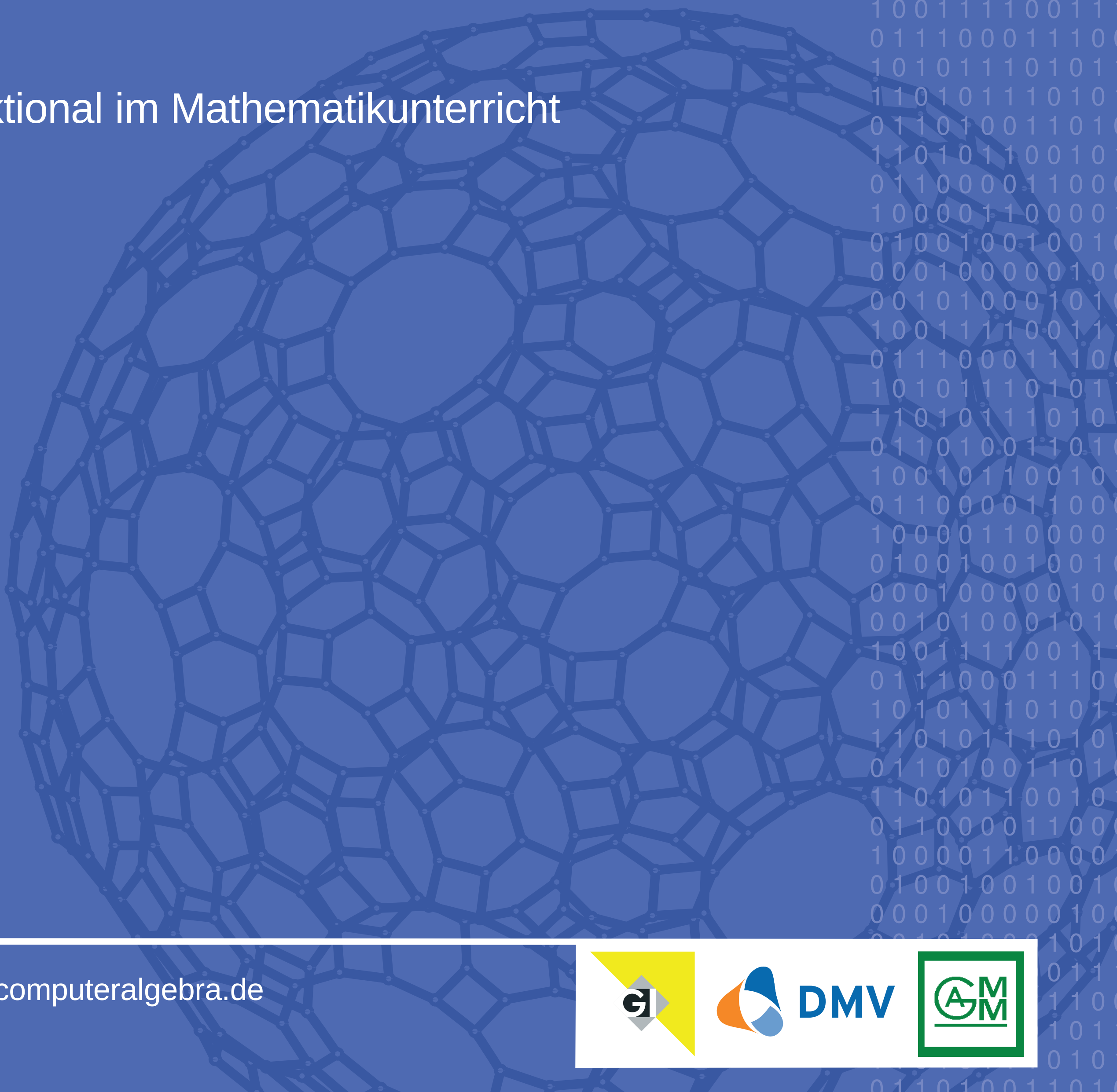
Oktober 2015

Computeralgebra Rundbrief

> Ausgabe 57

- Lernen durch Matrixvervollständigung
- Tropical Geometry in SINGULAR
- CAS funktional im Mathematikunterricht



www.fachgruppe-computeralgebra.de

GI DMV GAMM

Impressum

Der Computeralgebra-Rundbrief wird herausgegeben von der Fachgruppe Computeralgebra der GI in Kooperation mit der DMV und der GAMM (verantwortlicher Redakteur: Prof. Dr. Michael Cuntz, car@mathematik.de)

Der Computeralgebra-Rundbrief erscheint halbjährlich, Redaktionsschluss 15.02. und 15.09. ISSN 0933-5994. Mitglieder der Fachgruppe Computeralgebra erhalten je ein Exemplar dieses Rundbriefs im Rahmen ihrer Mitgliedschaft. Fachgruppe Computeralgebra im Internet: http://www.fachgruppe-computeralgebra.de.

Konferenzankündigungen, Mitteilungen, einzurichtende Links, Manuskripte und Anzeigenwünsche bitte an den verantwortlichen Redakteur.

GI (Gesellschaft für Informatik e.V.)
Wissenschaftszentrum
Ahrstr. 45
53175 Bonn
Telefon 0228-302-145
Telefax 0228-302-167
gs@gi-ev.de
http://www.gi-ev.de

DMV (Deutsche Mathematiker-Vereinigung e.V.)
Mohrenstraße 39
10117 Berlin
Telefon 030-20377-306
Telefax 030-20377-307
dmv@wias-berlin.de
http://www.dmv.mathematik.de

GAMM (Gesellschaft für Angewandte Mathematik und Mechanik e.V.)
Technische Universität Dresden
Institut für Statik und Dynamik der Tragwerke
01062 Dresden
Telefon 0351-463-33448
Telefax 0351-463-37086
GAMM@mailbox.tu-dresden.de
http://www.gamm-ev.de

Computeralgebra-Rundbrief

Nr. 57 Oktober 2015

Inhaltsverzeichnis

Mitteilungen der Sprecher

Liebe Mitglieder der Fachgruppe Computeralgebra,

am 28. September 2015 traf sich die Fachgruppenleitung an der Universität Kassel zu ihrer Herbstsitzung. Auf dieser hat Herr Heß, der bisherige Sprecher, den Stab an Herrn Kemper weitergegeben. Dies war auf der Sitzung im Frühjar 2014 bereits so vereinbart worden. Wir danken Herrn Heß für alles, was er in den letzten drei Jahren für die Fachgruppe getan hat. Beipielsweise hat er sicher durch die Verhandlungen über eine neue Ordnung der Fachgruppe navigiert, die die Kooperationen mit den beteiligten Gesellschaften (DMV, GI und GAMM) auf (steuer-)rechtlich solide Füße stellt. Herr Heß übernimmt nun das Amt des stellvertretenden Sprechers, er wird also auch in Zukunft sehr aktiv bleiben.

Herr Heß wird außerdem weiter Mitglied im Steering Committee der ISSAC bleiben, eine der wichtigsten Konferenzen über symbolisches und algebraisches Rechnen. Bei der diesjährigen ISSAC hat die Fachgruppe Preise für das beste Poster und die beste Software-Vorstellung gesponsert. Mehr hierzu in den Konferenzberichten des vorliegenden Hefts. Dies enthält wie immer auch Informationen über zukünftige Konferenzen, wobei an dieser Stelle schon auf das Minisymposium „Computeralgebra" der gemeinsamen Tagung der DMV und GAMM im März 2016 in Braunschweig hingewiesen sei, das unter starker Beteiligung der Fachgruppe organisiert wird.

Die nächste Computeralgebra-Tagung der Fachgruppe wird im Frühjahr 2017 in Kassel stattfinden. Wer die Tagung schon im Jahr 2016 erwartet hat, findet die Erklärung für die Jahreswahl in der Tatsache, dass 2016 der DFG-Schwerpunkt „Algorithmic and Experimental Methods in Algebra, Geometry and Number Theory " ausläuft, weshalb wir im kommenden Jahr eine Menge an Aktivitäten und Veranstaltungen im Bereich Computeralgebra erwarten.

Neben den üblichen Rubriken wie Buchbesprechungen, Konferenzen und Promotionen enthält diese Ausgabe des Rundbriefs vier Artikel, die ganz verschiedene Zielgruppen ansprechen, so dass wir die Hoffnung haben, dass für jeden Leser etwas dabei ist.

An dieser Stelle sei dem Redakteur des Rundbriefes, Herrn Michael Cuntz, ganz herzlicher Dank ausgesprochen. Bei ihm laufen die Fäden (sowie die Dateien) zusammen, und es erfordert jedes Mal einiges Geschick, in Technik und im Management, um diese zu einem fertigen Heft zu verknüpfen.

Zum Schluß bitten wir Sie wie immer, die Rundbrief-Redaktion mit weiteren Informationen, Themenvorschlägen, Beiträgen, Berichten über Promotionen und Habilitationen, Hinweisen auf Bücher, auf Programmpakete und auf Tagungen etc. zu unterstützen.

Wir wünschen Ihnen eine angenehme und anregende Lektüre dieses Hefts.

Gregor Kemper *Florian Heß*

Lernen durch Matrixvervollständigung

F. Kiraly
(University College London)

f.kiraly@ucl.ac.uk

Ein Sudoku-Exkurs

Vermutlich werden Sie, geneigter Leser, und die meisten Menschen in Ihrem Bekanntenkreis, von Sudoku gehört haben - den ursprünglich aus den USA stammenden Zahlenrätseln, bei denen man in eine mit Zahlen unvollständig ausgefüllte Tabelle weitere Zahlen einfüllen muss, nach einem fest vorgegebenen Muster. Zum Beispiel dieses hier:

	2	3			1	7		
		8	4	6			1	
9				5			4	8
5		4	3				2	
	9		8	7		1		
1					4	9		5
	7				6	8		2
8		1	7		2			
	6			3				1

Tabelle 1. *Das erste veröffentlichte Sudoku (bzw. eines der zwei ersten), im Jahre 1979 erschienen unter dem Namen "Number Place" in einer amerikanischen Rätselzeitschrift [3, 8]. Ziel ist es, die ganzen Zahlen zwischen (einschließlich) 1 und 9 so einzufüllen, dass in jedem 3x3-Block, jeder Zeile, und jeder Spalte jede dieser Zahlen genau einmal auftritt. Zusätzliche Hilfestellung: in der korrekten Lösung enthalten die Kreise die Zahlen 4,5,7,8.*

Sudokus (oder Sudokui? Sudokuta? Sudöker?), wie zum Beispiel das in Tabelle 1, entsprechen somit dankbarerweise dem gemeinhin verbreiteten und akzeptierten Klischee der Mathematik: überall Zahlen, kompliziert, schwer verständlich, und vollständig unnütz. Dies harmoniert passgenau mit dem Bild des Klischeemathematikers, der den ganzen Tag über geistesabwesend im Kopf oder an der Kreidetafel Sudokus löst, während er sich ab und zu den von Essensresten angegilbten, knielangen Bart krault, dabei manchmal Dinge raunt wie "ja, das ist es" oder "elementar, Watson" (in Abwesenheit eines Watson). Eines Tages springt er aus seinem seltenen Bade, läuft "Heureka" schreiend, wild gestikulierend, nur vom Barte bedeckt, durch die Gassen, und wird von einer Pferdekutsche überfahren. Am Rande nur sei angemerkt, dass alle Klischeemathematiker selbstverständlich männlich sind, auch die weiblichen (siehe: Bart). Klischees und Stereotype zu hinterfragen ist natürlich immer unangebracht.

Wie dem auch sei, in der real existierenden Welt verhalten sich die meisten Mathematiker doch relativ unauffällig, genauso die glücklicherweise in immer größerer Anzahl real existierenden Mathematikerinnen. Die überwältigende Mehrheit beider ist im Allgemeinen mehr als nur einen Sicherheitsabstand entfernt von der stationären Einweisung.

Und anstelle von abgehobener Gehirnakrobatik geht es in der Mathematik vor allem um folgerichtiges Schlussfolgern, das heißt, möglichst irrtumsfrei Aussagen zu treffen. Man kann das nun, wie Kunst, zum Selbstzweck betreiben, und daran ist auch nichts grundlegend falsch. Zweifelsohne von weitaus größerer gesellschaftlicher Relevanz sind aber die mathematischen und statistischen Modelle, die auf reale Vorgänge anwendbar sind, und somit folgerichtige Schlussfolgerungen über die Realität erlauben. Beispielsweise Maschinen, Autos oder Computer zu bauen; das Wetter vorherzusagen; oder die beste Therapie für eine Krankheit zu finden.

Am Ende dieses Artikels werden wir ein Modell sehen, Sudokus nicht ganz unähnlich, welches Sportergebnisse vorhersagen kann, mit relativ elementarem Wissen über Algebra und Statistik. Was aber viel viel wichtiger ist: wir werden auch sehen, wie man folgerichtig überprüfen kann, ob ein solches Modell und dessen Vorhersagen grober Unfug sind oder nicht. Schließlich ist etwas ja nicht allein dadurch richtig, dass es irgendwo steht, oder in komplizierten Formeln aufgeschrieben wurde - sondern es muss irrtumsfrei begründet werden. Das ist Mathematik.

Über das Vervollständigen der Matrix

Das am Ende vorgestellte Modell (welches wie gesagt unter anderem Sportergebnisse vorhersagen kann) beruht auf einem Prinzip, das dem des Sudoku nicht unähnlich ist: in eine Tabelle nach einem bestimmten Prinzip Zahlen einzutragen. Das Prinzip ist natürlich ein bisschen anders als beim Sudoku, im Folgenden wird die nötige Theorie dazu eingeführt.

Was ist eine Matrix?
Die bessere Frage zu Beginn ist vielleicht: wieso kann man überhaupt etwas vorhersagen, indem man Zahlen in eine Tabelle einfüllt. Die einfache Antwort lautet: dadurch, dass die eingefüllte Zahl selbst die Vorhersage ist. Und dadurch, dass die Tabelle eine Tabelle von Daten bzw. Messwerten ist. Ein Beispiel:

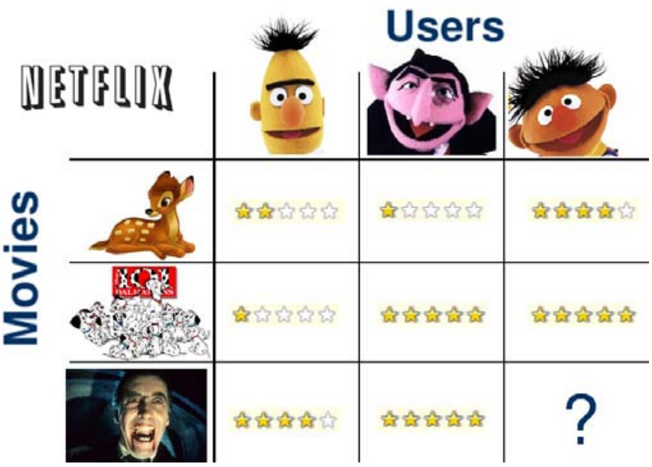


Tabelle 2. *Schematisch vereinfachte Darstellung des "Netflix Prize" Problems, für dessen Lösung die Firma Netflix im Jahr 2006 eine Million Dollar ausschrieb [11]. Zeilen entsprechen Filmen, Spalten entsprechen Benutzern, Einträge entsprechen Bewertungen. Ziel ist es, eine gute Vorhersage für fehlende Bewertungen einzufüllen.*

Tabelle 2 enthält Benutzerbewertungen von Filmen, wie sie zum Beispiel bei Netflix vorgenommen werden. Die verschiedenen Zeilen entsprechen verschiedenen Benutzern, die Spalten entsprechen verschiedenen Filmen. Ein Eintrag ist die Bewertung, die der Benutzer in derselben Zeile dem Film in derselben Spalte gegeben hat. Nicht jeder Benutzer bewertet jeden Film, und nicht jeder Film wird von jedem Benutzer bewertet, daher ist die Tabelle nicht komplett ausgefüllt.

