Differentielle dynamische Logiken: Automatisches Beweisen für hybride Systeme

André Platzer

Computer Science Department
Carnegie Mellon University
Pittsburgh, PA, USA
aplatzer@cs.cmu.edu

Abstract: Die Entwicklung und Analyse komplexer physikalischer Systeme, eingebetteter Systeme und computerisierter Steuerungssysteme ist außerordentlich kompliziert, durch die steigende Verbreitung und drastische Sicherheitsrelevanz allerdings von enormer Wichtigkeit und mit hohen Kosten verbunden. Hybride Systeme sind Modelle solcher komplexen physikalischen Systeme mit sich überlagerndem diskreten Schaltverhalten und kontinuierlicher Dynamik, die durch Differentialgleichungen beschrieben wird. Als theoretisches und praktisches Fundament für die Verifikation und Analyse hybrider Systeme führen wir die *differentielle dynamische Logik* ein. Mit dieser kann die Korrektheit von hybriden Systemen auf natürliche und elegante Art und Weise spezifiziert und verifiziert werden, um Fehler im Systementwurf zu entdecken oder die Fehlerfreiheit nachzuweisen. Der wichtigste praktische Beitrag dieser Arbeit ist ein automatisches Beweisverfahren für die differentielle dynamische Logik, welches hybride Systeme analysiert, indem es sie sukzessiv auf Eigenschaften ihrer Bestandteile reduziert. Unser theoretisches Hauptresultat zeigt, dass dieses Verfahren hybride Systeme *vollständig* relativ zu elementaren Eigenschaften von Differentialgleichungen behandelt. Für komplizierte hybride Systeme stellen wir weiterhin *differentielle Induktion* vor, mit der Differential(un)gleichungen analysiert werden können ohne sie lösen zu müssen. Auf der Basis zahlreicher algorithmischer Fortschritte demonstrieren wir unseren Ansatz anhand erfolgreich nachgewiesener Sicherheits-, Steuerbarkeits-, Lebendigkeits- und Kollisionsfreiheitseigenschaften für Zugsteuerungen wie dem *European Train Control System* und *Kreisverkehrmanövern im Flugverkehr*.

1 Motivation

Einwandfreie Funktionsfähigkeit von komplexen physikalischen Systemen sicherzustellen gehört zu den größten Herausforderungen und bedeutendsten Problemen der Informatik, Mathematik und Ingenieursdisziplinen. Zusätzlich zu nichttrivialer physikalischer Systemdynamik wird das Verhalten komplexer Systeme zunehmend von computerisierten Steuerungen und automatischer analoger oder digitaler Entscheidungsfindung bestimmt, beispielsweise im Luftfahrtbereich, bei Zugsteuerungen oder Anwendungen im Automobilbereich. Gleichzeitig erlangen korrekte Entscheidungen und korrekte Steuerungen in diesen Systemen immer größere Bedeutung, weil immer mehr sicherheitskritis-

che Prozesse von vollautomatischen oder teilautomatischen Steuerungen reguliert werden, etwa dem European Train Control System [ERT02], Kollisionsvermeidungsmanövern in der Flugsicherung [TPS98, LLL00], neuartige fahrerlose Automobiltechnik [Bue08] oder biomedizinische Anwendungen wie die automatische Glucoseregulierung für Diabetespatienten [PDP01]. Gleichzeitig steigen – wegen hoher Sicherheitsbedeutung und diffizilem Systemverhalten – die Entwicklungskosten. Im Automobil- und Luftfahrtbereich etwa übersteigen die Entwicklungs- und Fehlerbehebungskosten allein der Steuerungssoftware bereits 50% der Gesamtentwicklungskosten; Tendenz stark steigend.

Ein allgemeineres Phänomen in komplexen physikalischen Systemen wie diesen ist, dass korrektes Systemverhalten von korrekter Interaktion von Steuerungskomponenten mit der physikalischen Systemdynamik abhängt und keine isolierte Eigenschaft allein der Steuerungslogik oder allein des physikalischen Systems ist. Ein gemeinsames Modell für diese Systeme sind *hybride Systeme*, die sich durch interagierende diskrete und kontinuierliche Dynamik auszeichnen, welche Überlagerungen von physikalischer Systemdynamik mit diskreter Computersteuerung natürlich modellieren. Mit diesen Überlagerungen können hybride Systeme anspruchsvolle Systemdynamik auf einfache Art modellieren, erfordern allerdings auch ausgeklügelte Analysetechniken. Diese Analysetechniken für hybride Systeme, die wegen der Verbreitung in zahlreichen sicherheitskritischen Systemen von hoher praktischer Bedeutung sind, stellen den zentralen Gegenstand der hier vorgestellten Dissertation dar [Pla08c].

