kelso, Montgomery Slatkin und Svante Pääbo. Genetic history of an archaic hominin group from Denisova Cave in Siberia. *Nature*, 468(7327):1053–60, Dezember 2010.

[TKRM05] Benjamin P Tu, Andrzej Kudlicki, Maga Rowicka und Steven L McKnight. Logic of the yeast metabolic cycle: temporal compartmentalization of cellular processes. *Science (New York, N.Y.)*, 310(5751):1152–8, November 2005.

[WLvBB11] Henry Wirth, Markus Loffler, Martin von Bergen und Hans Binder. Expression cartography of human tissues using self organizing maps. *BMC Bioinformatics*, 12(1):306, 2011.

[WvBB12] Henry Wirth, Martin von Bergen und Hans Binder. Mining SOM expression portraits: feature selection and integrating concepts of molecular function. *BioData mining*, 5(1):18, Oktober 2012.



Dr. Henry Wirth, geboren am 05.10.1982 in Meerane, studierte von 2002 bis 2008 Informatik mit Vertiefungsrichtung 'Künstliche Intelligenz' an der TU Chemnitz. Nach bestandenem Diplom erhielt er ein Doktorats-Stipendium vom Helmholtz-Zentrum für Umweltforschung in Leipzig in Kooperation mit dem Interdisziplinären Zentrum für Bioinformatik der Universität Leipzig. Seine Promotion wurde 2012 mit dem Prädikat 'summa cum laude' vollzogen. Seitdem ist er als Postdoc am Zentrum für Bioinformatik tätig und ist dabei unter anderem in verschiedene Projekte im Kontext von Gliomen und Lymphomen involviert.

GI-Edition Lecture Notes in Informatics

Dissertations

Vol. D-1: Ausgezeichnete Informatikdissertationen 2000
Vol. D-2: Ausgezeichnete Informatikdissertationen 2001
Vol. D-3: Ausgezeichnete Informatikdissertationen 2002
Vol. D-4: Ausgezeichnete Informatikdissertationen 2003
Vol. D-5: Ausgezeichnete Informatikdissertationen 2004
Vol. D-6: Ausgezeichnete Informatikdissertationen 2005
Vol. D-7: Ausgezeichnete Informatikdissertationen 2006
Vol. D-8: Ausgezeichnete Informatikdissertationen 2007
Vol. D-9: Ausgezeichnete Informatikdissertationen 2008
Vol. D-10: Ausgezeichnete Informatikdissertationen 2009
Vol. D-11: Ausgezeichnete Informatikdissertationen 2010
Vol. D-12: Ausgezeichnete Informatikdissertationen 2011
Vol. D-13: Ausgezeichnete Informatikdissertationen 2012

P-1 Gregor Engels, Andreas Oberweis, Albert Zündorf (Hrsg.): Modellierung 2001.

P-2 Mikhail Godlevsky, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications, ISTA'2001.

P-3 Ana M. Moreno, Reind P. van de Riet (Hrsg.): Applications of Natural Lan-guage to Information Systems, NLDB'2001.

P-4 H. Wörn, J. Mühling, C. Vahl, H.-P. Meinzer (Hrsg.): Rechner- und sensorgestützte Chirurgie; Workshop des SFB 414.

P-5 Andy Schürr (Hg.): OMER – Object-Oriented Modeling of Embedded Real-Time Systems.

P-6 Hans-Jürgen Appelrath, Rolf Beyer, Uwe Marquardt, Heinrich C. Mayr, Claudia Steinberger (Hrsg.): Unternehmen Hochschule, UH'2001.

P-7 Andy Evans, Robert France, Ana Moreira, Bernhard Rumpe (Hrsg.): Practical UML-Based Rigorous Development Methods – Countering or Integrating the extremists, pUML'2001.

P-8 Reinhard Keil-Slawik, Johannes Magenheim (Hrsg.): Informatikunterricht und Medienbildung, INFOS'2001.

P-9 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Innovative Anwendungen in Kommunikationsnetzen, 15. DFN Arbeitstagung.

P-10 Mirjam Minor, Steffen Staab (Hrsg.): 1st German Workshop on Experience Management: Sharing Experiences about the Sharing Experience.

P-11 Michael Weber, Frank Kargl (Hrsg.): Mobile Ad-Hoc Netzwerke, WMAN 2002.

P-12 Martin Glinz, Günther Müller-Luschnat (Hrsg.): Modellierung 2002.

P-13 Jan von Knop, Peter Schirmbacher and Viljan Mahni_ (Hrsg.): The Changing Universities – The Role of Technology.

P-14 Robert Tolksdorf, Rainer Eckstein (Hrsg.): XML-Technologien für das Semantic Web – XSW 2002.