Möchte man nun vorhersagen, wie dem Benutzer X der Film Y gefallen würde, entspricht das der Aufgabe, einen plausiblen Wert für den Eintrag in der X-ten Spalte und der Y-ten Zeile zu finden. Macht man das für alle Filme, die X noch nicht gesehen hat, kann man daraus eine Filmempfehlung ableiten, indem man Filme mit hoher vorhergesagter Bewertung empfiehlt. Ähnlich erhält man eine Produktempfehlung, wenn man "Film" durch "Produkt des Onlinegroßhändlers O" ersetzt. Und so weiter.

Und nun zum Sport:

Athlet	200m	400m	800m	1500m
Bolt	19.19	45.28		
Farah			1:48.69	3:28.81
Johnson	19.32	43.18		
Kipketer		46.85	1:41.11	
Rudisha		45.45	1:40.91	
Yego			1:42.67	3:33.68

Tabelle 3. *Persönliche Bestzeiten einiger Weltspitzenläufer. Ziel ist es, diese in einem Modell zu verstehen. Interessante Fragen in dieser Tabelle wären z. B. die nach Rudishas Potenzial auf 1500m, oder Johnsons 800m-Zeit.*

Tabelle 3 enthält Bestleistungen von Weltspitzenläufern. Zeilen entsprechen den Athleten, Spalten verschieden langen Laufstrecken, und die Einträge den Bestzeiten. Vorhersagen sind hier interessant in Vorbereitung auf eines der längeren Rennen, für die oft eine mehrmonatige Trainingszeit erforderlich ist, wie zum Beispiel dem Marathon; oder, um eine Leistung außerhalb der "typischen" Lauflängen eines Athleten zu schätzen. Zusätzlich und insbesondere ist hier auch wichtig, diese Vorhersagen im Rahmen eines wissenschaftlich spärlichen Modelles zu sehen, welches im Optimalfall Rückschlüsse auf die zugrundeliegende Physiologie erlaubt.

Dem aufmerksamen Leser wird aufgefallen sein, dass die obigen Ausführungen zwar erklären, wieso man durch gutes Einfüllen der Einträge eine gute Vorhersage treffen kann, aber nichts darüber gesagt ist, wie man denn die Einträge nun praktisch einfüllt. Schließlich ist eine Vorhersage nicht allein deswegen gut, weil man irgendetwas eingefüllt hat. Der nächste Abschnitt wird das mathematische Prinzip hinter einer guten Einfüllstrategie beschreiben.

Dazu sei noch kurz die anfängliche Frage beantwortet. Eine Matrix (im mathematischen Sinne) ist die formelle Abstraktion einer Tabelle von Zahlen (ohne Zeilen- und Spaltenbeschriftung). Präziser:

Definition. *Eine (reelle)* Matrix *von Größe* $(m \times n)$, *ist ein tabellarisch geordnetes Tupel A von reellen Zahlen $A_{ij} \in \mathbb{R}$, mit Indizes $i \in \{1, 2, \ldots, m\}$ und $j \in \{1, 2 \ldots, n\}$. Man schreibt kurz $A \in \mathbb{R}^{m \times n}$ und interpretiert A_{ij} als den Eintrag in der i-ten Zeile und j-ten Spalte. Die i-te Zeile ist eine $(1 \times n)$-Matrix und wird mit A_{i*} notiert; die j-te Spalte ist eine $(m \times 1)$-Matrix und wird mit A_{*j} notiert.*

Dem Leser sind Matrizen vermutlich aus den Abiturklassen oder aus dem Studium vertraut, inklusive der üblichen Konventionen im Bezug auf Addition und Multiplikation, die als bekannt vorausgesetzt werden. Auch einem Leser mit abgeschlossenen Mathematikstudium sei die Lektüre der folgenden Abschnitte nahegelegt, da die Interpretation einer Matrix als Modell, und nicht als abstraktes Konzept, möglicherweise ungewohnt vorkommen kann.

Low-Rank Matrix Completion

Ein Einfüllprinzip, mit dem man gute Vorhersagen für Bewertungen und die sportlichen Leistungen bekommt, beruht auf der Annahme, dass die vollständige Matrix einen niedrigen Rang besitzt. Eine mögliche (wenn auch weniger gebräuchliche) Definition für den Rang einer Matrix lautet wie folgt:

Definition. *Sei $A \in \mathbb{R}^{m\times n}$ eine Matrix. Der Rang von A ist die kleinste Anzahl r an Zeilenprototypen $u_1, \dots, u_r$, sodass jede Zeile von A als Linearkombination der u_j dargestellt werden kann, d.h. für alle Zeilennummern i existieren $\lambda_{ij} \in \mathbb{R}$, sodass*

$$A_{i*} = \lambda_1 u_1 + \lambda_2 u_2 + \dots \lambda_r u_r.$$

Die Zeilenprototypen haben eine unmittelbare Interpretation in den Beispielszenarien. Wenn man zum Beispiel animmt, dass die Matrix mit den Filmbewertungen Rang r hat, entpricht das der Annahme, dass es r prototypische Filme oder "Grundgenres" wie Action, Drama, Komödie, etc gibt, aus denen jeder Film (zumindest im Hinblick auf die Bewertungen) zusammengesetzt ist. Die λ_{ij} beschreiben den Anteil des j-ten Genres an i-ten Film. Die Bewertungen der einzelnen Filme werden erklärt als lineare Mischung der Bewertung, die die Prototypen erhalten würden. Ähnlich verhält es sich mit den Sportlern - hier hat man prototypische Athleten, so wie den Sprinter oder den Langstreckenläufer.

Die "Prototypen" müssen hierbei nicht als reale Filme oder Athleten existieren, damit das Modell die Matrizen gut beschreibt. Es sei hier erwähnt, dass obwohl das Modell vielleicht plausibel erscheint, es im Prinzip weder zutreffend noch hilfreich sein muss. Ob die Modellannahme sinnvoll war, muss bei einer praktischen Anwendung immer erst überprüft werden.

Ein grundlegendes Resultat der Matrixalgebra besagt, dass man in der Definition oben für den Rang statt Zeilenprototypen auch Spaltenprototypen nehmen könnte, die Anzahl ist die gleiche. Am einfachsten ist das vielleicht zu sehen, indem man die Definition in Matrix-Multiplikations-Notation umschreibt:

Definition[1]**.** *Sei $M \in \mathbb{R}^{m\times n}$ eine Matrix. Der Rang von M ist die kleinste Zahl r, sodass Matrizen $U \in \mathbb{R}^{m\times r}$ und $V \in \mathbb{R}^{r\times n}$ existieren mit $M = UV$.*

Die Zeilen von U sind u_i, und die Einträge von V sind die λ_{ij} in der ursprünglichen Definition. Die Spalten von V sind Spaltenprototypen, und durch Transponieren von A sieht man, dass die kleinstmögliche Anzahl Zeilenprototypen gleich der kleinsten Anzahl Spaltenprototypen ist.

In den Beispielen bedeutet das, dass im Low-Rank-Modell zu den Filmgenres auch Benutzertypen gehören: Action-Fan, Drama-Fan, Komödien-Fan, usw. Und zu den Musterathleten auch prototypische Aufgaben: z. B. Sprinten, und Langstreckenlauf.

Low-Rank Matrix Completion, also das Einfüllen von Einträgen unter der Annahme niedrigen Ranges (wir wollen den gebräuchlicheren, englischen Ausdruck benutzen), bekommt so die Form eines Rang-udokus. Zum Beispiel diese unvollständige (10×10)-Matrix in Tabelle 4.

Die (von praktischem Nutzen komplett befreite, aber illustrative) Aufgabe ist es, sämtliche Einträge exakt oder mit einer numerischen Präzision von 1e-3 derart einzufüllen, dass die vollständige Matrix einen Rang von 2 besitzt. Es ist durchaus erlaubt, dass eine Zahl pro Zeile oder Spalte mehrmals auftritt, und es dürfen auch irrationale oder komplexe Zahlen eingefüllt werden, wenn es denn hilft.

-4			2	5			3		
4	4	-2							-4
4		-4			-3			6	
			-1	5	0			3	
	-2	2					-4	6	
			0		2	6			-2
					0	4	1		-4
6			-3	-9			-5		
	6					-6		9	-6
	6	-3		-3		-6			

Tabelle 4. *Rang-Rätsel. Ziel ist es, komplexe Zahlen derart einzufüllen, dass die vollständige Matrix Rang 2 hat. Die Lösung ist mit drei Nachkommastellen Präzision gesucht.*

1	2	3	4	5	6	7	8	9	10
2	1	4	3	6	5	8	7	10	9
1	1								
2	1								
1	2								
1	4								
3	1								
4	2								
3	5								
0	1								

Tabelle 5. *Rang-Rätsel. Ziel ist es, komplexe Zahlen derart einzufüllen, dass die vollständige Matrix Rang 2 hat. Die exakte Lösung gesucht.*

[1]Diese Definition des Ranges wird auch der "Zerlegungsrang" genannt. Wer andere Definitionen kennt wie den Zeilen- oder Spaltenrang, die im Abiturunterricht und in Universitätsvorlesungen wesentlich häufiger zu finden sind, sollte die Äquivalenz relativ schnell beweisen können.

Wie man einfüllt

Falls Sie sich am Rätsel versucht haben - falls nicht, würde ich an dieser Stelle darum bitten, dass Sie sich kurz Gedanken machen, wie Sie anfangen würden - wird Ihnen vermutlich aufgefallen sein, dass die Definition des Ranges (Zerlegungsrang, auch der Ihnen möglicherweise bekannte Zeilen-/Spaltenrang) nicht sehr hilfreich ist, um die Einträge einzufüllen. Naives Probieren hilft im Allgemeinen auch nicht, das im Gegensatz zum Sudoku im Prinzip unendlich viele Zahlen in Frage kommen.

Wie so oft besteht auch hier ein gewisser Unterschied zwischen der theoretischen Charakterisierung der Lösung und deren praktischer Konstruktion - den meisten angewandten Wissenschaftlern, sowie den Lesern des Rundbriefs dürfte dieser Unterschied wohl vertraut sein; dieser besteht in der Angabe einer konstruktiven Rechenvorschrift, eines sogenannten Algorithmus. Diesem auf die Spur kommt man vielleicht am besten in einer einfacheren Version des Rätsels, in Tabelle 5.

Die Aufgabe ist wieder die gleiche: alle fehlenden Einträge einzufüllen, sodass die Matrix Rang 2 besitzt, d.h., jede Zeile ist die Summe zweier "Prototypenzeilen". Im Beispiel kann man sich relativ schnell überlegen, dass man ohne Beschränkung der Allgemeinheit die ersten zwei (vollständigen) Zeilen als die Prototypen wählen kann. Da zwei Einträge in jeder anderen Zeile vorhanden sind, kann man die Lösung auf eine Übungsaufgabe in Gauss-Elimination zurückführen.

Die Lösung lässt sich explizit angeben (Kenntnis der Matrixinversen und Determinante vorausgesetzt): ist D die fehlende (8×8)-Matrix, so lassen sich die fehlenden Einträge bestimmen als $D = BA^{-1}C$, wo A die (2×2)-Matrix der ersten zwei Spalten und Zeilen, B die (8×2)-Matrix der ersten zwei Zeilen und letzten acht Spalten, und C die (2×8)-Matrix der letzten acht Zeilen und ersten zwei Spalten. Das heißt, für jeden fehlenden Eintrag D_{ij} gilt die Gleichung $D_{ij} = B_i A^{-1} C_j$, wo B_i die i-te Zeile von B, und C_j die j-te Spalte von C ist. Letzteres ist äquivalent (nach Umstellung und Multiplikation mit $\det(A)$) zur Formel $\det M^{(i,j)} = 0$, wo $M^{(i,j)}$ die Untermatrix mit den drei Zeilen $1, 2, i$ und drei Spalten $1, 2, j$ ist.

Mit anderen Worten, sobald man drei Zeilen und drei Spalten gefunden hat, in deren Schnittmenge insgesamt $8\ (= 3 \times 3 - 1)$ Einträge bekannt sind, kann man diese benutzen, um den neunten durch Auflösung nach der (3×3)-Determinante einzufüllen[2]. Tatsächlich beruht hierauf bereits die Hauptidee des praktischen Algorithmus für Low-Rank Matrix Completion, der sich in [6] findet - mittels weniger beobachteter Einträge die unbekannten einzeln einzufüllen.

Leider ist die Determinanten-Strategie in der obigen Form weder theoretisch noch praktisch zureichend. Zum einen erlaubt sie nicht, alle Einträge einzufüllen, die theoretisch einfüllbar wären. In der Praxis ist sie so nicht verwendbar, da eine Datenmatrix normalerweise mit Messungenauigkeiten behaftet ist und einer Matrix von niedrigem Rang nur nahe kommt.

Die Praxis wird im übernächsten Abschnitt behandelt (schließlich wollen wir ja Sportergebnisse vorhersagen). Der nächste Abschnitt ("Circuits") gibt einen kurzer Ausblick auf interessante theoretische Phänomene und Lösungshinweise zum Rätsel in Tabelle 4, kann jedoch vom Leser auch übersprungen werden; für eine genauere Abhandlung der Theorie sei auf die entsprechende Publikation [6] verwiesen.