2 Sicherheitskritische komplexe physikalische Systeme

Um typische Herausforderungen hybrider Systeme zu illustrieren, betrachtet die Arbeit zwei realistische Fallstudien, Zugsteuerung und Flugzeugsteuerung, als fortlaufende Beispiele. Beides sind Bereiche, die sich durch gleichermaßen hohe Komplexität und Sicherheitsrelevanz auszeichnen.

Zugsteuerung Moderne Hochgeschwindigkeitszüge, wie ICEs, brauchen etliche Kilometer, um zum Stillstand zu gelangen, sodass sichere Fahrt auf Sicht unmöglich wird. Das *European Train Control System* (ETCS) [ERT02] reguliert und sichert Zugfahrten mittels so genannter *movement authorities* (MA), die dynamisch in rapider Folge durch drahtlose Kommunikation mit Streckenzentralen, engl. *radio block controller* (RBC), bestimmt werden; siehe Abb. 1. Um zu bestimmen, ob

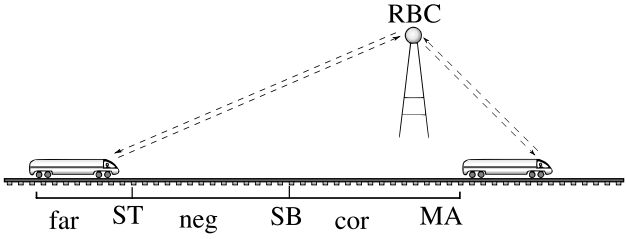
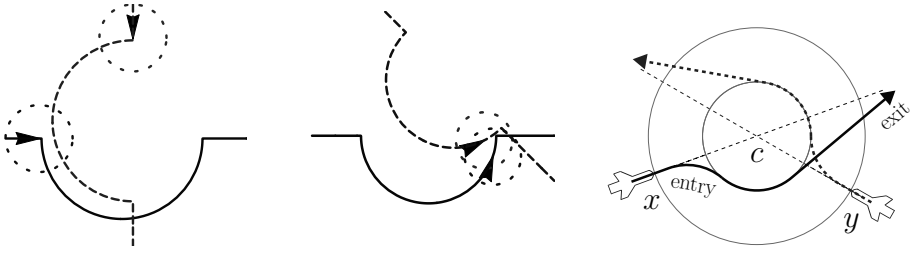


Abbildung 1: European Train Control System

die ETCS Zugsteuerung korrekt funktioniert, müssen wir analysieren, ob die Zugpositionen, die sich im Laufe der Zeit dynamisch ändern, jederzeit sicher getrennt sind. Dafür benötigen wir Techniken, um die Interaktion der Zugsteuerungslogik mit dem ETCS Kooperationsprotokoll und einem Modell der tatsächlichen, physikalischen Zugdynamik zu untersuchen. Schliesslich ist Kollisionsfreiheit keine isolierte Eigenschaft allein der diskreten Kooperationsebene des ETCS Protokolls, allein der lokalen Zugsteuerungsentscheidungen oder allein der kontinuierlichen Zugbewegung, sondern eine gemeinsame Eigenschaft ihrer Überlagerung.

Flugsteuerung In der Steuerung von Flugzeugen werden Kollisionsvermeidungsmanöver [TPS98, LLL00] eingesetzt, um Konflikte sich überschneidender Flugrouten aufzulösen, die während des freien Fluges in verschiedenen Richtungen auftreten können; siehe Abb. 2. Um korrektes Funktionieren der Kollisionsvermeidungsmanöver von



2a: Kreisverkehrmanöver 2b: Gegenbeispiel 2c: Korrigiertes Flugmanöver

Abbildung 2: Kollisionsvermeidungsmanöver im Flugverkehr: Beispiel, Fehler, Korrektur