P-15 Hans-Bernd Bludau, Andreas Koop (Hrsg.): Mobile Computing in Medicine.

P-16 J. Felix Hampe, Gerhard Schwabe (Hrsg.): Mobile and Collaborative Business 2002.

P-17 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Zukunft der Netze –Die Verletzbarkeit meistern, 16. DFN Arbeitstagung.

P-18 Elmar J. Sinz, Markus Plaha (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2002.

P-19 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund.

P-20 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund (Ergänzungsband).

P-21 Jörg Desel, Mathias Weske (Hrsg.): Promise 2002: Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen.

P-22 Sigrid Schubert, Johannes Magenheim, Peter Hubwieser, Torsten Brinda (Hrsg.): Forschungsbeiträge zur "Didaktik der Informatik" – Theorie, Praxis, Evaluation.

P-23 Thorsten Spitta, Jens Borchers, Harry M. Sneed (Hrsg.): Software Management 2002 – Fortschritt durch Beständigkeit

P-24 Rainer Eckstein, Robert Tolksdorf (Hrsg.): XMIDX 2003 – XML-Technologien für Middleware – Middleware für XML-Anwendungen

P-25 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Commerce – Anwendungen und Perspektiven – 3. Workshop Mobile Commerce, Universität Augsburg, 04.02.2003

P-26 Gerhard Weikum, Harald Schöning, Erhard Rahm (Hrsg.): BTW 2003: Datenbanksysteme für Business, Technologie und Web

P-27 Michael Kroll, Hans-Gerd Lipinski, Kay Melzer (Hrsg.): Mobiles Computing in der Medizin

P-28 Ulrich Reimer, Andreas Abecker, Steffen Staab, Gerd Stumme (Hrsg.): WM 2003: Professionelles Wissensmanagement – Er-fahrungen und Visionen

P-29 Antje Düsterhöft, Bernhard Thalheim (Eds.): NLDB'2003: Natural Language Processing and Information Systems

P-30 Mikhail Godlevsky, Stephen Liddle, Heinrich C. Mayr (Eds.): Information Systems Technology and its Applications

P-31 Arslan Brömme, Christoph Busch (Eds.): BIOSIG 2003: Biometrics and Electronic Signatures

P-32 Peter Hubwieser (Hrsg.): Informatische Fachkonzepte im Unterricht – INFOS 2003

P-33 Andreas Geyer-Schulz, Alfred Taudes (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft

P-34 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 1)

P-35 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 2)

P-36 Rüdiger Grimm, Hubert B. Keller, Kai Rannenberg (Hrsg.): Informatik 2003 – Mit Sicherheit Informatik

P-37 Arndt Bode, Jörg Desel, Sabine Rathmayer, Martin Wessner (Hrsg.): DeLFI 2003: e-Learning Fachtagung Informatik

P-38 E.J. Sinz, M. Plaha, P. Neckel (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2003

P-39 Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.): IT-Incident Management & IT-Forensics – IMF 2003

P-40 Michael Rebstock (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2004

P-41 Uwe Brinkschulte, Jürgen Becker, Dietmar Fey, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle, Thomas Runkler (Edts.): ARCS 2004 – Organic and Pervasive Computing

P-42 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Economy – Transaktionen und Prozesse, Anwendungen und Dienste

P-43 Birgitta König-Ries, Michael Klein, Philipp Obreiter (Hrsg.): Persistance, Scalability, Transactions – Database Mechanisms for Mobile Applications

P-44 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning. E-Services

P-45 Bernhard Rumpe, Wofgang Hesse (Hrsg.): Modellierung 2004

P-46 Ulrich Flegel, Michael Meier (Hrsg.): Detection of Intrusions of Malware & Vulnerability Assessment

P-47 Alexander Prosser, Robert Krimmer (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society

P-48 Anatoly Doroshenko, Terry Halpin, Stephen W. Liddle, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications

P-49 G. Schiefer, P. Wagner, M. Morgenstern, U. Rickert (Hrsg.): Integration und Datensicherheit – Anforderungen, Konflikte und Perspektiven

P-50 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 1) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-51 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 2) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-52 Gregor Engels, Silke Seehusen (Hrsg.): DELFI 2004 – Tagungsband der 2. e-Learning Fachtagung Informatik

P-53 Robert Giegerich, Jens Stoye (Hrsg.): German Conference on Bioinformatics – GCB 2004

P-54 Jens Borchers, Ralf Kneuper (Hrsg.): Softwaremanagement 2004 – Outsourcing und Integration

P-55 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): E-Science und Grid Adhoc-Netze Medienintegration

P-56 Fernand Feltz, Andreas Oberweis, Benoit Otjacques (Hrsg.): EMISA 2004 – Informationssysteme im E-Business und E-Government