Circuits

Ein natürlicher Ausgangspunkt der theoretischen Betrachtungen ist eine weitere Alternativdefinition des Ranges, der sogenannte Determinanten-Rang:

Definition. *Sei $M \in \mathbb{R}^{m \times n}$ eine Matrix. Der Rang von M ist die kleinste Zahl r, sodass die Determinanten aller $(r+1 \times r+1)$-Untermatrizen von M verschwinden.*

Die Äquivalenz zur den vorigen Definitionen des Ranges ist nicht trivial, aber klassisch; man kann diese Äquivalenz verstehen als Begründung einer allgemeineren (für Algebraiker relativ offensichtlichen) Determinanten-Strategie. Leider zeigt zum Beispiel das erste Rang-udoku, dass man im Allgemeinen mit der Determinanten-Strategie alleine nicht weit kommt (das Rätsel ist mit genau dieser bösartigen Absicht konstruiert). Es stellt sich heraus, dass man zu einer Verallgemeinerung der Determinante übergehen muss, sogenannten "Circuits":

Definition. *Sei $C \subseteq [m] \times [n]$ eine Menge von Indizes. C heißt ein Circuit (von Rang r), falls:*

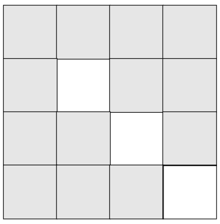
(i) *Für beliebige $e \in C$ lassen sich an den Indizes $C \setminus \{e\}$ beobachtete Einträgen zu einer (nicht notwendigerweise eindeutigen) Matrix von Rang r vervollständigen.*

(ii) *Im Allgemeinen lassen sich an den Indizes C beobachtete Einträge nicht zu einer Matrix von Rang r vervollständigen.*

Zum Beispiel ist jede $(r+1 \times r+1)$-Untermatrix ein Circuit; denn fehlt ein Eintrag, lässt sich dieser mit der Determinanten-Strategie zu einer Rang-r-Matrix vervollständigen (ebenso potenziell fehlende Einträge in anderen Zeilen und Spalten), somit ist Bedingung (i) erfüllt. Kennt man jedoch bereits alle Einträge, hat man im Allgemeinen keine Vervollständigung zu einer Matrix von Rang r - nämlich genau dann wenn die Matrix bereits Rang $r + 1$ hat, da eine solche Matrix auch nicht Untermatrix einer Rang-r-Matrix sein kann.

Allerdings ist nicht jeder Circuit von der Form einer Untermatrix. Beispielsweise kann man zeigen: das Indexmuster

[2] da mit $\det(A)$ multipliziert wurde, ist es notwendig, dass die bekannte (2×3)-Untermatrix vollen Rang besitzt; für eine "allgemeine" oder zufällige Matrix ist das der Fall, im Allgemeinen aber nicht.



ist ein (für das Rätsel in Tabelle 4 übrigens hilfreicher) Circuit von Rang 2. Interessanterweise hat dieser Circuit für allgemeine Matrizen genau zwei Vervollständigungen zu einer (4×4)-Matrix.

Ähnlich wie im Fall von Untermatrizen, kann man von einem Circuit eine Rekonstruktionsvorschrift ableiten:

Theorem. *Sei $C \subseteq [m] \times [n]$ ein Circuit (von Rang r). Dann existiert ein (bis auf Skalarmultiplikation) eindeutig bestimmtes Polynom P_C in den Einträgen einer Matrix M_c, $c \in C$, sodass folgendes gilt: Die Einträge M_c, $c \in C$ können zu einer Rang-r-Matrix vervollständigt werden genau dann, wenn gilt, dass P_C ausgewertet auf den $M_c, c \in C$ verschwindet, i.e., $P_C(M_c, c \in C) = 0$.*

Nach der Definition von Circuits muss jede Variable $M_c, c \in C$ im Circuit nichttrivial auftreten, somit kann man einen einzelnen fehlenden Eintrag e in C durch Auflösen von P_C nach der Variablen M_e bis auf endlich viele Alternativen genau bestimmen. Das Polynom für den $(r+1 \times r+1)$-Untermatrix-Circuit ist die Determinante (als Polynom in den Einträgen betrachtet).

Man sieht leicht, dass Zeilen- und Spaltennummerierung an der Tatsache, dass man einen Circuit vor sich hat, nichts wesentlich ändert; man kann zeigen, dass es selbst mit dieser Äquivalenz unendliche viele Circuits von festem Rang r gibt. Alle Circuits von Rang 1 sind bekannt, für höheren Rang ist das offen.

Es wird vermutet, dass eine vollständige Charakterisierung schwierig ist, da Verbindungen zu anderen, bereits längere Zeit offenen Problemen in der Kombinatorik gibt; aber bitte lassen Sie sich davon auf keinen Fall entmutigen. Beweise und weitere Details finden sich in [6].

Wie man nachprüft, dass die obigen Ideen praktisch funktionieren und die Vorhersagen gut sind

Im vorhergehenden Abschnitt haben wir gesehen, wie sich mittels Determinanten (oder allgemeiner: Circuits) Einträge in eine unvollständige Matrix einfüllen lassen. Selbst schöne theoretische Resultate sind aber keine Garantie, dass die Strategie in der Praxis auch funktioniert, z. B. für die Filmbewertungen oder die Sportergebnisse. Zum einen müssen etwaige Annahmen nicht in den Daten erfüllt sein; und selbst wenn, in der modernen Wissenschaft ist nur systematische Beobachtung von (realen, tatsächlichen) guten Vorhersagen ein ausreichender Nachweis für die Fähigkeit der Methode, gute Vorhersagen zu treffen.

Empirische Validierung

Wie ein solcher Nachweis nach dem Stand der statistichen Wissenschaft erfolgen kann, wird im Folgenden erklärt. Daran lässt sich dann ablesen, ob die naive Strategie "finde eine $(r{+}1{\times}r{+}1)$-Untermatrix mit einem fehlenden Eintrag, fülle diesen mit der Determinante ein" gut funktioniert oder nicht.

Für eine Vorhersagemethode ist, nach dem statistichen Induktionsschluss, eine gute Vorhersagefähigkeit empirisch bestätigt, wenn unter ähnlichen Bedingungen systematisch gute Vorhersagen beobachtet wurden. Um eine solche Vohersage zu simulieren, geht man beispielsweise folgendermaßen vor: ein Eintrag aus der unvollständigen Datenmatrix wird entfernt, und mittels der Methode aus den anderen Einträgen vorhergesagt. Das wird mehrmals wiederholt, und man erhält mehrere vorhergesagte Einträge. Die Vorhersagen werden dann mit den jeweils echten Einträgen verglichen, eine gute Vorhersagemethode besitzt im Durchschnitt einen niedrigen Fehler. Niedrig ist hier immer im Vergleich zu naiven Methoden zu sehen, wie den Eintrag uninformiert zu raten, oder den Mittelwert der Zeile/Spalte einzufüllen.

Wir beschreiben etwas formaler eine Möglichkeit für ein solches sogenanntes Kreuzvalidierungsschema[3]: Seien $x_1, \dots, x_N \in [m] \times [n]$ Indizes, an denen Einträge beobachtet wurden. Seien $y_1, \dots, y_N \in \mathbb{R}$ die dazugehörigen Einträge. Fixiere eine (abstrakte) Vorhersagemethode V.

Schritt 1: *Ziehe zufällig k Indizes $x_{i_1}, \dots, x_{i_k}$ (ohne Zurücklegen).*

Schritt 2: *Benutze die Methode V, um Vorhersagen $f_{i_1}, \dots, f_{i_k}$ für die Indizes zu machen. Zur Vorhersage von f_{i_j} werden alle Index/Eintrags-Paare benutzt außer (x_{i_j}, y_{i_j}), damit es sich auch tatsächlich um ein Vorhersage handelt.*

Schritt 3: *Berechne eine Vorhersagefehlerstatistik, zum Beispiel denn mittleren Absolutfehler (mean absolute error, MAE), der definiert ist als*

$$\text{MAE von } V = \frac{1}{k} \sum_{j=1}^{k} |f_{i_j} - y_{i_j}|.$$

Standardfehler oder Konfidenzintervalle erhält man aus der Stichprobe der Absolutfehler $|f_{i_j} - y_{i_j}|$. Zwei Vorhersagemethoden V_1, V_2 (z. B. Determinanten-Strategie, Mittelwert einfüllen) lassen sich über gepaare Stichprobentests auf den Absolutfehlern vergleichen.

Falls der MAE der Determinanten-Strategie signifikant unter dem MAE einer naiven Strategie (z. B. Mittelwert einfüllen) liegt, kann dann der Schluss getroffen werden, dass die Determinanten-Strategie eine Vorhersage erlaubt, auf dem betrachteten Datensatz.

[3] Das vorgestellte Validierungsschema ist eine Variante der "leave-one-out cross-validation". Der Subsampling-Schritt Nummer 1 ist eine Möglichkeit, um bei großen N Zeit zu sparen; wann immer möglich, wählt man bei der leave-one-out cross-validation $k = N$. Eine Übersicht über andere ebenfalls sinnvolle Vaidierungsschemata und quantitative Schätzgarantien findet sich in [4], Kapitel 7.

Normalerweise werden Methoden auf mindestens zwei Arten von Datensätzen verglichen: einem synthetischen Datensatz, der maschinell mit korrekten Modelleigenschaften (z. B. Rang 2) erzeugt wurde, und einem realen Datensatz.

Wenn die Methode auf dem synthetischen Datensatz Vorhersagen treffen kann, beweist das, dass sie unter den eingebauten Modellannahmen funktioniert. Wenn die Methode auf dem realen Datensatz vorhersagen kann, beweist dies - lediglich genau das. Es zeigt nämlich strenggenommen nicht, dass der reale Datensatz ebenfalls den Modellannahmen folgt, obwohl es das plausibel macht, wenn andere Gründe unplausiblen scheinen. Umgekehrt, wenn die Methode auf dem synthetischen Datensatz vorhersagen kann, aber nicht auf dem realen, liefert das einen starker Hinweis dafür, dass die Modellannahmen für den realen Datensatz nicht zutreffen.

Tabelle 6 zeigt MAE der Determinanten-Strategie "finde eine (3×3)-Untermatrix mit einem fehlenden Eintrag, fülle diesen mit der Determinante ein" und der Strategien "Median der Spalte", und "Mittelwert der Spalte", geschätzt wie oben mit $k = 100$, auf zwei Datensätzen. Bei Datensatz 1 handelt es sich um die komplette (10×10)-Matrix aus dem zweiten Rätsel, mit Rang 2. Bei Datensatz 2 handelt es sich um die Datenmatrix der offiziellen Sportergebnisse von 101.775 männlichen britischen Läufern seit 1954, wie sie in [1] verwendet wurde.

Die Aufgabe in Datensatz 1 ist die Vorhersage eines gleichverteilt zufälligen Eintrages, die Aufgabe in Datensatz 2 ist die Vorhersage einer gleichterteilt zufällig gewählten Marathonzeit.

Methode	Tabelle 5	Athleten
Spalten-Median	1.1 ± 0.2	32 ± 3min
Spalten-MW	1.5 ± 0.2	34 ± 3min
Determinanten	0 ± 0	27 ± 4min

Tabelle 6. *Empirische Vorhersagegüten verschiedener Vorhersagestrategien (Zeilen) auf zwei Datensätzen (Spalten). Tabelle 5 ist eine* (10×10)*-Matrix von Rang exakt 2; der Athleten-Datensatz ist in [1] beschrieben. Die mittleren Absolutfehler sind nach dem beschriebenen Kreuzvalidierungsverfahren, mit* $k = 100$ *geschätzt. Der berichtete Standardfehler ist die empirische Standardabweichung des Mittelwertes der einzelnen Vorhersagefehler (Absolutresiduale).*

Die Ergebnisse zeigen empirisch, dass die Determinanten-Strategie auf der (zweiten) Rätselmatrix perfekt funktioniert, wie erwartet. Leider ist sie auf den Athleten nicht wesentlich besser (im Rahmen des statistischen Unsicherheit) als die naiven Strategien, die überhaupt keine Information über die einzelnen Athleten benutzen - und selbst wenn sie ein kleines bisschen besser wäre, ist die Vorhersage einer Marathonzeit mit einem mittleren (nicht maximalen) Fehler in der Größenordnung von 30 Minuten Abweichung in der Praxis kaum zu gebrauchen. Wie oben ausgeführt, ist sind das alles starke Hinweise darauf, dass ein Rang-2-Modell für die Matrix der Athleten nicht zutrifft, oder präziser, dass mindestens eine der impliziten Annahmen der Determinanten-Vorhersagestrategie nicht, oder nicht gut genug erfüllt ist.

Es rauscht

Nun fragen Sie sich sicher, geneigter Leser, was hier denn falsch gelaufen ist. Immerhin wurde gerade der Nachweis erbracht, dass das oben beschriebene Einfüllen mit Determinanten für die Sportdaten ganz und gar nicht gut funktioniert. Beziehungsweise, genau genommen wurde lediglich beschrieben, wie man die Güte der vorgeschlagenen Methode überprüft. Den nachprüfbaren Nachweis in der Form eines der Tabelle 1 vergleichbaren Ergebnisses erhalten Sie, sobald Sie den entsprechenden Code auf den erwähnten Daten ausgeführt haben ([5]). Es sei angemerkt, dass das durch Glauben der Tabelle 6 nicht ersetzt werden kann, daher sind Sie eingeladen, das auch tatsächlich praktisch in der Realität mit einem Computer zu tun ([5]), und erst daraus korrekt zu schließen, dass die Methode schlecht ist.

Was schief gelaufen ist, ist allerdings nicht nur die Methode. Tatsächlich wurde hier die Erbsünde der modernen Wissenschaft begangen: es wurde von einem Modell ausgegangen, bevor die Daten überhaupt betrachtet wurden; es wurde eine Erklärung für die Realität angeboten, bevor diese überhaupt beobachtet und in einem Experiment geprüft wurde. Das low-rank-Modell wurde Ihnen präsentiert mit Verweis auf die Sport-Anwendung, ohne dass genau erklärt wurde, warum gerade das ein gutes Modell sein soll, oder besser als andere Modelle. Dieser Versuchung zu erliegen ist umso einfacher, je mathematisch schöner und intuitiv plausibler das Modell oder die Erklärung ist, aber Schönheit und Plausibilität einer Annahme machen sie leider nicht wahr.

Natürlich ist das auch ein bisschen der Erzählreihenfolge in diesem Artikel geschuldet, der existierende Resultate wiedergibt; wenn aber erstmals behauptet wird "Modell X ist gut für die Daten Y", dann sind zuerst die Daten Y gut zu untersuchen. Wenn man das im für den Fall der Sportergebnisse macht (siehe [5]), dann sieht man (qualitativ) folgendes ein:

Größere Blöcke in der Matrix haben fast Rang 1, wenn man sie logarithmiert, und

(3×3)-Untermatrizen (nach Logarithmieren) haben fast Rang 2, aber eben nicht ganz.

Beides lässt sich z. B. mit geeigneter Anwendung der Singulärwertzerlegung feststellen.

Aus den obigen Beobachtungen kann man die Hypothese ableiten, dass der *Logarithmus* der Datenmatrix eine *mit Messungenauigkeiten behaftete* Rang-2-Matrix ist. Der Logarithmus macht im Rahmen bekannter Potenzgesetze für sportliche Leistungen Sinn, und Messungenauigkeiten sind ein Standardphänomen auf realen Daten.

Nur den Logarithmus zu nehmen hilft etwas bei der Vorhersage, aber nicht allzu viel. Der genauen Struktur der Messungenauigkeiten kommt man auf die Spur, indem man einen Eintrag fixiert, und viele Vorhersagen durch die Determinanten-Strategie (an Hand verschieden positionierter Untermatrizen) betrachtet.