Flugzeugen unter allen Umständen sicherzustellen, muss die zeitliche Evolution der Flugzeuge im Luftraum behutsam analysiert werden, und zwar unter Berücksichtigung der Effekte, die Steuerungsentscheidungen auf das Systemverhalten haben. Dies ergibt erneut eine Überlagerung der physikalischen Systemdynamik mit deren Steuerung. Das Manöver in Abb. 2a beispielsweise wurde von Tomlin et al. [TPS98] vorgeschlagen und versucht Kollisionsvermeidung in der Luft durch Kreisverkehr zu erreichen. Die Grundidee ist, dass Flugzeuge längs Kreisbahnen sicher aneinander vorbei geleitet werden sollen. Unser (automatisch gefundenes) Gegenbeispiel in Abb. 2b, bei dem die Flugzeuge trotz versuchten Ausweichmanövers kollidieren, verdeutlicht, wie wichtig es ist, Protokolle systematisch und automatisch auf ihre Korrektheit hin für alle möglichen Situationen zu untersuchen. Das Manöver in Abb. 2c wurde in dieser Arbeit eingeführt, um das klassische Kreisverkehrmanöver zu korrigieren, und erfolgreich verifiziert.

3 Hybride Systeme

Als gemeinsames mathematisches Modell für komplexe physikalische Systeme sind *hybride Systeme* [ACH+95, BBM98] als dynamische Systeme [Sib75] definiert, deren Systemzustand sich im Laufe der Zeit gemäß interagierender Regeln der diskreten und

kontinuierlichen Dynamik ändert. Hybride Systeme haben zum Ziel, Überlagerungen physikalischer Systemdynamik mit Steuerungsdynamik natürlich zu modellieren.

Dynamik hybrider Systeme Bei diskreten Transitionen wechselt das hybride System seinen Zustand instantan und möglicherweise unstetig. Während kontinuierlicher Transitionen folgt der Systemzustand einer kontinuierlichen Funktion und variiert gemäß Differentialgleichungen. Kontinuierliche Dynamik resultiert beispielsweise aus der stetigen Bewegung eines Zuges auf dem Gleis (Zugposition z entwickelt sich mit Geschwindigkeit v längs der Differentialgleichung $z' = v$, in der z' die Ableitung von z nach der Zeit darstellt) oder von der kontinuierlichen Variation seiner Geschwindigkeit im Laufe der Zeit ($v' = a$ mit Beschleunigung a). Anderes Verhalten lässt sich natürlicher als diskrete Dynamik modellieren, beispielsweise die spontane Änderung von Steuerungsvariablen wie der Beschleunigung (also dem Ändern von a durch das Setzen von $a := -b$ mit Bremskraft $b > 0$) oder der Veränderung von Statusinformationen eines diskreten Controllers.

Beide Arten von Dynamik interagieren, beispielsweise wenn Messungen des kontinuierlichen Zustands Entscheidungen der diskreten Steuerung beeinflussen (der Zug schaltet in den Bremsmodus wenn v zu hoch ist). Ebenso interagieren sie, wenn die resultierenden Steuerungsentscheidungen die Steuerungsvariablen der kontinuierlichen Dynamik beeinflussen (etwa der Änderung von a in $z'' = a$). Die Überlagerung kontinuierlicher Dynamik mit analoger oder diskreter Steuerung bewirkt komplexes Systemverhalten, welches weder durch rein kontinuierliche Methoden behandelt werden kann (wegen der Unstetigkeiten, die diskrete Transitionen hervorrufen) noch allein durch Betrachten der diskreten Wechsel (weil die Sicherheit vom kontinuierlichen Zustand abhängt). Abb. 3 zeigt verschiedene Abläufe der Position z und Geschwindigkeit v (gestrichelt) im ETCS Controller über die Zeit t, wobei die Beschleunigung währenddessen gesteuert wird. Nur die unterste Wahl von v und z ist sicher (erfüllt dass die Zugposition innerhalb der MA Schranke m liegt, d.h., $z \leq m$).

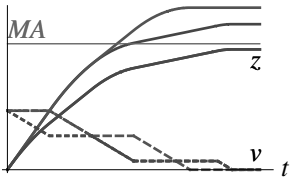


Abbildung 3: Zugläufe

Hybride Automaten Neben anderen Modellen für hybride Systeme [BBM98] ist das Modell der *hybriden Automaten* [ACH+95] eine weit verbreitete Notation. Diese spezifizieren diskrete und kontinuierliche Dynamik visuell in einem Graphen. Siehe Abb. 4 für ein (viel zu stark) vereinfachtes Beispiel einer Zugsteuerung. Jeder Knoten entspricht einem kontinuierlichen dynamischen System und kann mit einer Differentialgleichung und einer Invariantenregion gekennzeichnet sein, welche die maximale Domäne möglicher Evolutionen angibt. Im Knoten *brems* von Abb. 4 etwa findet die Differen-