P-57 Klaus Turowski (Hrsg.): Architekturen, Komponenten, Anwendungen

P-58 Sami Beydeda, Volker Gruhn, Johannes Mayer, Ralf Reussner, Franz Schweiggert (Hrsg.): Testing of Component-Based Systems and Software Quality

P-59 J. Felix Hampe, Franz Lehner, Key Pousttchi, Kai Ranneberg, Klaus Turowski (Hrsg.): Mobile Business – Processes, Platforms, Payments

P-60 Steffen Friedrich (Hrsg.): Unterrichtskonzepte für inforrmatische Bildung

P-61 Paul Müller, Reinhard Gotzhein, Jens B. Schmitt (Hrsg.): Kommunikation in verteilten Systemen

P-62 Federrath, Hannes (Hrsg.): „Sicherheit 2005“ – Sicherheit – Schutz und Zuverlässigkeit

P-63 Roland Kaschek, Heinrich C. Mayr, Stephen Liddle (Hrsg.): Information Systems – Technology and ist Applications

P-64 Peter Liggesmeyer, Klaus Pohl, Michael Goedicke (Hrsg.): Software Engineering 2005

P-65 Gottfried Vossen, Frank Leymann, Peter Lockemann, Wolffried Stucky (Hrsg.): Datenbanksysteme in Business, Technologie und Web

P-66 Jörg M. Haake, Ulrike Lucke, Djamshid Tavangarian (Hrsg.): DeLFI 2005: 3. deutsche e-Learning Fachtagung Informatik

P-67 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 1)

P-68 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 2)

P-69 Robert Hirschfeld, Ryszard Kowalcyk, Andreas Polze, Matthias Weske (Hrsg.): NODe 2005, GSEM 2005

P-70 Klaus Turowski, Johannes-Maria Zaha (Hrsg.): Component-oriented Enterprise Application (COAE 2005)

P-71 Andrew Torda, Stefan Kurz, Matthias Rarey (Hrsg.): German Conference on Bioinformatics 2005

P-72 Klaus P. Jantke, Klaus-Peter Fähnrich, Wolfgang S. Wittig (Hrsg.): Marktplatz Internet: Von e-Learning bis e-Payment

P-73 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): “Heute schon das Morgen sehen“

P-74 Christopher Wolf, Stefan Lucks, Po-Wah Yau (Hrsg.): WEWoRC 2005 – Western European Workshop on Research in Cryptology

P-75 Jörg Desel, Ulrich Frank (Hrsg.): Enterprise Modelling and Information Systems Architecture

P-76 Thomas Kirste, Birgitta König-Riess, Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Informationssysteme – Potentiale, Hindernisse, Einsatz

P-77 Jana Dittmann (Hrsg.): SICHERHEIT 2006

P-78 K.-O. Wenkel, P. Wagner, M. Morgenstern, K. Luzi, P. Eisermann (Hrsg.): Land- und Ernährungswirtschaft im Wandel

P-79 Bettina Biel, Matthias Book, Volker Gruhn (Hrsg.): Softwareengineering 2006

P-80 Mareike Schoop, Christian Huemer, Michael Rebstock, Martin Bichler (Hrsg.): Service-Oriented Electronic Commerce

P-81 Wolfgang Karl, Jürgen Becker, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle (Hrsg.): ARCS´06

P-82 Heinrich C. Mayr, Ruth Breu (Hrsg.): Modellierung 2006

P-83 Daniel Huson, Oliver Kohlbacher, Andrei Lupas, Kay Nieselt and Andreas Zell (eds.): German Conference on Bioinformatics

P-84 Dimitris Karagiannis, Heinrich C. Mayr, (Hrsg.): Information Systems Technology and its Applications

P-85 Witold Abramowicz, Heinrich C. Mayr, (Hrsg.): Business Information Systems

P-86 Robert Krimmer (Ed.): Electronic Voting 2006

P-87 Max Mühlhäuser, Guido Rößling, Ralf Steinmetz (Hrsg.): DELFI 2006: 4. e-Learning Fachtagung Informatik

P-88 Robert Hirschfeld, Andreas Polze, Ryszard Kowalczyk (Hrsg.): NODe 2006, GSEM 2006

P-90 Joachim Schelp, Robert Winter, Ulrich Frank, Bodo Rieger, Klaus Turowski (Hrsg.): Integration, Informationslogistik und Architektur

P-91 Henrik Stormer, Andreas Meier, Michael Schumacher (Eds.): European Conference on eHealth 2006

P-92 Fernand Feltz, Benoît Otjacques, Andreas Oberweis, Nicolas Poussing (Eds.): AIM 2006