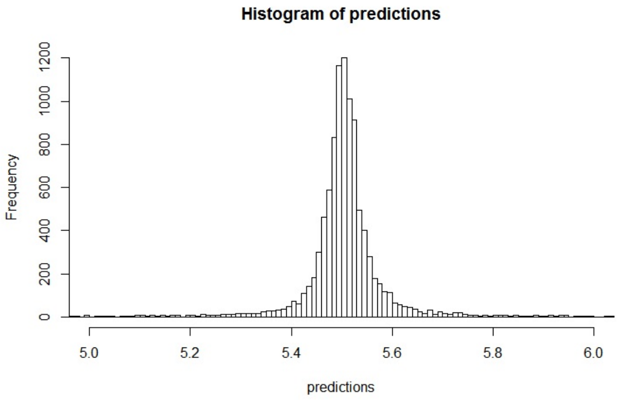


Schaubild. Typisches Histogramm von Vorhersagen durch zufällige Determinanten auf der logarithmierten Matrix der Athleten. Die x-Achse zeigt den vorhergesagten Wert, die y-Achse die Absoluthäufigkeit im jeweiligen Intervall. Zu beoachten ist eine Streuung um den tatsächlichen Wert (hier 5.5), mit einigen Outliern. Typisch ist auch das vereinzelte Auftreten absurd großer Vorhersagen (hier nicht gezeigt).

Das Schaubild zeigt ein typisches Histogramm der Vorhersagen. Man sieht, dass die Vorhersagen um den tatsächlich beobachteten Wert streuen, an den Enden mitunter extrem, aber um den tatsächlichen Wert konzentrieren. Das legt eine leicht verbesserte Strategie[4] nahe: zuerst Logarithmus ziehen; viele Vorhersagen mit der Determinanten-Strategie machen, dann den Median nehmen (robust gegenüber extremen Werten); schließlich exponentieren.

Und siehe da, das funktioniert auch: der MAE einer solchen Strategie auf dem Datensatz beträgt $3.4(\pm 0.5)$ Prozent, das entspricht der gegenwärtig besten bekannten Vorhersagegüte, und einem mittleren Fehler von 3 bis 4 Minuten beim Marathon. Für eine technisch präzisere Beschreibung eines Algorithmus, empirische Ergebnisse, sowie eine ausführliche Behandlung des Themas siehe [1].

Wie oben wird zum Überprüfen dieser Behauptung nachdrücklich eingeladen ([5]). Das Wichtigste ist dazu die empirische Bestimmung des Vorhersagefehlers per Kreuzvalidierung; als zweiten Schritt würde man dieselbe Strategie auf einem oder mehreren synthetischen Datensätzen validieren, der dem reellen nachempfunden ist, und prüfen, ob die Modellannahmen ausschlaggebend waren für die gute Vorhersage.

Des Weiteren würde man immer, auch hier, gerne exakt nachprüfen, warum denn funktioniert, was funktioniert - liegt es am Rang (hier: 2); daran, dass ein Low-Rank-Modell angenommen wurde; und/oder an der speziellen Methode, mit der man die Einträge einfüllt? Vielleicht werden ja nicht alle Komponenten benötigt. Tatsächlich stellt sich heraus, dass andere Methoden, inklusive bekannterer Strategien, die auf der Low-Rank-Annahme beruhen, auch solche mit Rang 2, nicht vergleichbar gut sind; und dass ein Rang von 3 sogar (unter Umständen) noch besser funktioniert. Das genau herauszuarbeiten bedarf aber entsprechend präziser empirischer Vergleiche, daher sei dafür abschließend ein letztes Mal auf das Athletik-Paper [1] verwiesen, und zum eigenen Experimentieren eingeladen.

Ausklang

Und so kann man tatsächlich schlussfolgern, dass Sportergebnisse mit einer Sudoku-ähnlichen Strategie vorhergesagt werden können. Wobei eine solche Schlussfolgerung notwendigerweise auf einer irrtumsfrei folgerichtigen (= mathematisch korrekten) Argumentation und einer präzisen empirisch-experimentellen Validierung beruhen muss - was insbesondere bedeutet, dass irgendwo tatsächlich Sportergebnisse vorhergesagt werden müssen, und dass in Zahlen präzisiert werden muss, wie gut das gelungen ist.

Die besondere Schönheit einer solchen Validierung (wie im vorigen Abschnitt vorgestellt und z. B. in [4], Kapitel 7, ausführlicher erklärt) besteht darin, dass diese unabhängig von der Methode möglich ist, mit der die Vorhersagen erzielt werden; somit können beliebige Methoden auf ihre Vorhersagefähigkeit hin geprüft werden, sei es Raten, Determinanten, oder Krakenorakeln [12].

Um auf die anfängliche Diskussion zurückzukommen, genau darin beruht auch der wichtigste und größte [5] Unterschied zwischen Mathematiker und Klischeemathematiker: in der sorgfältigen Überprüfung von mathematischen und wissenschaftlichen Schlussfolgerungen. Wenn man sich für die reale Welt interessiert, bedeutet das insbesondere eine quantitative und empirisch-experimentelle Bewertung der Hypothesen (z. B. Methode X kann Y gut vorhersagen), die sich dann als falsch oder richtig herausstellen - und dadurch potentiell als praktisch nützlich. Ein bisschen Gehirnakrobatik mag ja dazugehören, aber das ist nicht so wichtig.

[4] Im Fachsprech wird diese Strategie, d.h., viele Vorhersagen auf verschiedenen Teildatensätzen machen und dann den Median nehmen, “bragging” genannt; ein Kofferwortsynonym für “robust bootstrap aggregation”. Bragging ist verwandt mit der bekannteren und älteren, jedoch mathematisch ein bisschen komplizierteren “bagging”-Strategie nach Breiman, welche für die Determinanten-Vorhersagen in [1] verwendet wird. Auf dem Athleten-Datensatz sind bagging und bragging von Determinanten ungefähr gleich gut. Eine Übersicht über Bragging und andere Varianten des Bagging findet man in [2].

[5] wenn auch nicht der einzige. Es stimmt zwar, dass ich (a) an der Kreidetafel und im Kopf schon öfters Rang-Rätsel wie in den Tabellen 5 un 6 gelöst habe, (b) einen Bart trage, (c) beinahe schon überfahren wurde, und (d) mich als Mann fühle. Aber: (a) wie im Artikel erklärt wurde, sind diese tatsächlich praktisch nützlich, (b) es ist ein Schnurrbart, der ohnehin wieder in Mode kommt, (c) das geht den meisten Londonern genauso, und (d) ungefähr die Hälfte unserer Studenten sowie meiner Doktoranden sind weiblich. Mit diesen vier Dingen habe ich übrigens nicht nur kein Problem, sondern bin auch ganz glücklich darüber. Mit Ausnahme von (c) vielleicht.

Ich würde Sie, geneigter Leser, nach diesen Worten herzlich dazu einladen, Tabellen, Daten, oder einfach Fakten, die Sie interessieren, aus einem solchen empirischen Blickwinkel zu betrachten, und in ihnen möglicherweise bisher ungesehene mathematische Gesetzmäßigkeiten - unter Umständen abseits Ihrer Lieblingsmethoden oder Lieblingssichtweisen - zu entdecken.

Falls Sie dafür gerne Anregungen hätten: wie wäre es denn mit den Filmbewertungen, die am Anfang nur relativ kurz besprochen wurden. Den 1-Million-Dollar-Netflix-Preis können Sie zwar leider nicht mehr gewinnen (dieser wurde im Jahre 2009 verliehen), und der Netflix-Preis-Datensatz ist aus Datenschutzgründen ebenfalls nicht mehr verfügbar [7]. Ein gerne genommener Ersatz ist aber z. B. der frei verfügbare MovieLens-Datensatz [10]; oder der Jester-Datensatz, benannt nach einem sich an den Benutzer anpassenden Witzempfehlungsalgorithmus [9].

Oder, falls Sie ein bisschen enttäuscht waren, dass es sich bei dem “Sport” in “Sportergebnisse” um Leichtathletik handelte: wie wäre es mit einem Rätsel wie in Tabelle 7, das einem Sudoku ebenfalls relativ ähnlich ist, und wo in der Regel[6] ebenfalls ganze Zahlen kleiner als 10 eingefüllt werden. So elementar die Fragestellung auch klingt, mit einer guten (d.h. wie beschrieben wissenschaftlich stringenten und statistisch validierten, und nicht einfach irgendeiner Unfugs-)Lösung wären Sie ganz vorne mit dabei im gerade aufkeimenden Forschungsgebiet der quantitativen Sportwissenschaften.

	2		1	0				3
4		1	4			2		2
	1		3	1			3	
2				1		0		1
0	1				0		3	
	3		0		2	2		2
0	2				3		1	
		1		2	2			3
0		0	2				3	

Tabelle 7. *Eine Anregung zur Matrixvervollständigung. Ziel ist es, eine Methode zu finden, die die fehlenden Zahlen gut vorhersagt, und im Optimalfall auch modelliert. Hilfestellung: die (fehlende) Beschriftung der ersten Zeile ist “Bayern München”. Außerdem wurde die alberne Bezeichnung “Fußboku” absichtlich vermieden.*

Ein Rätselhinweis zum Schluss: Low-Rank Matrix Completion ist möglicherweise nicht die beste Methode für die genannten Probleme, und auch nicht die einfachste Methode, die man probieren könnte. Aber vielleicht fällt Ihnen bei der kritischen Betrachtung der Daten ohnehin etwas Besseres ein, genau das ist ja das Spannende an der Wissenschaft.

Literatur

[1] Duncan AJ Blythe, Franz J Király. Quantification and prediction of individual athletic performance. *arXiv*, 1505:01147, 2015.

[2] Peter Bühlmann. Bagging, subagging and bragging for improving some prediction algorithms. *In: Recent Advances and Trends in Nonparametric Statistics*, Elsevier, 2003.

[3] Howard Garns. Number Place. *Dell Pencil Puzzles & Word Games*, 16:6, 1979.

[4] Trevor Hastie, Robert Tibshirani, Jerome Friedman. The Elements of Statistical Learning: Data Mining, Inference and Prediction. Second Edition. *Springer Series in Statistics*, Springer, 2009.

[5] Franz J Király.
`http://mloss.org/software/view/524`

[6] Franz J Király, Louis Theran, Ryota Tomioka. The Algebraic Combinatorial Approach for Low-Rank Matrix Completion. *Journal of Machine Learning Research*, 16(Aug):1391–1436, 2015.

[7] Arvind Narayanan, Vitaly Shmatikov. Robust De-anonymization of Large Sparse Datasets *IEEE Symposium on Security and Privacy*, 111–125, 2008.

[8] Ed Pegg Jr. Sudoku Variations. *mathpuzzle.com*, Sep 6, 2005.

[9] Jester 5.0 - Jokes for your sense of humour
`http://eigentaste.berkeley.edu/`
Abgerufen Oktober 16, 2015.

[10] The MovieLens data
`http://grouplens.org/datasets/movielens/`
Abgerufen Oktober 16, 2015.

[11] The Netflix Prize Rules
`http://www.netflixprize.com/rules`
Abgerufen Oktober 16, 2015.

[12] Wikipedia: Paul (Krake)
`https://de.wikipedia.org/wiki/Paul_(Krake)`
Abgerufen Oktober 16, 2015.

[6] aber nicht immer, wie z. B. am 16. Spieltag der Saison 71/72

Tropical Geometry in SINGULAR

Y. Ren
(TU Kaiserslautern)

ren@mathematik.uni-kl.de

Introduction

Tropical geometry studies balanced polyhedral complexes which arise in numerous areas of mathematics and beyond. In SINGULAR [4] we are naturally interested in its application in algebraic geometry.

Given a polynomial ideal $I \trianglelefteq K[\underline{x}] = K[x_1, \ldots, x_n]$ over a field K with possibly trivial valuation $\nu : K \to \mathbb{R}$, we would like to determine its tropical variety

$$\mathrm{Trop}_\nu(I) := \{w \in \mathbb{R}^n \mid \mathrm{in}_{\nu,w}(I) \text{ monomial free}\},$$

as it inherently carries information about the affine algebraic variety $X := V(I) \subseteq k^n$ cut out by I (see [11] for details). Tropical geometers sometimes refer to them as combinatorial shadows of their algebraic counterparts.

For example, enumerative geometers have been studying tropical varieties to count algebraic curves with carefully chosen characteristics (see Figure 1). While counting, it is important to recognize if multiple objects are casted to the same shadow and, if needs be, determine that number of objects. The theorem that proved this to be possible is referred to as *Mikhalkin's Correspondence Theorem.*

While studying tropical varieties, sometimes it is helpful to compute concrete examples. Up until now, the only software that has been able to do so was GFAN [6] by A. N. Jensen, whose algorithms were developed in a collaboration with Bogart, Speyer, Sturmfels and Thomas [1]. However GFAN is restricted to the rational numbers $K = \mathbb{Q}$ and the valuation $\nu = 0$ being trivial, i.e. p-adic valuations ν_p are excluded. Nonetheless, it is also possible to compute over the field of rational Laurent series $K = \mathbb{Q}((t))$ with its natural valuation thanks to the trick of homogenization and dehomogenization.

The difficulty of non-trivial valuations comes from the fact that the classical Gröbner basis theory does not take any valuations on its ground field into account, as it relies solely on a chosen ordering on the monomials. This makes it unsuited for the problem at hand.

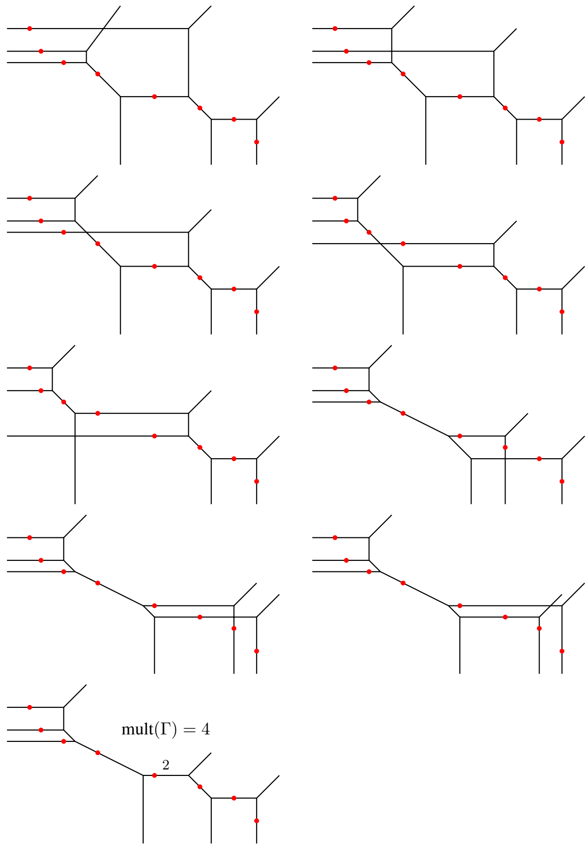


Figure 1: *tropical curves of degree 3 and genus 0 through 8 points in general position*

Progress to date

Ever since version 3-1-6, SINGULAR has been supporting convex geometry thanks to two interfaces [7, 9] to GFANLIB [6] and POLYMAKE [5] respectively. And, in version 4-0-2, we have successfully implemented algorithms for computing tropical varieties over $\mathbb{Q}$ with respect to both trivial and p-adic valuations.