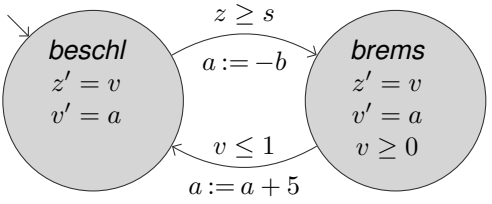


Abbildung 4: Hybrider Automat für eine (zu) stark vereinfachte Zugsteuerung

tialgleichung $z' = v, v' = a$ nur innerhalb der Invariantenregion $v \geq 0$ Anwendung (der Zug fährt durch Bremsen nicht rückwärts). Die Kanten geben das diskrete Schaltverhalten zwischen den jeweiligen Knoten der kontinuierlichen Evolution an. Kanten können mit Bedingungen beschriftet sein, die gelten müssen um der Kante zu folgen, und mit diskreten Zustandstransformationen, die sofortigen Effekt haben, wenn das System der Kante folgt. Beispielsweise kann der Automat in Abb. 4 einer Kante folgen, um den Knoten *beschl* zu verlassen, wenn die Zugposition z den Punkt s passiert hat, was wiederum die Beschleunigung per $a := -b$ auf Bremsen setzt und den Knoten *brems* betritt.

Um ein rein kompositionelles Modell zu erhalten, also eines wo der Effekt jeder Operation eine einfache Funktion ihrer Bestandteile ist, kristallisiert die Arbeit die neue Notation der *hybriden Programme* [Pla08b] als geeigneteres Modell für formale Analysen heraus. Hybride Programm sind der wesentliche Kern klassischer Programmiersprachen wie C, erweitert um Nichtdeterminismen für freie Wahlen der Steuerung oder Umgebung, sowie Differentialgleichungen, die kontinuierliches Verhalten der Systemdynamik ausdrücken. Ein Ausschnitt von Abb. 4 entspräche beispielsweise $\texttt{if}(z \geq s)\, a := -b;\ z' = v, v' = a$.

4 Differentielle dynamische Logik

Als natürliche Spezifikations- und Verifikationssprache für Sicherheits-, Lebendigkeits-, Steuerbarkeits- und allgemeinerer Korrektheitseigenschaften hybrider Systeme stellt die Arbeit eine neue Logik vor: die *differentielle dynamische Logik* $\mathsf{d}\mathcal{L}$ [Pla08b, Pla08c]. Im Gegensatz zu anderen Logiken [Pra76, Eme90, DN00] ermöglicht es die differentielle dynamische Logik direkt Aussagen über das Verhalten hybrider Systeme zu treffen.

Spezifikation mit $\mathsf{d}\mathcal{L}$ Angenommen *ETCS* bezeichnet das hybride System der ETCS Steuerung, also ein Steuerungsprogramm mit Differentialgleichungen für die kontinuierliche Zugbewegung. Dann drückt die folgende $\mathsf{d}\mathcal{L}$ Formel beispielsweise aus, dass die Zugposition z während der Zugfahrt immer innerhalb der erlaubten Grenze m der movement authority verbleiben wird, sofern die Bremskraft b positiv ist und der Anfangszustand des Systems eine Geschwindigkeit v hat, die die quadratische Bedingung $v^2 \leq 2b(m - z)$ erfüllt:

$$b > 0 \wedge v^2 \leq 2b(m - z) \ \rightarrow\ [\mathit{ETCS}]\, z \leq m \tag{1}$$

Diese logische Formel folgt einem üblichen Spezifikationsmuster für hybride Systeme. Unter einer bestimmten Bedingung an den Anfangszustand des Systems (links des Implikationszeichens $\rightarrow$) drückt Formel (1) eine Sicherheitseigenschaft über das zukünftige Verhalten des *ETCS*-Controllers aus. Die Formel besagt, dass *alle* Zustände, die durch Systemläufe des Controllers zusammen mit der Systemdynamik erreichbar sind, innerhalb der movement authority liegen (ausgedrückt durch die Modalität in $[\mathit{ETCS}]\, z \leq m$). Dual dazu drückt $\langle \mathit{ETCS} \rangle\, z > m$ aus, dass es einen Ablauf von *ETCS* gibt, der die MA verletzt – was von der Anfangsgeschwindigkeit und Steuerungseintscheidungen abhängt; vrgl. Abb. 3. Die Logik $\mathsf{d}\mathcal{L}$ ist abgeschlossen unter logischen Operatoren. Wenn ϕ, ψ $\mathsf{d}\mathcal{L}$