P-93 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 1

P-94 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 2

P-95 Matthias Weske, Markus Nüttgens (Eds.): EMISA 2005: Methoden, Konzepte und Technologien für die Entwicklung von dienstbasierten Informationssystemen

P-96 Saartje Brockmans, Jürgen Jung, York Sure (Eds.): Meta-Modelling and Ontologies

P-97 Oliver Göbel, Dirk Schadt, Sandra Frings, Hardo Hase, Detlef Günther, Jens Nedon (Eds.): IT-Incident Mangament & IT-Forensics – IMF 2006

P-98 Hans Brandt-Pook, Werner Simonsmeier und Thorsten Spitta (Hrsg.): Beratung in der Softwareentwicklung – Modelle, Methoden, Best Practices

P-99 Andreas Schwill, Carsten Schulte, Marco Thomas (Hrsg.): Didaktik der Informatik

P-100 Peter Forbrig, Günter Siegel, Markus Schneider (Hrsg.): HDI 2006: Hochschuldidaktik der Informatik

P-101 Stefan Böttinger, Ludwig Theuvsen, Susanne Rank, Marlies Morgenstern (Hrsg.): Agrarinformatik im Spannungsfeld zwischen Regionalisierung und globalen Wertschöpfungsketten

P-102 Otto Spaniol (Eds.): Mobile Services and Personalized Environments

P-103 Alfons Kemper, Harald Schöning, Thomas Rose, Matthias Jarke, Thomas Seidl, Christoph Quix, Christoph Brochhaus (Hrsg.): Datenbanksysteme in Business, Technologie und Web (BTW 2007)

P-104 Birgitta König-Ries, Franz Lehner, Rainer Malaka, Can Türker (Hrsg.) MMS 2007: Mobilität und mobile Informationssysteme

P-105 Wolf-Gideon Bleek, Jörg Raasch, Heinz Züllighoven (Hrsg.) Software Engineering 2007

P-106 Wolf-Gideon Bleek, Henning Schwentner, Heinz Züllighoven (Hrsg.) Software Engineering 2007 – Beiträge zu den Workshops

P-107 Heinrich C. Mayr, Dimitris Karagiannis (eds.) Information Systems Technology and its Applications

P-108 Arslan Brömme, Christoph Busch, Detlef Hühnlein (eds.) BIOSIG 2007: Biometrics and Electronic Signatures

P-109 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 1

P-110 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 2

P-111 Christian Eibl, Johannes Magenheim, Sigrid Schubert, Martin Wessner (Hrsg.) DeLFI 2007: 5. e-Learning Fachtagung Informatik

P-112 Sigrid Schubert (Hrsg.) Didaktik der Informatik in Theorie und Praxis

P-113 Sören Auer, Christian Bizer, Claudia Müller, Anna V. Zhdanova (Eds.) The Social Semantic Web 2007 Proceedings of the 1st Conference on Social Semantic Web (CSSW)

P-114 Sandra Frings, Oliver Göbel, Detlef Günther, Hardo G. Hase, Jens Nedon, Dirk Schadt, Arslan Brömme (Eds.) IMF2007 IT-incident management & IT-forensics Proceedings of the 3rd International Conference on IT-Incident Management & IT-Forensics

P-115 Claudia Falter, Alexander Schliep, Joachim Selbig, Martin Vingron and Dirk Walther (Eds.) German conference on bioinformatics GCB 2007

P-116 Witold Abramowicz, Leszek Maciszek (Eds.)
Business Process and Services Computing
1st International Working Conference on Business Process and Services Computing
BPSC 2007

P-117 Ryszard Kowalczyk (Ed.)
Grid service engineering and manegement
The 4th International Conference on Grid Service Engineering and Management
GSEM 2007

P-118 Andreas Hein, Wilfried Thoben, Hans-Jürgen Appelrath, Peter Jensch (Eds.)
European Conference on ehealth 2007

P-119 Manfred Reichert, Stefan Strecker, Klaus Turowski (Eds.)
Enterprise Modelling and Information Systems Architectures
Concepts and Applications

P-120 Adam Pawlak, Kurt Sandkuhl, Wojciech Cholewa,
Leandro Soares Indrusiak (Eds.)
Coordination of Collaborative Engineering - State of the Art and Future Challenges

P-121 Korbinian Herrmann, Bernd Bruegge (Hrsg.)
Software Engineering 2008
Fachtagung des GI-Fachbereichs Softwaretechnik

P-122 Walid Maalej, Bernd Bruegge (Hrsg.)
Software Engineering 2008 - Workshopband
Fachtagung des GI-Fachbereichs Softwaretechnik

P-123 Michael H. Breitner, Martin Breunig, Elgar Fleisch, Ley Pousttchi, Klaus Turowski (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Technologien, Prozesse, Marktfähigkeit
Proceedings zur 3. Konferenz Mobile und Ubiquitäre Informationssysteme
(MMS 2008)