The algorithms for the trivial valuation were taken from the existing work [1], while for p-adic valuations we have developed new techniques that allow us to fall back to the trivial valuation [10]. We are effectively tracing any tropical variety over $\mathbb{Q}$ under a p-adic valuation to a tropical variety over $\mathbb{Z}$ under the trivial valuation. However, the new ideals over $\mathbb{Z}$ are of more general form than the old ideals over $\mathbb{Q}$ for which all existing algorithms were designed, so that new computational approaches had to be developed. During this, we are heavily relying on SINGULAR's native standard basis engine for coefficient rings in arbitrary orderings.

In a way, this new technique can be seen as a generalization of the homogenization and dehomogenization strategy to compute over $\mathbb{Q}((t))$:

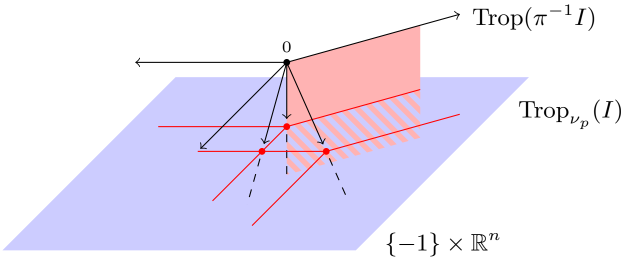


Figure 2: *tropical varieties with p-adic valuation over $\mathbb{Q}$ and trivial valuation over $\mathbb{Z}$ respectively*

During implementation, we paid special attention to unify our new algorithms for tropical varieties over $\mathbb{Z}$ and the existing algorithms for tropical varieties over $\mathbb{Q}$ in a common framework. All algorithms were implemented as part of the GFANLIB interface and are publicly available as part of the official SINGULAR distribution.

To compute tropical varieties, load `gfanlib.so` and use the command `tropicalVariety`. The command takes an ideal as first argument and has an optional second argument depending on which valuation you want to compute with:

```
                     SINGULAR                         / Version
 A CAS for Polynomial Computations                   /   4.0.2
                                                   0<
 Decker, Greuel, Pfister, Schoenemann              \   March
 FB Mathematik der TU Kaiserslautern                \   2015
> LIB "gfanlib.so";
> ring r = 0,(x,y,z,w),dp;
> ideal I = x+2y-3z, 3y-4z+5w;
> tropicalVariety(I,number(2)); // 2-adic val.
RAYS
-2 -1 1 -1 1     # 0
-1 1 -1 1 -1     # 1
0 -3 1 1 1       # 2
0 1 -3 1 1       # 3
0 1 1 -3 1       # 4
0 1 1 1 -3       # 5
LINEALITY_SPACE
0 -1 -1 -1 -1    # 0
MAXIMAL_CONES
{0 1}    # Dimension 3
{0 2}
{0 4}
{1 3}
{1 5}
> tropicalVariety(I,number(3)); // 3-adic val.
> tropicalVariety(I,number(5)); // 5-adic val.
> tropicalVariety(I,number(7)); // 7-adic val.
> tropicalVariety(I,number(11)); // 11-adic val.
> tropicalVariety(I); // trivial valuation
```

Figure 3: *computing tropical varieties of the same ideal with respect to multiple valuations on $\mathbb{Q}$*

As sketched in Figure 2, for p-adic valuations the output is a polyhedral fan whose intersection with the affine hyperplane on which the first coordinate is -1 yields the wanted tropical variety. This is akin to how POLYMAKE represents polyhedra and polyhedral complexes. The tropical varieties are combinatorially of the form:

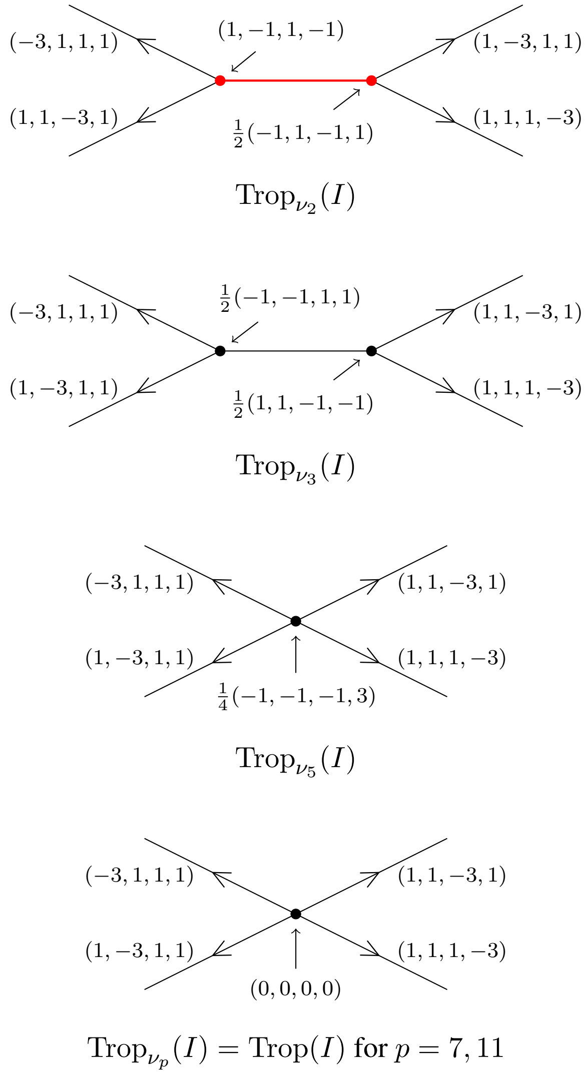


Figure 4: *tropical varieties of the same ideal with respect to multiple valuations on $\mathbb{Q}$*

The intersection of the affine hyperplane with the two highlighted rays in Figure 3 yield two distinct vertices in $\mathrm{Trop}_{\nu_2}(I)$ of Figure 4, whereas the intersection with the highlighted maximal cone yields the bounded edge connecting them. The remaining rays represent points at infinity, which is why the remaining maximal cones represent unbounded edges. The tropical variety has a lineality space generated by the weight vector $(1,1,1,1)$, which is due to the homogeneity of our input ideal.

Note how the tropical varieties dance around for the 2-, 3- and 5-adic valuation before settling to what is obtained with respect to the trivial valuation. This suggests that 2, 3 and 5 are so called bad primes for the modular techniques involving our ideal [2], which is no surprise as they appear as coefficients of our generators.

Current and Future work

One major bottleneck in our computation are standard bases computations over $\mathbb{Z}$ in arbitrary orderings. Thanks to the theory of Gröbner walks, it is only necessary once at the very beginning. There is currently a group of SINGULAR developers actively working on it, including Christian Eder, Anne Frübis-Krüger, Gerhard Pfister and Adrian Popescu, and any improvement will greatly benefit our performance for p-adic valuations. However, it may also be worthwhile to consider algorithms tailored to our ideals which exploit some of the common structure that they share [8].

Moreover, starting with the next version SINGULAR will support modified standard bases algorithms. One promising candidate for tropical computations is the so called *saturating standard bases algorithm*, in which each new basis element is checked for divisibility by the variables. Because we assume our ideal to be saturated with respect to all variables to begin with, we may use it indiscriminately without altering our ideal. This technique was originally applied in the monomial tests during the study of GIT-fans to great success [3], and we hope that it will do equally well in the massive amount of monomial tests in our tropical algorithms.

Feature-wise, the biggest priorities are the computation of multiplicities and the ability to exploit symmetries in our computations.

References

[1] Tristam Bogart, Anders N. Jensen, David Speyer, Bernd Sturmfels and Rekha R. Thomas. Computing tropical varieties. *J. Symbolic Comput.*, 42(1-2):54–73, 2007.

[2] Janko Böhm, Wolfram Decker, Claus Fieker and Gerhard Pfister. The use of bad primes in rational reconstruction. *Mathematics of Computation*, 84:3013-3027, 2015.

[3] Janko Böhm, Simon Keicher and Yue Ren. `gitfan.lib`: A SINGULAR library for computing GIT-fans, 2012.

[4] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister and Hans Schönemann. SINGULAR 4-0-2 — A computer algebra system for polynomial computations, 2015. `https://www.singular.uni-kl.de`.

[5] Ewgenij Gawrilow and Michael Joswig. polymake: a framework for analyzing convex polytopes. In *Polytopes — combinatorics and computation (Oberwolfach, 1997)*, *DMV Sem.* 29:43-74, 2000

[6] Anders N. Jensen. GFAN 0.5, a software system for Gröbner fans and tropical varieties, 2011. `http://home.math.au.dk/jensen/software/gfan/gfan.html`.

[7] Anders N. Jensen, Yue Ren and Frank Seelisch. `gfanlib.so`: A SINGULAR interface to GFANLIB, 2012.

[8] Thomas Markwig, Yue Ren and Oliver Wienand. Standard Bases in mixed Power Series and Polynomial Rings over Rings. arXiv:1509.07528, 2015.

[9] Yue Ren. `polymake.so`: A SINGULAR interface to POLYMAKE, 2012.

[10] Yue Ren. Tropical geometry in SINGULAR. PhD thesis, Technische Universität Kaiserslautern, 2015, `https://kluedo.ub.uni-kl.de/frontdoor/index/index/docId/4169`.

[11] Diane Maclagan and Bernd Sturmfels. Introduction to tropical geometry. volume 161 of *Graduate Studies in Mathematics*, American Mathematical Society, 2015.

OpenDreamKit: Open Digital Research Environment Toolkit for the Advancement of Mathematics[1]

OpenDreamKit Consortium

contact@opendreamkit.org

About

OpenDreamKit is a Horizon 2020 European Research Infrastructure project (#676541) that will run for four years, starting from September 2015. It will provide substantial funding to the open source computational mathematics ecosystem, and in particular popular tools such as LinBox, MPIR, SageMath, GAP, Pari/GP, LMFDB, Singular, MathHub, and the IPython/Jupyter interactive computing environment.

From this ecosystem, OpenDreamKit will deliver a flexible toolkit enabling research groups to set up Virtual Research Environments, customised to meet the varied needs of research projects in pure mathematics and applications, and supporting the full research life-cycle from exploration, through proof and publication, to archival and sharing of data and code.

The project involves about 50 people spread over 15 sites in Europe, with a total budget of about 7.6 million euros. The largest portion of that will be devoted to employing an average of 11 researchers and developers working full time on the project. Additionally, the participants will contribute the equivalent of six other people working full time.

Abstract

OpenDreamKit will deliver a flexible toolkit enabling research groups to set up Virtual Research Environments, customised to meet the varied needs of research projects in pure mathematics and applications, and supporting the full research life-cycle from exploration, through proof and publication, to archival and sharing of data and code.

OpenDreamKit will be built out of a sustainable ecosystem of community-developed open software, databases, and services, including popular tools such as LinBox, MPIR, Sage(sagemath.org), GAP, PariGP, LMFDB, and Singular. We will extend the Jupyter Notebook environment to provide a flexible UI. By improving and unifying existing building blocks, OpenDreamKit will maximise both sustainability and impact, with beneficiaries extending to scientific computing, physics, chemistry, biology and more, and including researchers, teachers, and industrial practitioners.

We will define a novel component-based VRE architecture and adapt existing mathematical software, databases, and UI components to work well within it on varied platforms. Interfaces to standard HPC and grid services will be built in. Our architecture will be informed by recent research into the sociology of mathematical collaboration, so as to properly support actual research practice. The ease of set up, adaptability and global impact will be demonstrated in a variety of demonstrator VREs.

We will ourselves study the social challenges associated with large-scale open source code development and publications based on executable documents, to ensure sustainability.

OpenDreamKit will be conducted by a Europe-wide steered by demand collaboration, including leading mathematicians, computational researchers, and software developers with a long track record of delivering innovative open source software solutions for their respective communities. All produced code and tools will be open source.

Motivation

This proposal grew out of a reflection on the needs of the (pure) mathematics community in terms of computational software and databases. The highly successful development in the last decades of systems such as GAP, LinBox, LMFDB, PARI, Sage, or Singular, has proven the viability and power of collaborative open source development models, by users and for users, even for delivering general purpose systems targeting a large public (researchers, teachers, engineers, amateurs, . . .).

Yet some critical long term investments, in particular on the technical side, are in order to boost the productivity and lower the entry barrier:

- Streamline access, distribution, portability on a wide range of platforms, including High Performance Computers or cloud services.
- Improve user interfaces, in particular in the promising area of collaborative workspaces as those provided by SageMathCloud.
- Lower barriers between research communities and promote dissemination. For example make it easy for a specialist of scientific computing to use tools from pure mathematics, and reciprocally.

[1] Dieser Artikel ist der Seite http://opendreamkit.org entnommen; Abdruck mit freundlicher Genehmigung.

- Bring together the developers communities to promote tighter collaboration and symbiosis, accelerate joint development, and share best practices.
- Outsource as much of the development as possible to larger communities to focus the work forces on their core specialty: the implementation of mathematical algorithms and databases.

Many people in the community have been working really hard on the above items but lack crucially manpower or funding; the purpose is to supply them with such.

The European H2020 call EINFRA-9: e-Infrastructure for Virtual Research Environment was a natural fit: putting the emphasis on Virtual Research Environments nicely wraps up all the above needs in a single aim.

A great opportunity is the rapid emergence of key technologies, and in particular the Jupyter (previously IPython) platform for interactive and exploratory computing which targets all areas of science.

We built the consortium by gathering core European developers of the aforementioned systems for pure mathematics, and reaching toward the numerical community, and in particular the Jupyter community, to work together on joint needs.

By definition this project will be mostly funding actions in Europe; however those actions will be carried out, as usual, in close collaborations with the worldwide community.

Partner

- Jacobs University Bremen
  - Michael Kohlhase
  - Florian Rabe
  - Christian Maeder
  - Mihnea Iancu
- Logilab
  - Florent Cayré
  - Olivier Cayrol
  - David Douard
  - Julien Cristau
  - Serge Guelton
- Simula Research Laboratory
  - Hans Petter Langtangen
  - Min Ragan-Kelley
  - Martin Sandve Alnæs
- University of Kaiserslautern
  - Wolfram Decker
- University of Oxford
  - Dmitrii Pasechnik
  - Ursula Martin
  - Edith Elkind
- University of Sheffield
  - Neil Lawrence
  - Michael Croucher
- University of Silesia
  - Marcin Kostur
  - Jerzy Łuczka
  - Jan Aksamit
- University of Southampton
  - Hans Fangohr
  - Ian Hawke
- University of St Andrews
  - Steve Linton
  - Alexander Konovalov
  - Markus Pfeiffer
- University of Warwick
  - John E. Cremona
- Universität Zurich
  - Paul-Olivier Dehaye
- Université Joseph Fourier
  - Clément Pernet @ClementPernet : site leader
  - Jean-Guillaume Dumas @jgdumas
- Université Paris-Sud
  - Nicolas M. Thiéry
  - Benoît Pilorget
  - Viviane Pons
  - Florent Hivert
  - Samuel Lelièvre
  - Loïc Gouarin
- Université de Bordeaux
  - Vincent Delecroix
  - Karim Belabas
  - Bill Allombert
  - Adrien Boussicault
- Université de Versailles – Saint-Quentin-en-Yvelines
  - Luca De Feo
  - Nicolas Gama

CAS funktional im Mathematikunterricht

H. Körner
(Studienseminar Oldenburg für das Lehramt an Gymnasien)

hen.koerner@t-online.de

Zusammenfassung

Mathematikunterricht mit CAS. Was bleibt? Was ändert sich? In diesem Artikel wird anhand von Beispielen der Einfluss eines so mächtigen Werkzeuges auf Inhalte, Schwerpunkte und Methoden des Mathematikunterrichts diskutiert.