Formeln sind, dann auch die folgenden $\mathsf{d}\mathcal{L}$ Formeln (wobei α ein hybrides Programm ist):

$$\neg\phi \mid \phi \wedge \psi \mid \phi \vee \psi \mid \phi \rightarrow \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid [\alpha]\phi \mid \langle\alpha\rangle\phi$$

Verifikation mit $\mathsf{d}\mathcal{L}$ Bislang ist die Spezifikation (1) – so natürlich sie auch zu verstehen sein mag – nur eine Behauptung. Der wichtigste Schritt ist, diese Behauptung über das korrekte Verhalten der ETCS Steuerung entweder durch einen stichhaltigen Beweis zu belegen oder durch ein Gegenbeispiel zu widerlegen. Dafür bietet die vorgestellte Arbeit ein Beweisverfahren, welches eine Behauptung wie (1) samt dem darin enthaltenen hybriden Steuerungssystem *ETCS* systematisch analysiert und schrittweise zerlegt, bis der Wahrheitsgehalt der Behauptung entschieden werden kann.

Die zentrale theoretische und praktische Herausforderung hierbei ist die Behandlung der interagierenden diskreten und kontinuierlichen Dynamik hybrider Systeme. Diese Herausforderungen sind enorm. In der Tat sind schon simple Fragen über hybride Systeme unentscheidbar, es gibt also keinen Algorithmus der in allen Fällen mit der richtigen Antwort terminiert. Zahlreiche Analyseverfahren für hybride Systeme weisen Korrektheitsprobleme auf, können also sowohl fälschlicherweise mit "sicher" als auch fehlerhaft mit "unsicher" antworten, sofern sie überhaupt terminieren. Dies ist nur bedingt hilfreich, wenn man sich als Entwickler fragt, ob denn die Zug- oder Flugzeugsteuerung richtig funktioniert und Kollisionen wirklich verhindert.

Im Gegensatz dazu ist das $\mathsf{d}\mathcal{L}$ Beweisverfahren korrekt. Als grundlegendes Resultat dieser Arbeit wird ausserdem das erste Vollständigkeitsresultat für hybride Systeme bewiesen: Mit dem $\mathsf{d}\mathcal{L}$ Verfahren können *alle* wahren Aussagen auf Basis elementarer Eigenschaften der Differentialgleichungen nachgewiesen werden [Pla08b]. Darauf aufbauend sind ferner praxistaugliche Fixpunkt-Algorithmen für hybride Systeme entwickelt worden [PC08], die automatisch die Systeminvarianten synthetisieren, welche für Beweise erforderlich sind.

In praktischen Beispielen wie ETCS (Abb. 1) oder sogar Kollisionsvermeidungsmanövern für Flugzeuge (Abb. 2) funktioniert das $\mathsf{d}\mathcal{L}$-Verfahren sehr erfolgreich und kann Systeme automatisch beweisen, die weit jenseits der Möglichkeiten bisheriger Ansätze liegen. Während typische machbare Systemgrössen bislang eher auf vierdimensionale, lineare Systeme beschränkt waren [ACH+95, Fre05], können die $\mathsf{d}\mathcal{L}$ Algorithmen auch 28-dimensionale nichtlineare Dynamik für 5 Flugzeuge mit komplizierten Differentialgleichungen bei gut skalierendem Speicherverbrauch noch erfolgreich verifizieren (Tab. 1).

Tabelle 1: Experimentelle Resultate (Auszug)

Fallstudie	Laufzeit(s)	Speicher(MB)	Beweisschritte	Dimension
ETCS Sicherheit	183	87	169	15
ETCS Steuerbarkeit	1	6	17	5
Kreisverkehr (2 Flugzeuge)	14	8	117	13
Kreisverkehr (3 Flugzeuge)	387	42	182	18
Kreisverkehr (4 Flugzeuge)	730	39	234	23
Kreisverkehr (5 Flugzeuge)	1964	88	317	28

5 Resultate und Beiträge

Die vorgestellte Dissertation [Pla08c] basiert auf Resultaten aus der symbolischen und mathematischen Logik, dem automatischen Beweisen, der Differentialalgebra, Computeralgebra, reellen algebraischen Geometrie, Analysis, sowie Theorie der Differentialgleichungen und dynamischen Systeme. Sie besitzt sowohl hohen theoretischen als auch hohen algorithmischen, praktischen und angewandten Anteil. Die Kernresultate sind in zahlreichen Veröffentlichungen, darunter 3 Zeitschriftenartikeln, näher beschrieben, etwa [Pla08b, Pla08a, PC08]. Die wichtigsten Hauptbeiträge sind im folgenden aufgeführt.