P-124 Wolfgang E. Nagel, Rolf Hoffmann, Andreas Koch (Eds.)
9th Workshop on Parallel Systems and Algorithms (PASA)
Workshop of the GI/ITG Speciel Interest Groups PARS and PARVA

P-125 Rolf A.E. Müller, Hans-H. Sundermeier, Ludwig Theuvsen, Stephanie Schütze, Marlies Morgenstern (Hrsg.)
Unternehmens-IT:
Führungsinstrument oder Verwaltungsbürde
Referate der 28. GIL Jahrestagung

P-126 Rainer Gimnich, Uwe Kaiser, Jochen Quante, Andreas Winter (Hrsg.)
10th Workshop Software Reengineering (WSR 2008)

P-127 Thomas Kühne, Wolfgang Reisig, Friedrich Steimann (Hrsg.)
Modellierung 2008

P-128 Ammar Alkassar, Jörg Siekmann (Hrsg.)
Sicherheit 2008
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)
2.-4. April 2008
Saarbrücken, Germany

P-129 Wolfgang Hesse, Andreas Oberweis (Eds.)
Sigsand-Europe 2008
Proceedings of the Third AIS SIGSAND European Symposium on Analysis, Design, Use and Societal Impact of Information Systems

P-130 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
1. DFN-Forum Kommunikations-technologien Beiträge der Fachtagung

P-131 Robert Krimmer, Rüdiger Grimm (Eds.)
3rd International Conference on Electronic Voting 2008
Co-organized by Council of Europe, Gesellschaft für Informatik and E-Voting. CC

P-132 Silke Seehusen, Ulrike Lucke, Stefan Fischer (Hrsg.)
DeLFI 2008:
Die 6. e-Learning Fachtagung Informatik

P-133 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 1

P-134 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 2

P-135 Torsten Brinda, Michael Fothe, Peter Hubwieser, Kirsten Schlüter (Hrsg.)
Didaktik der Informatik –
Aktuelle Forschungsergebnisse

P-136 Andreas Beyer, Michael Schroeder (Eds.)
German Conference on Bioinformatics
GCB 2008

P-137 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2008: Biometrics and Electronic Signatures

P-138 Barbara Dinter, Robert Winter, Peter Chamoni, Norbert Gronau, Klaus Turowski (Hrsg.)
Synergien durch Integration und Informationslogistik
Proceedings zur DW2008

P-139 Georg Herzwurm, Martin Mikusz (Hrsg.)
Industrialisierung des Software-Managements
Fachtagung des GI-Fachausschusses Management der Anwendungsentwicklung und -wartung im Fachbereich Wirtschaftsinformatik

P-140 Oliver Göbel, Sandra Frings, Detlef Günther, Jens Nedon, Dirk Schadt (Eds.)
IMF 2008 - IT Incident Management & IT Forensics

P-141 Peter Loos, Markus Nüttgens, Klaus Turowski, Dirk Werth (Hrsg.)
Modellierung betrieblicher Informationssysteme (MobIS 2008)
Modellierung zwischen SOA und Compliance Management

P-142 R. Bill, P. Korduan, L. Theuvsen, M. Morgenstern (Hrsg.)
Anforderungen an die Agrarinformatik durch Globalisierung und Klimaveränderung

P-143 Peter Liggesmeyer, Gregor Engels, Jürgen Münch, Jörg Dörr, Norman Riegel (Hrsg.)
Software Engineering 2009
Fachtagung des GI-Fachbereichs Softwaretechnik

P-144 Johann-Christoph Freytag, Thomas Ruf, Wolfgang Lehner, Gottfried Vossen (Hrsg.)
Datenbanksysteme in Business, Technologie und Web (BTW)

P-145 Knut Hinkelmann, Holger Wache (Eds.)
WM2009: 5th Conference on Professional Knowledge Management

P-146 Markus Bick, Martin Breunig, Hagen Höpfner (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Entwicklung, Implementierung und Anwendung
4. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2009)

P-147 Witold Abramowicz, Leszek Maciaszek, Ryszard Kowalczyk, Andreas Speck (Eds.)
Business Process, Services Computing and Intelligent Service Management
BPSC 2009 · ISM 2009 · YRW-MBP 2009

P-148 Christian Erfurth, Gerald Eichler, Volkmar Schau (Eds.)
9th International Conference on Innovative Internet Community Systems
I^{2}CS 2009

P-149 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
2. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-150 Jürgen Münch, Peter Liggesmeyer (Hrsg.)
Software Engineering
2009 - Workshopband