Es sind drei Aspekte, die die grundlegenden Erweiterungen des CAS ausmachen:

(A) Parallele Verfügbarkeit von Termen, Graphen und Tabellen

(B) Algebraisch – syntaktische Fertigkeiten des CAS.

(C) Freie Definition von – auch mehrstelligen – Funktionen.

Die durch (A) bedingten Modifikationen erfolgen schon durch GTR und TK, müssen aber natürlich beim Arbeiten mit einem CAS immer auch integrativ mitgedacht werden. Schon diese Trias „Graph-Tabelle-Term“ nivelliert stark die traditionelle Überbetonung der syntaktisch orientierten Algebra im traditionellen Mathematikunterricht. In diesem Beitrag wird das Augenmerk auf die Möglichkeiten von CAS gelegt, die über GTR und TK hinausgehen. Dies erfolgt anhand unterrichtserprobter Beispiele, die die folgenden zentralen Thesen zur Arbeit mit einem CAS konkretisieren (ausführlicher in [1]).

(1) Die Arbeit mit einem CAS fordert weniger syntaktische Termumformungskompetenz, fördert aber Kompetenz im Erfassen algebraischer Strukturen und Zusammenhänge.

(2) Es wird ein tragfähiges, flexibles Variablenkonzept benötigt. Statisches Termdenken und dynamisches Funktionsdenken müssen in Beziehung gesetzt werden. Die Arbeit mit einem CAS erfordert dann mehr funktionales Denken.

(3) Die Möglichkeit der freien Definition mehrstelliger Funktionen schafft schülerbezogene Gestaltungs- und Untersuchungsmöglichkeiten. Die Arbeit mit einem CAS erfordert dann mehr algorithmisches Denken.

Zu (1): Die pq-Formel

Quadratische Zusammenhänge und damit einhergehende Lösungen von zugehörigen Gleichungen treten in so vielen Verwendungszusammenhängen auf, dass eine Kenntnis und Fertigkeit im Lösen notwendig einzufordern ist. Im technikfreien Unterricht ist dann die Anwendung der pq-Formel oder auch das sukzessive Lösen mit quadratischer Ergänzung das zweckmäßigste Verfahren und als sichere Basiskompetenz einzufordern. Die Verfügbarkeit grafischer Werkzeuge relativiert hier ein erstes Mal: Wer in Anwendungskontexten an konkreten Lösungen interessiert ist, wird mit schnell erzeugbaren grafischen Lösungen (Nullstellen von Parabeln) hinreichend zufrieden sein, Anwendungskontexte erzwingen sowieso Näherungslösungen. Mit einem CAS kommt es zu einer zweiten Relativierung: Wer eine exakte Lösung braucht, erhält sie auf Knopfdruck, auch die pq-Formel selbst. Der Nutzer muss allerdings den Ausdruck und die Termstruktur erfassen, denn zu einem ‚aufklärenden’ Mathematikunterricht gehört auch der verständige Nachvollzug der Genesis der Formel. Dies führt zu einer massiven Verschiebung der Ziele für die Behandlung der pq-Formel: An die Stelle der sicheren Erzeugung von Lösungen zu Fuß („Generieren“) tritt der verständige, Einsicht schaffende Einblick und Umgang mit der Formel („Prozessieren“), Algebra dient der Einsicht, weniger der Erzeugung von Lösungen. Erst wenn erfasst ist, wie sich z. B. die Symmetrie der Parabeln in der Lösungsformel widerspiegelt, wie $-\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$ mit dem Scheitelpunkt $(-\frac{p}{2}|-\frac{p^2}{4}-q)$ zusammenhängt, entsteht verständiges Wissen um quadratische Zusammenhänge und dies ist das entscheidende Motiv für die Behandlung der pq-Formel und quadratischer Ergänzung. Da die Lösungen mit einem CAS auf Knopfdruck erscheinen, wird ein möglichst vorgängiges Erfassen der Gleichungsstruktur wichtiger, Schüler sollten erfassen, dass $\frac{1}{x} = 2x-8$ auf eine quadratische Gleichung führt, $\frac{1}{x^2} = 2x-8$ aber nicht. Gibt ein CAS keine exakte Lösung der zweiten Gleichung an, sollte dies im Unterricht angesprochen werden. Das Reden über Terme gewinnt, das Manipulieren von Termen verliert an Bedeutung.

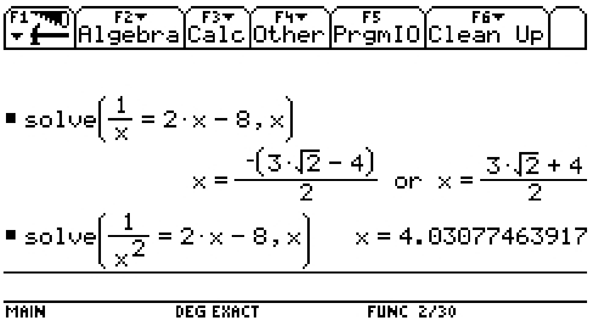


Abbildung 1: *Gleichungen lösen mit CAS.*

Das Lösen quadratischer Gleichungen mit einem CAS zeigt, wie Technologie traditionelle inhaltliche Schwerpunktsetzungen verändern kann (und dann auch sollte) und welchen Stellenwert händische Verfahren dann noch haben. Verallgemeinernd gilt: Die algebraischen Fertigkeiten eines CAS führen zu einem qualitativen und quantitativen Wandel in der Bedeutung und Funktion händischer Verfahren. Sie dienen weniger dazu, eine Lösung zu finden, sondern sollen vielmehr Einsicht in prinzipielle Lösungsmöglichkeiten geben und Transparenz schaffen. Das CAS bietet die Möglichkeit, Kompetenzen im Wechselspiel aus ‚Technikeinsatz' und ‚Lösung von Hand' zu erzeugen, eine undialektische Gegenüberstellung von ‚händisch' und ‚mit Technik' greift jedoch zu kurz und verspielt produktive Möglichkeiten.

Zu (2): Mehrstellige Funktionen statt am Beispiel mehrstelliger Funktionen

Ein grundlegendes Merkmal von CAS ist die Möglichkeit, Formeln als Funktionen zu definieren und diese dann als Makros in Problembearbeitungen einzusetzen.

2.1 Formeln der Geometrie als Funktionen

Wenn schon früh Formeln auch explizit als Funktionen eingeführt werden, z. B. die Flächenformel eines Dreiecks als $A(g,h) = \frac{1}{2} \cdot g \cdot h$, dann findet die wichtige Vernetzung von Formeln und Funktionen entsprechend frühzeitig und explizit statt. Wenn man $F(r) = \pi \cdot r^2$ statt $F = \pi \cdot r^2$ lernt, ist der kovariante Zusammenhang augenscheinlich und heuristisch produktiv. Das Anwenden von Formeln für Flächeninhalte sollte also durch funktionale Betrachtungen und entsprechende Implementierung im CAS ergänzt werden, das CAS wird so zur dynamischen Formelsammlung. Neben die klassische Darstellung der Formel in ihrem syntaktischen Aufbau tritt die Darstellung als Funktion ($\frac{1}{2} \cdot g \cdot h \leftrightarrow A(g,h)$). Letztere ermöglicht dann Untersuchungen mit entsprechenden grafisch-tabellarischen Verfahren indem ein Parameter zum Argument der Funktion wird.

2.2 Ein Klassiker: Die Zinsformel $K(t,p,A) = A \cdot (1+\frac{p}{100})^t$

Typische Fragen im Kontext dieser Formel können folgende sein:

- Wie entwickelt sich ein Kapital von 5000€, das mit 3% jährlich verzinst wird? Wann sind es 8000€?
- Was passiert mit unterschiedlichem Anfangskapital A, wenn es über 5 Jahre mit 3% verzinst wird? Natürlich kann man hier tabellarisch Beispiele durchrechnen und dann entdecken, dass das Kapital um ca. ein Drittel angewachsen ist. Mit funktionaler Brille sieht man aber sofort die Proportionalität:
$$K(A) = (1+\frac{3}{100})^{10} \cdot A \approx 1{,}3439 \cdot A.$$
- Wie entwickelt sich ein Kapital von 5000€ in 10 Jahren in Abhängigkeit des Zinssatzes? Für eine Ausbildung und Schärfung solcher Zusammenhänge helfen grafische Darstellungen (vgl. Abb. 2). Die produktive Heuristik „Variiere einen Parameter, lasse die übrigen fest“, liefert Einsicht in Kovarianzen und Änderungen bei Variationen von Parametern.

Geraden, Parabeln, Potenz- und Exponentialfunktionen haben ihren Auftritt und schärfen den Blick. Denn bei b) könnte man nach der Grafik auch Exponentialfunktionen vermuten. Genaueres Hinschauen („Zoomen“) oder Termkompetenz klären aber auf. Wieder wird syntaktische Umformungskompetenz durch grafisch-tabellarisches Prozessieren mit Formeln ersetzt. An die Stelle von Termumformungskompetenz tritt ‚Funktionskompetenz'.

2.3 Binomialverteilung

Die Formel für die Binomialverteilung kann wie in den vorangestellten Beispielen von Schülern als dreistellige Funktion erzeugt und zur Beantwortung von diesbezüglichen Fragen benutzt werden. Das zweite und dritte Ergebnis machen allerdings stutzig. 5000 ist der Erwartungswert und hat die höchste Wahrscheinlichkeit, die zwar kleiner als die vorher bestimmte ist, aber sicher nicht 0 und auch nicht undefiniert. Was ist passiert? Der im CAS implementierte Befehl (Binompdf) leistet dagegen das Erwartete.

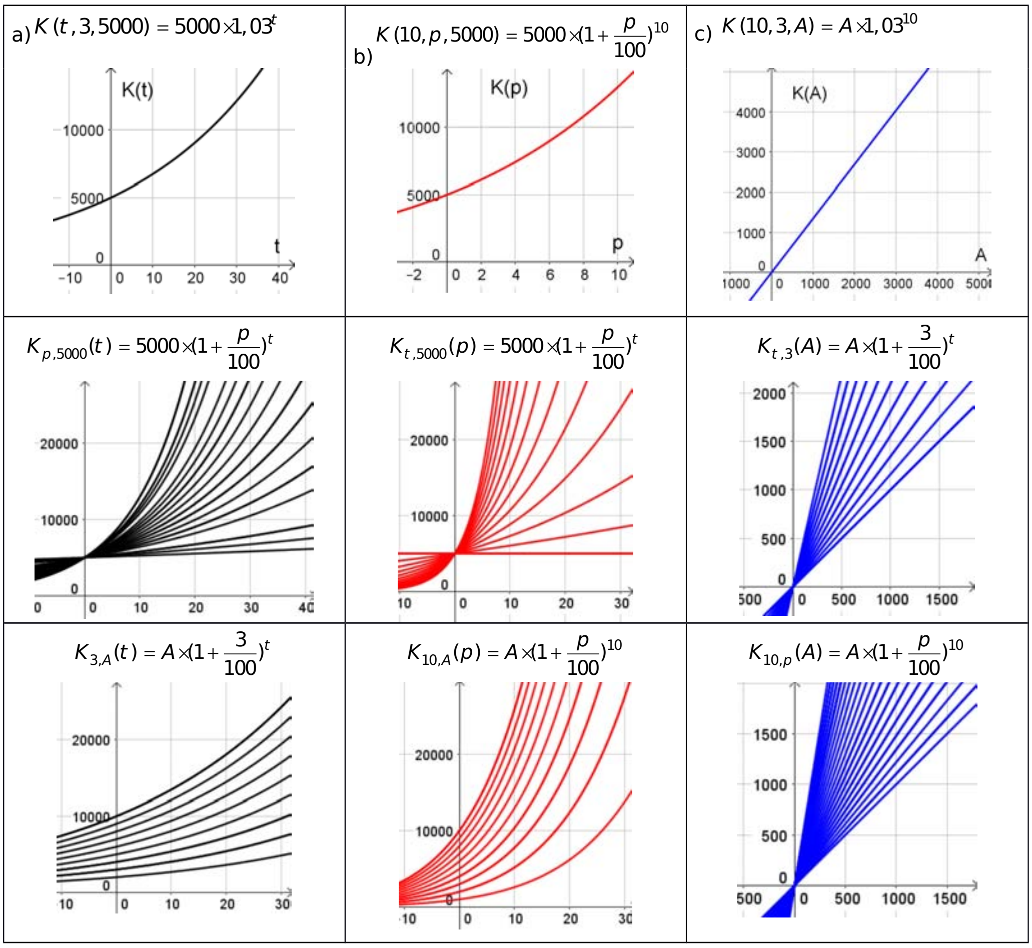


Abbildung 2: *Grafische Darstellungsmöglichkeiten der Zinsformel*

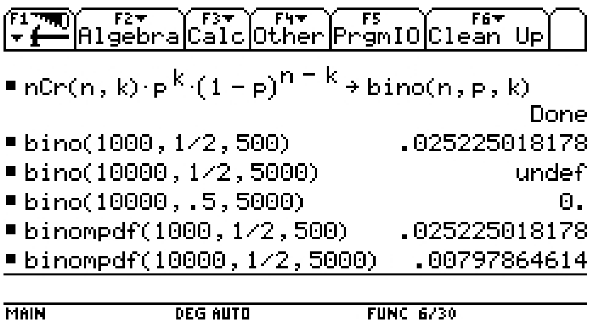


Abbildung 3: *Experimente mit Binomialverteilungen.*

Dies kann ein Beispiel dafür sein, wie das Arbeiten mit einem CAS nicht Mathematik verhindert sondern anregt. Das falsche Ergebnis von „bino“ regt zur Reflexion auf die Struktur der Formel an und man erfasst: Hier werden sehr kleine Zahlen mit sehr großen Zahlen multipliziert. Dies kann zu numerischen Katastrophen bzw. Stellenauslöschung führen. 0,5 und 1/2 sind für das CAS auch nicht dasselbe. In diesem Zusammenhang entsteht die Einsicht, dass es bessere Verfahren (z. B. rekursive) gibt.