Konzeptionelle und praktische Hauptbeiträge Die Arbeit stellt eine Reihe neuer Logiken vor, die differentiellen dynamischen Logiken für hybride Systeme ($\mathsf{d}\mathcal{L}$ [Pla08b] und deren sukzessive Erweiterungen DAL [Pla08a] und dTL [Pla07]), die die logische Quintessenz der Dynamik hybrider Systeme prägnant erfassen. Diese Logiken bieten eine uniforme Semantik und auf den Punkt gebrachte Sprache zur Spezifikation und Verifikation von Korrektheitseigenschaften allgemeiner hybrider Systeme selbst mit nichtlinearer Dynamik. Dies funktioniert sogar in der Gegenwart von Störungen in der Systemdynamik. Der praktische Hauptbeitrag ist ein Beweisverfahren, welches das Verhalten hybrider Systeme axiomatisiert: ein gut automatisierbarer, analytischer Sequenzenkalkül zur Analyse des Systemverhaltens. Dank weiterer Beiträge zum automatischen Beweisen (freie reelle Variablen und Skolemisierung mit Quantorenelimination) und der kompositionellen Natur des Verifikationsansatzes ist das Verfahren praktisch gut einsetzbar. Insbesondere für parametrische hybride Systeme, also Systeme mit symbolischen Parametern statt speziellen Zahlen in der Systemdynamik, ist das Verfahren effizient.

Theoretische Hauptbeiträge Die eingeführten Beweisverfahren werden als vollständig relativ zur Differentialgleichungsbehandlung nachgewiesen. Dies ist der erste relative Vollständigkeitsbeweis für Beweisverfahren hybrider Systeme und überhaupt der erste formale Begriff hybrider Vollständigkeit. Diese Resultate bringen hybride und kontinuierliche Verifikation beweistheoretisch in Deckung und zeigen, dass hybride Systeme mit interagierenden, sich wiederholenden diskreten und kontinuierlichen Evolutionen verifiziert werden können, wann immer dies mit Differentialgleichungen möglich ist.

Algorithmische Hauptbeiträge Die Arbeit stellt *differentielle Induktion* vor, mit der Eigenschaften von Differentialgleichungen sowie differential-algebraischer Gleichungen anhand ihrer lokalen Dynamik nachgewiesen werden können ohne sie lösen zu müssen. Differentialgleichungen praktischer Systeme, wie die der Flugdynamik, können meist nicht explizit gelöst werden oder fallen ausserhalb entscheid-

Abbildung 5: Differentielle (In-)varianten F für Sicherheit und Lebendigkeit

barer Arithmetik. Differentielle Invarianten, F, hingegen, ändern ihren Wahrheitswert längs der Differentialgleichungen $x_1' = \theta_1, \ldots, x_n' = \theta_n$ nicht, und können mit einfachen Bedingungen an symbolische Richtungsableitungen charakterisiert werden, vrgl. Abb. 5:

$$\bigwedge_{(b\sim c)\in F} \left(\left(\sum_{i=1}^{n} \frac{\partial b}{\partial x_i}\theta_i \right) \sim \left(\sum_{i=1}^{n} \frac{\partial c}{\partial x_i}\theta_i \right) \right) \text{ für Teilformeln } b \sim c \text{ mit } \sim \in \{=, \geq, >, ..\}$$

Die Invarianz der Formel $x^2 \geq 5$ entlang der Differentialgleichung $x' = 3x^3$ etwa kann so rein durch Betrachten der lokalen Dynamik leicht festgestellt werden anhand der Bedingung $\frac{\partial x^2}{\partial x} 3x^3 \geq \frac{\partial 5}{\partial x} 3x^3$, welches die allgemeingültige Formel $2x \cdot 3x^3 \geq 0$ ergibt.

Auf der Basis dieser Beweisverfahren entwickelt die Arbeit ausserdem Fixpunkt-Algorithmen, die die benötigten Invarianten und differentiellen Invarianten berechnen und die zugrundeliegende Systemdynamik bei Bedarf verfeinern. Zusammen mit zahlreichen algorithmischen Verbesserungen der Behandlung reeller Arithmetik sind die vorgestellten Techniken in dem ersten Beweiswerkzeug für hybride Systeme implementiert (Abb. 6).