P-151 Armin Heinzl, Peter Dadam, Stefan Kirn, Peter Lockemann (Eds.)
PRIMIUM
Process Innovation for Enterprise Software

P-152 Jan Mendling, Stefanie Rinderle-Ma, Werner Esswein (Eds.)
Enterprise Modelling and Information Systems Architectures
Proceedings of the 3rd Int'l Workshop EMISA 2009

P-153 Andreas Schwill, Nicolas Apostolopoulos (Hrsg.)
Lernen im Digitalen Zeitalter
DeLFI 2009 – Die 7. E-Learning Fachtagung Informatik

P-154 Stefan Fischer, Erik Maehle Rüdiger Reischuk (Hrsg.)
INFORMATIK 2009
Im Focus das Leben

P-155 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2009:
Biometrics and Electronic Signatures
Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

P-156 Bernhard Koerber (Hrsg.)
Zukunft braucht Herkunft
25 Jahre »INFOS – Informatik und Schule«

P-157 Ivo Grosse, Steffen Neumann, Stefan Posch, Falk Schreiber, Peter Stadler (Eds.)
German Conference on Bioinformatics 2009

P-158 W. Claupein, L. Theuvsen, A. Kämpf, M. Morgenstern (Hrsg.)
Precision Agriculture Reloaded – Informationsgestützte Landwirtschaft

P-159 Gregor Engels, Markus Luckey, Wilhelm Schäfer (Hrsg.)
Software Engineering 2010

P-160 Gregor Engels, Markus Luckey, Alexander Pretschner, Ralf Reussner (Hrsg.)
Software Engineering 2010 – Workshopband
(inkl. Doktorandensymposium)

P-161 Gregor Engels, Dimitris Karagiannis Heinrich C. Mayr (Hrsg.)
Modellierung 2010

P-162 Maria A. Wimmer, Uwe Brinkhoff, Siegfried Kaiser, Dagmar Lück-Schneider, Erich Schweighofer, Andreas Wiebe (Hrsg.)
Vernetzte IT für einen effektiven Staat
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2010

P-163 Markus Bick, Stefan Eulgem, Elgar Fleisch, J. Felix Hampe, Birgitta König-Ries, Franz Lehner, Key Pousttchi, Kai Rannenberg (Hrsg.)
Mobile und Ubiquitäre Informationssysteme
Technologien, Anwendungen und Dienste zur Unterstützung von mobiler Kollaboration

P-164 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2010: Biometrics and Electronic Signatures Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

P-165 Gerald Eichler, Peter Kropf, Ulrike Lechner, Phayung Meesad, Herwig Unger (Eds.)
10th International Conference on Innovative Internet Community Systems (I^2CS) – Jubilee Edition 2010 –

P-166 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
3. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-167 Robert Krimmer, Rüdiger Grimm (Eds.)
4th International Conference on Electronic Voting 2010
co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC

P-168 Ira Diethelm, Christina Dörge, Claudia Hildebrandt, Carsten Schulte (Hrsg.)
Didaktik der Informatik
Möglichkeiten empirischer Forschungsmethoden und Perspektiven der Fachdidaktik

P-169 Michael Kerres, Nadine Ojstersek Ulrik Schroeder, Ulrich Hoppe (Hrsg.)
DeLFI 2010 - 8. Tagung der Fachgruppe E-Learning der Gesellschaft für Informatik e.V.

P-170 Felix C. Freiling (Hrsg.)
Sicherheit 2010
Sicherheit, Schutz und Zuverlässigkeit

P-171 Werner Esswein, Klaus Turowski, Martin Juhrisch (Hrsg.)
Modellierung betrieblicher Informationssysteme (MobIS 2010)
Modellgestütztes Management

P-172 Stefan Klink, Agnes Koschmider Marco Mevius, Andreas Oberweis (Hrsg.)
EMISA 2010
Einflussfaktoren auf die Entwicklung flexibler, integrierter Informationssysteme
Beiträge des Workshops der GI-Fachgruppe EMISA (Entwicklungsmethoden für Informationssysteme und deren Anwendung)

P-173 Dietmar Schomburg, Andreas Grote (Eds.)
German Conference on Bioinformatics 2010

P-174 Arslan Brömme, Torsten Eymann, Detlef Hühnlein, Heiko Roßnagel, Paul Schmücker (Hrsg.)
perspeGKtive 2010
Workshop „Innovative und sichere Informationstechnologie für das Gesundheitswesen von morgen“

P-175 Klaus-Peter Fähnrich, Bogdan Franczyk (Hrsg.)
INFORMATIK 2010
Service Science – Neue Perspektiven für die Informatik
Band 1

P-176 Klaus-Peter Fähnrich, Bogdan Franczyk (Hrsg.)
INFORMATIK 2010
Service Science – Neue Perspektiven für die Informatik
Band 2