Zu (3): Algorithmisches Arbeiten mit mehrstelligen Funktionen

Erarbeitete Formeln können von Schülerinnen und Schülern selbsttätig implementiert werden und dann für komplexere Probleme als Werkzeug benutzt werden. Damit werden die Fertigkeiten des CAS enorm erweitert. Es ist gerade diese Offenheit des CAS, die einen wesentlichen didaktischen Gehalt ausmacht und ein solches Werkzeug so wirkmächtig macht, denn erst in der spezifischen ‚Einrichtung’ des Geräts durch den Nutzer kann sich die Produktivität voll entfalten.

3.1 Änderungsraten/Ableitung

Definiert man die durchschnittliche Änderungsrate als zweistellige Funktion $msek(a, h) = \frac{f(a+h)-f(a)}{h}$, steht ein Werkzeug für die Beschreibung von Änderungen zur Verfügung, das durchgehend in dynamischer Art und Weise grafisch-tabellarisch mit einem CAS genutzt werden kann. Wenn man hier a festhält und h variiert, kann näherungsweise die lokale Änderung an einer Stelle berechnet werden (lokaler Aspekt), hält man h fest und variiert a, kann das lokale Änderungsverhalten für variable Argumente näherungsweise grafisch-tabellarisch untersucht werden (globaler Aspekt).

Zu beachten ist: Die für $h = 0$ entstehende Sekantenfolge ist hier jetzt eine Schar paralleler Geraden und nicht, wie im klassischen Vorgehen, ein Geradenbüschel durch den zu untersuchenden Punkt P. Es wird allein mit dem Konzept „mittlere Änderungsrate“ so flexibel gearbeitet, dass damit alle Fragen zum Änderungsverhalten mit hinreichender Genauigkeit beantwortet werden können. Man erhält vom Nutzer gesetzte Genauigkeiten für gesuchte Werte in Anwendungskontexten, kann aber auch das für Grenzprozesse hier konstitutive Dilemma erleben, dass das, was man eigentlich möchte nicht geht ($h = 0$) und das, was geht, eigentlich das ist, was man nicht möchte. Die Dynamisierung des Differenzenquotienten mit dem CAS fördert und festigt adäquate Grundvorstellungen zum Änderungsverhalten, ist gleichzeitig ein heuristisches Werkzeug zum Entdecken von Zusammenhängen und bereitet neuartige Begriffsbildung (Grenzwert) vor, indem der infinitesimale Prozess durch sukzessives Durchlaufen mit unterschiedlichen Parameterwerten erlebbar wird. Es wird anderseits aber auch deutlich, dass die begriffliche Weitung zum Grenzwert nicht notwendig ist, wenn es allein um das Berechnen hinreichend ‚akzeptabler’ Werte geht, dass „Grenzwertbildung“ ein kognitiver Prozess ist, seine Motivierung also eine innermathematische! Also hilft die Sekantensteigungsfunktion nicht mehr weiter. Terme müssen untersucht werden, Algebra kommt ins Spiel, es müssen Differenzenquotienten für konkrete Funktionen aufgestellt und berechnet werden.

Damit ist ein umittelbares Motiv für eine genauere Untersuchung gegeben, die h-Methode entsteht, aus msek(x, h) wird durch einen gedanklichen Übergang $f'(x)$. Die Ausgabe des CAS kann Motiv für eigene Suche und Aufklärung sein. Will man nun mit den CAS-Ausdrücken den Grenzübergang mit der h-Methode vollziehen, gelingt es unmittelbar nur bei den ersten beiden Beispielen in Abb. 5, bei den übrigen nicht (eine Einbettung in ein durchgehendes Konzept zum Analysisunterricht gibt [2]).

3.2 Mehrschrittige Algorithmen als Formeln

Neben Formeln können auch Algorithmen als mehrstellige Funktionen im CAS definiert werden. Das sukzessive Abarbeiten eines Kalküls wird dann durch eine gezielte Belegung von Argumenten ersetzt (Abb. 6).

a) Gerade durch zwei Punkte (xp—yp) und (xq—yq)

b) Abstand eines Punktes von einer Ebene: „PKEB(vp,vn,d)“

c) Tangente von $y1(x)$ an der Stelle t

d) Trapezsumme für $y1(x)$ von $x = a$ bis $x = b$ mit n Intervallen: „TRAPEZ(a,b,n)“

Die Beispiele zeigen, dass im Verlauf des Unterrichts Schülerinnen und Schüler im CAS eine Formelsammlung erzeugen können, die einen dynamisch, situativen Gebrauch der Formeln gestattet und sie damit zu einem produktiven Werkzeug macht. Die eigene ‚Programmierung’ solcher Formeln setzt aber immer die algebraische Herleitung mit Variablen voraus, so dass die Lernenden unmittelbar die Produktivität und den Mehrwert des Arbeitens mit Variablen und zugehöriger Algebraisierungen erleben können. Grundlegende Fähigkeit beim Arbeiten mit solchen selbst definierten Makros ist die Substitution, die im Grunde schon beim Arbeiten mit den eingebauten Befehlen erforderlich ist. Diese sind eben auch mehrstellige Funktionen, bei deren Anwendung vorgegebene Argumente zielgerecht substituiert werden müssen (solve(Gleichung, Variable)). Unabhängig von allen inhaltsbezogenen Argumenten für das Arbeiten mit selbstdefinierten, mehrstelligen Funktionen, liegt ein weiteres Argument für die Thematisierung dieser Aspekte in der Aufklärung über die Arbeitsweise benutzter Technik. Im CAS gibt es vielfältige, entsprechend vordefinierte Funktionen, deren Erzeugung auf diese Weise durchsichtig gemacht wird. DOTP(Vektor1,Vektor2) (Skalarprodukt) kann ein Schüler auf einfache Weise dann selbst erzeugen. Die Beispiele zeigen weiterhin, dass es zentral um die Entwicklung einer instrumentellen Wechselbeziehung zwischen digitalem Werkzeug und Schüler geht. „Technologische Kompetenz“ heißt dann, dass inhalts- bzw. prozessorientierte Kompetenzen im Dialog mit diesen Werkzeugen erworben werden. Nicht zuletzt zeigen langjährige Unterrichtserfahrungen aber auch: So wie einerseits CAS eine gewisse händische Übungsvielfalt und –tiefe obsolet macht, so erzwingt es andererseits auch umgekehrt gewisse händische Fertigkeiten und Fähigkeiten (Kopfrechnen, Schätzen, Erfassen von Termstrukturen), die ohne CAS vielleicht von geringerer Bedeutung waren. Die durch ein CAS bedingte Beschleunigung bei der Ausführung der Kalküle erzwingt dann, fast dialektisch, eine entsprechende Entschleunigung im händischen Erstzugang. Dies sei abschließend als erstes Axiom technologiegestützten Unterrichts formuliert: Je mehr Technologien in inner- und außermathematischen Anwendungssituationen im Unterricht mit verfahrensbeschleunigenden Effekten eingesetzt werden, desto notwendiger ist eine entschleunigende, verstehensorientierte vorgängige, meist rechnerfreie, Einführung.

Literatur

[1] H. Körner CAS im Mathematikunterricht – Was bleibt? Was ändert sich?. *MU* (60) 1/2014, S.16-29.

[2] H. Körner Vom Bestand zur Änderung und zurück – Ein Konzept für die Analysis. in: Heintz, G., Pinkernell, G., Schacht, F. (Hrsg.): *Digitale Werkzeuge für den Mathematikunterricht*, Festschrift für Hans-Jürgen Elschenbroich, Neuss 2015.

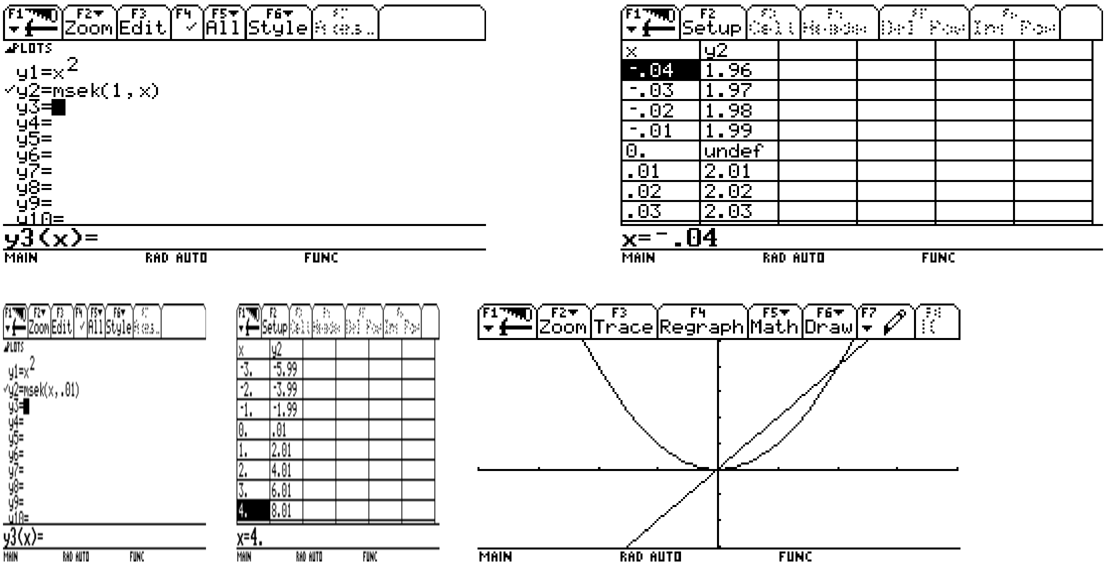


Abbildung 4: *Lokale Änderung an der Stelle x=1: msek(1,x) und die Änderungsratenfunktion (Ableitung): msek(x,0.01)*

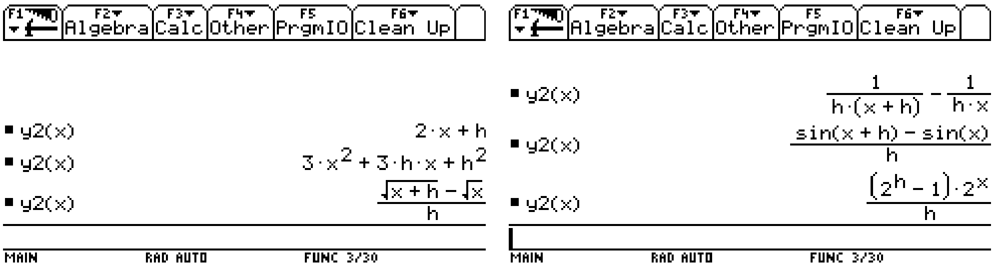
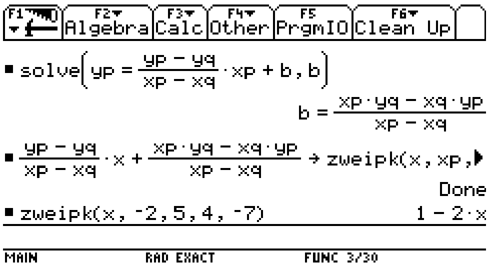
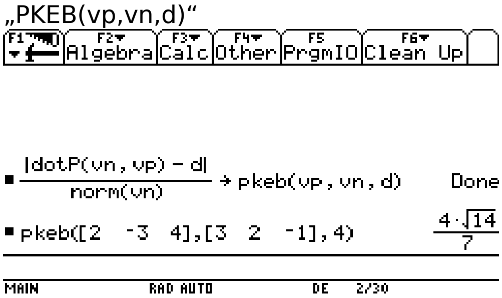


Abbildung 5: *y2(x) als die Sekantensteigungsfunktionen zu y1(x)*

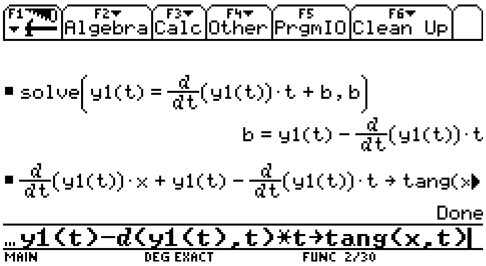
a) Gerade durch zwei Punkte (xp|yp) und (xq|yq)



b) Abstand eines Punktes von einer Ebene: „PKEB(vp,vn,d)“



c) Tangente von *y1(x)* an der Stelle t



d) Trapezsumme für y1(x) von x=a bis x=b mit *n* Intervallen: „TRAPEZ(a,b,n)“

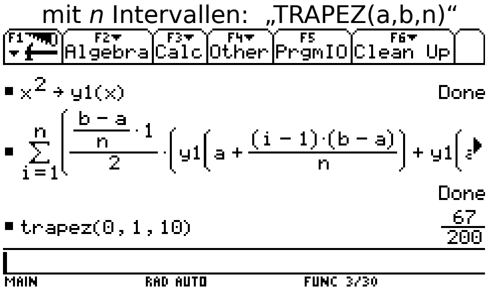


Abbildung 6: *Mehrschrittige Algorithmen*

Promotionen in der Computeralgebra

Felix Grelak:
Affineness of Deligne-Lusztig Varieties
Betreuer: Ulrich Görtz (Essen)
Zweitgutachter: Sascha Orlik (Wuppertal)
Juni 2014

Zusammenfassung: Deligne-Lusztig varieties are varieties over finite fields which were introduced about 40 years ago by Deligne and Lusztig and whcih play a fundamental role in the representation theory of finite groups of Lie type (via their l-adic cohomology). While "most" Deligne-Lusztig varieties are known to be affine varieties, it is still an open question whether this is true in general.

In this thesis, a new combinatorial criterion for affineness of Deligne-Lusztig varieties (refining a criterion by Harashita) is presented. Several combinatorial criteria are evaluated and compared, and new candidates for possibly non-affine Deligne-Lusztig varieties are given.

Furthermore, an algorithm to compute whether a given Deligne-Lusztig variety (for the general linear group) is affine is developed. Because of the large computational complexity of the problem, it was not possible to carry through the computation for new cases, however.

Yue Ren:
Tropische Geometrie in SINGULAR
Betreuer: Thomas Markwig (Kaiserslautern)
Zweitgutachter: Anders N. Jensen (Aarhus)
Februar 2015
`https://kluedo.ub.uni-kl.de/frontdoor/index/index/docId/4169`

Zusammenfassung: Das Ziel dieser Dissertation ist die Entwicklung und Implementation eines Algorithmus zur Berechnung von tropischen Varietäten über allgemeine bewertete Körper. Die Berechnung von tropischen Varietäten über Körper mit trivialer Bewertung ist ein hinreichend gelöstest Problem. Hierfür kombinieren die Autoren Bogart, Jensen, Speyer, Sturmfels und Thomas eindrucksvoll klassische Techniken der Computeralgebra mit konstruktiven Methoden der konvexer Geometrie.