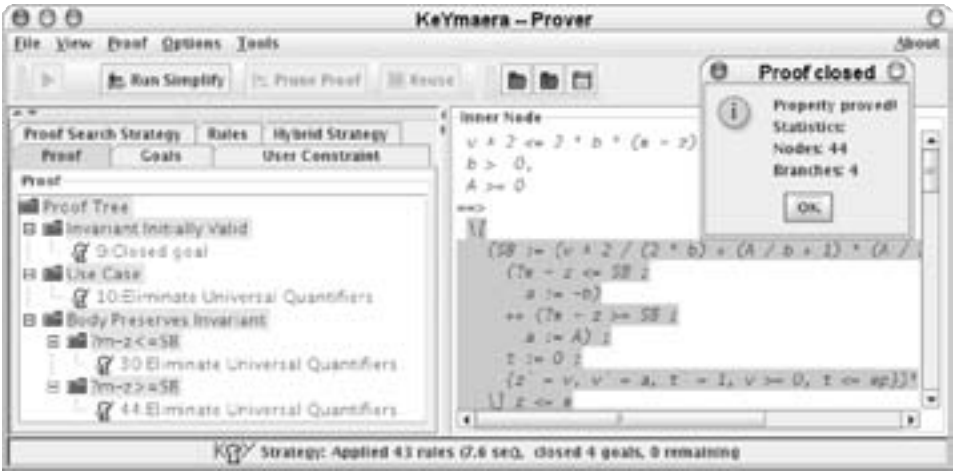


Abbildung 6: Verifikationswerkzeug KeYmaera für hybride Systeme

Angewandte Hauptbeiträge Die Arbeit demonstriert die Fähigkeiten der Logiken, Beweiskalküle und Algorithmen durch Verifikation der Kollisionsfreiheit in realistischen Zugsteuerungsanwendungen und anspruchsvollen Flugmanövern (Abb. 1 und 2). Insgesamt kann der vorgestellte logik-basierte Verifikationsansatz für hybride Systeme realistische Anwendungen verifizieren, die weit ausserhalb der Möglichkeiten bisheriger Ansätze sind, sowohl aus theoretischen Gründen (bisherige Beschränkungen der Systemklassen) als auch Skalierbarkeitsgründen; siehe Tab. 1.

6 Zusammenfassung

Diese Arbeit leistet einerseits Grundlagenforschung, indem sie den weltweit ersten Ansatz zur kohärenten logischen Analyse hybrider Systeme vorstellt, und sogar die relative Vollständigkeit des entwickelten Beweisverfahrens nachweist. In diesem eleganten Rahmen belegt die relative Vollständigkeit ein seit langem ungeklärtes Verhältnis zwischen der Analyse von hybriden Systemen und der Analyse rein kontinuierlicher Systeme beweistheoretisch. Andererseits ermöglichen die entwickelten Analyse- und Beweisverfahren praktische Werkzeuge wie KeYmaera, mit denen realistische Steuerungsmodelle aus dem Zug- und Luftfahrtbereich erfolgreich analysiert und verifiziert werden können. Dadurch leistet die vorgestellte Arbeit gleichermaßen grundlegende Beiträge zur Theorie, Praxis, und Anwendung von Analysemethoden für hybride Systeme, die von bedeutender praktischer Relevanz geprägt und bisherigen Ansätzen in Bezug auf die theoretische Fundierung und Skalierbarkeit auf größere und nichtlineare Systeme deutlich überlegen sind.

Danksagung Diese Arbeit ist im DFG SFB "Automatic Verification and Analysis of Complex Systems" (AVACS) entstanden. Mein besonderer Dank gebührt meinem Doktorvater Prof. Ernst-Rüdiger Olderog, den externen Gutachtern meiner Dissertation, Prof. Tobias Nipkow von der TU München und Prof. George J. Pappas von der University of Pennsylvania und Prof. Werner Damm, Direktor von AVACS, für deren hervorragende Unterstützung meiner Arbeit, sowie Prof. Edmund M. Clarke, der mich mehrfach an die Carnegie Mellon University einlud, für seine wertvolle Hilfe und Unterstützung.

References

[ACH+95] Rajeev Alur, Costas Courcoubetis, Nicolas Halbwachs, Thomas A. Henzinger, Pei-Hsin Ho, Xavier Nicollin, Alfredo Olivero, Joseph Sifakis, and Sergio Yovine. The Algorithmic Analysis of Hybrid Systems. *Theor. Comput. Sci.*, 138(1):3–34, 1995.

[BBM98] Michael S. Branicky, Vivek S. Borkar, and Sanjoy K. Mitter. A Unified Framework for Hybrid Control: Model and Optimal Control Theory. *IEEE T. Automat. Contr.*, 43(1):31–45, 1998.