P-177 Witold Abramowicz, Rainer Alt, Klaus-Peter Fähnrich, Bogdan Franczyk, Leszek A. Maciaszek (Eds.)
INFORMATIK 2010
Business Process and Service Science – Proceedings of ISSS and BPSC

P-178 Wolfram Pietsch, Benedikt Krams (Hrsg.)
Vom Projekt zum Produkt
Fachtagung des GI-Fachausschusses Management der Anwendungsentwicklung und -wartung im Fachbereich Wirtschafts-informatik (WI-MAW), Aachen, 2010

P-179 Stefan Gruner, Bernhard Rumpe (Eds.)
FM+AM`2010
Second International Workshop on Formal Methods and Agile Methods

P-180 Theo Härder, Wolfgang Lehner, Bernhard Mitschang, Harald Schöning, Holger Schwarz (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW)
14. Fachtagung des GI-Fachbereichs „Datenbanken und Informationssysteme“ (DBIS)

P-181 Michael Clasen, Otto Schätzel, Brigitte Theuvsen (Hrsg.)
Qualität und Effizienz durch informationsgestützte Landwirtschaft, Fokus: Moderne Weinwirtschaft

P-182 Ronald Maier (Hrsg.)
6th Conference on Professional Knowledge Management
From Knowledge to Action

P-183 Ralf Reussner, Matthias Grund, Andreas Oberweis, Walter Tichy (Hrsg.)
Software Engineering 2011
Fachtagung des GI-Fachbereichs Softwaretechnik

P-184 Ralf Reussner, Alexander Pretschner, Stefan Jähnichen (Hrsg.)
Software Engineering 2011
Workshopband
(inkl. Doktorandensymposium)

P-185 Hagen Höpfner, Günther Specht, Thomas Ritz, Christian Bunse (Hrsg.)
MMS 2011: Mobile und ubiquitäre Informationssysteme Proceedings zur 6. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2011)

P-186 Gerald Eichler, Axel Küpper, Volkmar Schau, Hacène Fouchal, Herwig Unger (Eds.)
11th International Conference on Innovative Internet Community Systems (I^2CS)

P-187 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
4. DFN-Forum Kommunikations-technologien, Beiträge der Fachtagung 20. Juni bis 21. Juni 2011 Bonn

P-188 Holger Rohland, Andrea Kienle, Steffen Friedrich (Hrsg.)
DeLFI 2011 – Die 9. e-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V.
5.–8. September 2011, Dresden

P-189 Thomas, Marco (Hrsg.)
Informatik in Bildung und Beruf
INFOS 2011
14. GI-Fachtagung Informatik und Schule

P-190 Markus Nüttgens, Oliver Thomas, Barbara Weber (Eds.)
Enterprise Modelling and Information Systems Architectures (EMISA 2011)

P-191 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2011
International Conference of the Biometrics Special Interest Group

P-192 Hans-Ulrich Heiß, Peter Pepper, Holger Schlingloff, Jörg Schneider (Hrsg.)
INFORMATIK 2011
Informatik schafft Communities

P-193 Wolfgang Lehner, Gunther Piller (Hrsg.)
IMDM 2011

P-194 M. Clasen, G. Fröhlich, H. Bernhardt, K. Hildebrand, B. Theuvsen (Hrsg.)
Informationstechnologie für eine nachhaltige Landbewirtschaftung
Fokus Forstwirtschaft

P-195 Neeraj Suri, Michael Waidner (Hrsg.)
Sicherheit 2012
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 6. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)

P-196 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2012
Proceedings of the 11th International Conference of the Biometrics Special Interest Group

P-197 Jörn von Lucke, Christian P. Geiger, Siegfried Kaiser, Erich Schweighofer, Maria A. Wimmer (Hrsg.)
Auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2012

P-198 Stefan Jähnichen, Axel Küpper, Sahin Albayrak (Hrsg.)
Software Engineering 2012
Fachtagung des GI-Fachbereichs Softwaretechnik

P-199 Stefan Jähnichen, Bernhard Rumpe, Holger Schlingloff (Hrsg.)
Software Engineering 2012
Workshopband

P-200 Gero Mühl, Jan Richling, Andreas Herkersdorf (Hrsg.)
ARCS 2012 Workshops

P-201 Elmar J. Sinz Andy Schürr (Hrsg.)
Modellierung 2012

P-202 Andrea Back, Markus Bick, Martin Breunig, Key Pousttchi, Frédéric Thiesse (Hrsg.)
MMS 2012:Mobile und Ubiquitäre Informationssysteme

P-203 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)
5. DFN-Forum Kommunikations-technologien
Beiträge der Fachtagung

P-204 Gerald Eichler, Leendert W. M. Wienhofen, Anders Kofod-Petersen, Herwig Unger (Eds.)
12th International Conference on Innovative Internet Community Systems (I2CS 2012)

P-205 Manuel J. Kripp, Melanie Volkamer, Rüdiger Grimm (Eds.)
5th International Conference on Electronic Voting 2012 (EVOTE2012)
Co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC

P-206 Stefanie Rinderle-Ma, Mathias Weske (Hrsg.)
EMISA 2012
Der Mensch im Zentrum der Modellierung

P-207 Jörg Desel, Jörg M. Haake, Christian Spannagel (Hrsg.)
DeLFI 2012: Die 10. e-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V.
24.–26. September 2012

P-208 Ursula Goltz, Marcus Magnor, Hans-Jürgen Appelrath, Herbert Matthies, Wolf-Tilo Balke, Lars Wolf (Hrsg.)
INFORMATIK 2012

P-209 Hans Brandt-Pook, André Fleer, Thorsten Spitta, Malte Wattenberg (Hrsg.)
Nachhaltiges Software Management

P-210 Erhard Plödereder, Peter Dencker, Herbert Klenk, Hubert B. Keller, Silke Spitzer (Hrsg.)
Automotive – Safety & Security 2012
Sicherheit und Zuverlässigkeit für automobile Informationstechnik

P-211 M. Clasen, K. C. Kersebaum, A. Meyer-Aurich, B. Theuvsen (Hrsg.)
Massendatenmanagement in der Agrar- und Ernährungswirtschaft
Erhebung - Verarbeitung - Nutzung
Referate der 33. GIL-Jahrestagung
20. – 21. Februar 2013, Potsdam

P-212 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2013
Proceedings of the 12th International Conference of the Biometrics Special Interest Group
04.–06. September 2013
Darmstadt, Germany

P-213 Stefan Kowalewski, Bernhard Rumpe (Hrsg.)
Software Engineering 2013
Fachtagung des GI-Fachbereichs Softwaretechnik

P-214 Volker Markl, Gunter Saake, Kai-Uwe Sattler, Gregor Hackenbroich, Bernhard Mit schang, Theo Härder, Veit Köppen (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW) 2013
13. – 15. März 2013, Magdeburg

P-215 Stefan Wagner, Horst Lichter (Hrsg.)
Software Engineering 2013
Workshopband
(inkl. Doktorandensymposium)
26. Februar – 1. März 2013, Aachen

P-216 Gunter Saake, Andreas Henrich, Wolfgang Lehner, Thomas Neumann, Veit Köppen (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW) 2013 – Workshopband
11. – 12. März 2013, Magdeburg

P-217 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)
6. DFN-Forum Kommunikations-technologien
Beiträge der Fachtagung
03.–04. Juni 2013, Erlangen

P-218 Andreas Breiter, Christoph Rensing (Hrsg.)
DeLFI 2013: Die 11 e-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V. (GI)
8. – 11. September 2013, Bremen

P-219 Norbert Breier, Peer Stechert, Thomas Wilke (Hrsg.)
Informatik erweitert Horizonte
INFOS 2013
15. GI-Fachtagung Informatik und Schule
26. – 28. September 2013

P-220 Matthias Horbach (Hrsg.)
INFORMATIK 2013
Informatik angepasst an Mensch, Organisation und Umwelt
16. – 20. September 2013, Koblenz

P-221 Maria A. Wimmer, Marijn Janssen, Ann Macintosh, Hans Jochen Scholl, Efthimios Tambouris (Eds.)
Electronic Government and Electronic Participation
Joint Proceedings of Ongoing Research of IFIP EGOV and IFIP ePart 2013
16. – 19. September 2013, Koblenz

P-222 Reinhard Jung, Manfred Reichert (Eds.)
Enterprise Modelling and Information Systems Architectures (EMISA 2013)
St. Gallen, Switzerland
September 5. – 6. 2013

P-223 Detlef Hühnlein, Heiko Roßnagel (Hrsg.)
Open Identity Summit 2013
10. – 11. September 2013
Kloster Banz, Germany

P-224 Eckhart Hanser, Martin Mikusz, Masud Fazal-Baqaie (Hrsg.)
Vorgehensmodelle 2013
Vorgehensmodelle – Anspruch und Wirklichkeit
20. Tagung der Fachgruppe Vorgehensmodelle im Fachgebiet Wirtschaftsinformatik (WI-VM) der Gesellschaft für Informatik e.V.
Lörrach, 2013^

The titles can be purchased at:

Köllen Druck + Verlag GmbH
Ernst-Robert-Curtius-Str. 14 · D-53117 Bonn
Fax: +49 (0)228/9898222
E-Mail: druckverlag@koellen.de