[Bue08] Martin Buehler. Summary of DGC 2005 results. *J Field Robotics*, 23:465–466, 2008.

[DN00] Jennifer M. Davoren and Anil Nerode. Logics for Hybrid Systems. *IEEE*, 88(7):985–1010, 2000.

[Eme90] Allen Emerson. Temporal and Modal Logic. In Jan van Leeuwen, editor, *Handbook of Theoretical Computer Science, Volume B: Formal Models and Sematics (B)*, pages 995–1072. MIT Press, 1990.

[ERT02] ERTMS User Group. ERTMS/ETCS System Requirements Specification, 2002. Version 2.2.2.

[Fre05] Goran Frehse. PHAVer: Algorithmic Verification of Hybrid Systems Past HyTech. In Manfred Morari and Lothar Thiele, editors, *HSCC*, volume 3414 of *LNCS*, pages 258–273. Springer, 2005.

[LLL00] Carolos Livadas, John Lygeros, and Nancy A. Lynch. High-Level Modeling and Analysis of TCAS. *Proc. IEEE - Special Issue on Hybrid Systems: Theory & Applications*, 88(7):926–947, 2000.

[PC08] André Platzer and Edmund M. Clarke. Computing Differential Invariants of Hybrid Systems as Fixedpoints. In Aarti Gupta and Sharad Malik, editors, *CAV*, volume 5123 of *LNCS*, pages 176–189. Springer, 2008.

[PDP01] Robert S. Parker, Francis J. Doyle, and Nicholas A. Peppas. The intravenous route to blood glucose control. *IEEE Engineering in Medicine and Biology*, 20(1):65–73, 2001.

[Pla07] André Platzer. A Temporal Dynamic Logic for Verifying Hybrid System Invariants. In Sergei N. Artëmov and Anil Nerode, editors, *LFCS*, volume 4514 of *LNCS*, pages 457–471. Springer, 2007.

[Pla08a] André Platzer. Differential-Algebraic Dynamic Logic for Differential-Algebraic Programs. *Journal of Logic and Computation*, 2008. To appear.

[Pla08b] André Platzer. Differential Dynamic Logic for Hybrid Systems. *Journal of Automated Reasoning*, 41(2):143–189, 2008.

[Pla08c] André Platzer. *Differential Dynamic Logics: Automated Theorem Proving for Hybrid Systems*. PhD thesis, Department of Computing Science, University of Oldenburg, 2008.

[Pra76] Vaughan R. Pratt. Semantical Considerations on Floyd-Hoare Logic. In *FOCS*, pages 109–121. IEEE, 1976.

[Sib75] Konstantin S. Sibirsky. *Introduction to Topological Dynamics*. Noordhoff, 1975.

[TPS98] Claire Tomlin, George J. Pappas, and Shankar Sastry. Conflict resolution for air traffic management. *IEEE T. Automat. Contr.*, 43(4):509–521, 1998.

André Platzer erhielt 2004 sein Diplom in Informatik an der Universität Karlsruhe (TH) und 2008 seinen Doktortitel in Informatik an der Universität Oldenburg, beide mit Auszeichnung. Unmittelbar nach seiner Promotion nahm Dr. Platzer einen Ruf an als Assistant Professor im Computer Science Department der Carnegie Mellon University, Pittsburgh, PA, USA. Zu seinen Forschungsinteressen zählen die Verifikation hybrider Systeme, Logiken, Beweisverfahren und Model Checking, sowie Techniken aus dem Bereich symbolisch-numerischer Verfahren. André Platzer ist Autor von 18 Veröffentlichungen, darunter 3 Zeitschriftenartikeln. Er ist alleiniger Autor oder Hauptautor der Mehrzahl dieser Publikationen. Dr. Platzer begutachtet regelmässig Beiträge für die bedeutendsten Fachzeitschriften und internationalen Konferenzen im Bereich formaler Methoden. Seine Arbeiten wurden mehrfach mit Preisen ausgezeichnet, unter anderem dem Best Paper Award der TABLEAUX, dem Woody Bledsoe Award, dem Berkman Faculty Development Award und dem Dean's Innovation Fund Award der Carnegie Mellon University. Neben der Forschung widmet sich Asst. Prof. Platzer der Betreuung mehrerer Studenten und Doktoranden und hält Vorlesungen über hybride Systeme, automatisches Beweisen und Entscheidungsprozeduren an der Carnegie Mellon University.