Haben wir allerdings einen Grundkörper mit nichttrivialer Bewertung, wie zum Beispiel den Körper der p-adischen Zahlen $\mathbb{Q}_p$, dann stößt die konventionelle Gröbnerbasentheorie scheinbar an ihre Grenzen. Die zugrundeliegenden Monomordnungen sind nicht geeignet um Problemstellungen zu untersuchen, die von einer nicht-trivialen Bewertung auf den Koeffizienten abhängig sind. Dies führte zu einer Reihe von Arbeiten, welche die gängige Gröbnerbasentheorie modifizieren um die Bewertung des Grundkörpers einzubeziehen.

In dieser Arbeit präsentieren wir einen alternativen Ansatz und zeigen, wie sich die Bewertung mittels einer speziell eingeführten Variable emulieren lässt, so dass eine Modifikation der klassischen Werkzeuge nicht notwendig ist.

Im Rahmen dessen wird Theorie der Standardbasen auf Potenzreihen über einen Koeffizientenring verallgemeinert. Hierbei wird besonders Wert darauf gelegt, dass alle Algorithmen bei polynomialen Eingabedaten mit ihren klassischen Pendants übereinstimmen, sodass für praktische Zwecke auf bereits etablierte Softwaresysteme zurückgegriffen werden kann. Darüber hinaus wird die Konstruktion des Gröbnerfächers sowie die Technik des Gröbnerwalks für leicht inhomogene Ideale eingeführt. Dies ist notwendig, da bei der Einführung der neuen Variable die Homogenität des Ausgangsideal gebrochen wird.

Alle Algorithmen wurden in SINGULAR implementiert und sind als Teil der offiziellen Distribution erhältlich. Es ist die erste Implementation, welche in der Lage ist tropische Varietäten mit p-adischer Bewertung auszurechnen. Im Rahmen der Arbeit entstand ebenfalls ein SINGULAR Paket für konvexe Geometrie, sowie eine Schnittstelle zu POLYMAKE.

Konstantin Ziegler:
Counting classes of special polynomials
Betreuer: Joachim von zur Gathen (Bonn)
Zweitgutachter: Jens Franke (Bonn)
April 2015
`http://hss.ulb.uni-bonn.de/2015/3981/3981.htm`

Zusammenfassung: Die meisten natürlichen Zahlen sind zusammengesetzt und die meisten univariaten Polynome über einem endlichen Körper sind reduzibel. Der Primzahlsatz und ein klassischer Satz von Gauß zählen näherungsweise und exakt die verbleibenden Elemente.

Bei Polynomen in zwei oder mehr Variablen wandelt sich das Bild. Die meisten multivariaten Polynome sind irreduzibel. Wir zeigen Zählergebnisse für Klassen multivariater Polynome über einem endlichen Körper, nämlich die *reduziblen*, die *s-potenzvollen* (teilbar duch die s-te Potenz eines nichtkonstanten Polynoms) und die *relativ irreduziblen* (irreduzibel, aber reduzibel in einer Körpererweiterung). Hierzu präsentieren wir exakte Formeln und Näherungen mit einem relativen Fehler der im Wesentlichen exponentiell in der Eingabegröße abnimmt.

Desweiteren ist ein univariates Polynom f über einem Körper F *zerlegbar*, wenn $f = g \circ h$ mit nichtlinearen Polynomen g und h. Es liegt intuitiv nahe, dass

die zerlegbaren nur eine kleine Minderheit unter allen Polynomen darstellen. Der *zahme* Fall, wenn die Charakteristik p von F kein Teiler von $n = \deg f$ ist, ist gut erschlossen und untere und obere Schranke an die Zahl der zerlegbaren Polynome sind asymptotisch gleich. Im *wilden* Fall, wenn p ein Teiler von n ist, sind die Schranken gröber, insbesondere wenn p der kleinste Primteiler von n ist und n genau zweimal teilt.

Das Zählen mittels Inklusion-Exklusion liegt nahe, erfordert aber das Bestimmen von *Kollisionen*, dass heißt, unter geeigneter Normierung, verschiedener Komponenten (g, h) die das gleiche f ergeben. Im zahmen Fall klassifiziert der Zweite Satz von Ritt alle Kollisionen zweier solcher Paare. Wir zeigen eine Normalform für Kollisionen beliebig vieler Zusammensetzungen mit beliebig vielen Komponenten. Diese Verallgemeinerung liefert eine exakte Formel für die Anzahl der zerlegbaren Polynome vom Grad n, wenn n teilerfremd zu p ist. Im wilden Fall klassifizieren wir alle Kollisionen vom Grad $n = p^2$ und erhalten die genaue Anzahl der zerlegbaren Polynome vom Grad p^2.

Leo Margolis:
Torsionseinheiten in ganzzahligen Gruppenringen nicht auflösbarer Gruppen
Betreuer: Wolfgang Kimmerle (Stuttgart)
Zweitgutachter: Angel del Rio (Murcia), Meinolf Geck (Stuttgart)
Juni 2015

Zusammenfassung: The object of the thesis are torsion subgroups and torsion units of the normalized unit group of integral group rings of finite groups. Two algorithmic methods are the basis for the results. The first one is the HeLP - method which is in the mean time available as GAP - package (developed by A.Bächle and L.Margolis, cf. arxiv.org/abs/1507.08174). The second method is a lattice method for units involving the interplay between ordinary and modular character theory. This new method has been created during the work on the thesis.

Various results on torsion subgroups of the integral group ring of $PSL(2, p^f)$ are presented. In the case when $p = 2$ or $f = 1$ a Sylowlike theorem is established. For some groups even the first Zassenhaus conjecture could be proved. The prime graph question is proved for every $PGL(2, p)$ as well as for M_{10} and $PGL(2, 9)$. The latter completes the proof of Kimmerle and Konovalov on the prime graph question for any group whose orders of almost simple images have at most three pairwise different prime divisors. Moreover the prime graph question for almost simple groups whose order has four different prime divisors is considered. Except for the, maybe infinite, series of such groups isomorphic to $PGL(2, 3^f)$ and five other exceptional groups a positive answer is given.

Marta Pieropan:
Torsors and generalized Cox rings for Manin's conjecture
Betreuer: Ulrich Derenthal (Hannover)
Zweitgutachter: Timothy D. Browning (Bristol), Jürgen Hausen (Tübingen)
Juni 2015

Abstract: The distribution of rational points on Fano varieties over number fields is predicted by Manin's conjecture. For some varieties this can be verified via lattice point counting after a parameterization of the set of rational points via integral points on affine spaces. When the parameterization uses the connection between Cox rings and universal torsors, this approach is known as universal torsor method.

In this thesis the parameterization step is made precise by giving a construction of integral models of torsors via finitely generated Cox rings and by describing explicitely their sets of integral points. These results are then applied to parameterize the rational points on split smooth quartic del Pezzo surfaces and on a split singular quartic del Pezzo surface. They are also used to deduce Manin's conjecture for split smooth proper toric varieties over imaginary quadratic fields.

To adapt the universal torsor method to non-split varieties we introduce the notion of generalized Cox rings and Cox sheaves, and we study their properties and the relation to torsors under quasitori. To illustrate the application to Manin's conjecture, we compute certain generalized Cox rings of Châtelet surfaces.

Yamidt Bermúdez Tobon:
An efficient algorithm to compute an elliptic curve from a corresponding function field automorphic form
Betreuer: Gebhard Böckle (Heidelberg)
Zweitgutachter: Ernst-Ulrich Gekeler (Saarbrücken)
Juli 2015

Abstract: Elliptic modular forms of weight 2 and elliptic modular curves are strongly related. In the rank-2 Drinfeld module situation, we have still modular curves that can be described analytically through Drinfeld modular forms. Gekeler and Reversat prove how the results of Drinfeld can be used to construct the analytic uniformization of the elliptic curve attached to a given automorphic form. Longhi, building on ideas of Darmon, defines a multiplicative integral that theoretically allows to find the corresponding Tate parameter. In this thesis we develop and present a polynomial time algorithm to compute the integral proposed by Longhi. Also we devised a method to find a rational equation of the corresponding representative for the isogeny class.

Melanie Gerling: Eigenschaften chromatischer Polynome
Betreuer: Wolfram Koepf (Kassel)
Zweitgutachter: Peter Tittmann (Mittweida)
Oktober 2015

Zusammenfassung: Die Berechnung des 1912 von Birkhoff eingeführten chromatischen Polynoms eines Graphen stellt bekanntlich ein NP-vollständiges Problem dar. Dieses gilt somit erst recht für die Verallgemeinerung des chromatischen Polynoms zum bivariaten chromatischen Polynom nach Dohmen, Pönitz und Tittmann aus dem Jahre 2003. Eine von Averbouch, Godlin und Makowsky 2008 vorgestellte Rekursionsformel verursacht durch wiederholte Anwendung im Allgemeinen einen exponentiellen Rechenaufwand. Daher war das Ziel der vorliegenden Dissertation, Vereinfachungen zur Berechnung des bivariaten chromatischen Polynoms spezieller Graphentypen zu finden. Hierbei wurden folgende Resultate erzielt:

Für Vereinigungen von Sternen, für vollständige Graphen, aus welchen die Kanten von Sternen mit paarweise voneinander verschiedenen Ecken gelöscht wurden, für spezielle Splitgraphen und für vollständig partite Graphen konnten rekursionsfreie Gleichungen zur Berechnung des bivariaten chromatischen Polynoms mit jeweils linear beschränkter Rechenzeit gefunden werden.

Weiterhin werden Möglichkeiten der Reduktion allgemeiner Splitgraphen, bestimmter bipartiter Graphen sowie vollständig partiter Graphen vorgestellt. Bei letzteren erweist sich eine hierbei gefundene Rekursionsformel durch eine polynomiell beschränkte Laufzeit als effektive Methode.

Ferner konnte in einem Abschnitt zu Trennern in Graphen gezeigt werden, dass der Spezialfall der trennenden Cliquen, welcher im univariaten Fall sehr einfach ist, im bivariaten Fall sehr komplexe Methoden erfordert.

Ein Zusammenhang zwischen dem bivariaten chromatischen Polynom und dem Matchingpolynom wurde für vollständige Graphen, welchen die Kanten von Sternen mit paarweise voneinander verschiedenen Ecken entnommen wurden, sowie für Bicliquen hergestellt.

Die vorliegende Dissertation liefert darüber hinaus auch einige Untersuchungen zum trivariaten chromatischen Polynom, welches auf White (2011) zurückgeht und eine weitere Verallgemeinerung des bivariaten chromatischen Polynoms darstellt. Hierbei konnte gezeigt werden, dass dessen Berechnung selbst für einfache Graphentypen schon recht kompliziert ist. Dieses trifft sogar dann noch zu, wenn man die einzelnen Koeffizienten als bivariate Polynome abspaltet und einzeln berechnet.

Abschließend stellt die Arbeit zu vielen Resultaten Implementierungen mit dem Computeralgebrasystem *Mathematica* bereit, welche zahlreiche Möglichkeiten zu eigenständigen Versuchen bieten.

Habilitationen in der Computeralgebra

Christian Stump:
Coxeter-Catalan structures
April 2015

Abstract: This habilitation thesis at the Freie Universität Berlin is about *Coxeter–Catalan structures*. These are structures appearing in contexts for which there exist classification theorems according to Shephard-Todd or Cartan-Killing types (and as such can be associated to reflection groups), and which are counted by the associated Catalan numbers for reflection groups. The study of these Coxeter–Catalan structures is a highly active area of research within algebraic and geometric combinatorics, with connections to other fields such as invariant theory, algebraic geometry, and representation theory. The key motivation is to uniformly describe similar combinatorial phenomena that can be found in the various fields, and thereby exhibiting relations between a priori unrelated concepts.

Since the earliest appearances in the 1980's in the context of quiver representation theory, Coxeter–Catalan structures were exhibited, mainly within the past 15 years, in the following avenues of research: (1) root systems for semisimple Lie algebras, (2) real and complex reflection groups and the noncrossing partition lattice, (3) cluster algebras and cluster categories, and (4) subword complexes arising in Schubert calculus. Their Coxeter–Catalan structures were established by multiple authors, and as well in this cumulative habilitation thesis. We provide the first uniform approach to connect the Coxeter–Catalan structures in the first two contexts in collaboration with D. Armstrong and H. Thomas. The other parts of this habilitation, partially in collaborations with C. Ceballos, J.-P. Labbé, and V. Pilaud, exhibit the connections of the first three contexts with the forth, thereby showing that subword complexes play a central role in the theory, and using this new context to re-establish previously known results, to obtain new and unexpected results, and to prove previously conjectured results.

An important role in my study of Coxeter–Catalan structures is the usage of computer algebra implementations to provide a framework for computer experiments. That framework allowed me to develop the discussed structures by exploring examples and by gathering data. It moreover greatly helped to formulate and to test conjectures.

Michael Wibmer:
Affine difference algebraic groups
Juni 2015

Abstract: Determining all algebraic relations among special functions and their transforms under various operations like differentiating, shifting, or scaling is a classical and important problem. For example, Hölder's theorem states that the gamma function does not satisfy an algebraic differential equation over $\mathbb{C}(x)$. The relation

$$xJ_{\alpha+2}(x) - 2(\alpha+1)J_{\alpha+1}(x) + xJ_\alpha(x) = 0$$

satisfied by the Bessel function $J_\alpha(x)$ is an example of an algebraic relation with respect to the operation of shifting.

Picard-Vessiot theory provides a formal algebraic approach to studying the algebraic relations among the solutions of a linear differential equation. Indeed, these relations are encoded in a certain algebraic group, called the Galois group of the differential equation and there exist algorithms for computing these groups. These algorithms heavily rely on the structure theory of algebraic groups.

In the last decade there emerged Galois theories for linear differential (or difference) equations that are able to handle not only the algebraic relations among the solutions but also the algebraic relations among the solutions and their transforms under operations like differentiating or shifting. These Galois theories are also known as parameterized Picard-Vessiot theories and several researchers, including Michael Singer, Phyllis Cassidy, Charlotte Hardouin, Lucia Di Vizio, Alexey Ovchinnikov and the author have contributed to their development. In the parameterized Picard-Vessiot theory the Galois groups are not simply defined by algebraic equation as in the standard Picard-Vessiot theory, but the equations defining the Galois groups involve operations like differentiating and shifting. For the operation of differentiating the resulting groups are called differential algebraic groups and there exists a comprehensive theory for these groups initiated by Ellis Kolchin and his school. If the equations defining the group involve operations like shifting or scaling, one speaks of a difference algebraic group. These groups have so far been studied only very little. However, for constructing algorithms to compute the Galois groups in this case a thorough understanding of difference algebraic groups is indispensable.

This is the starting point of the thesis which lays the foundations for a comprehensive theory of difference algebraic groups. The setting is purely algebraic and inspired by difference algebra. The operations of shifting or scaling are replaced by the action of an arbitrary ring endomorphism denoted by σ. The equations defining a difference algebraic group then involve the formal symbol σ, for example the equations

$$Y\sigma(Y)^T = \sigma(Y)^T Y = I_n,$$

where Y is an $n \times n$ matrix of indeterminates, define a difference algebraic subgroup of GL_n. So over the finite field with q elements, if we define $\sigma(a) = a^q$, then the corresponding group is the unitary group $U(n, q)$.

Similarly, any linear difference equation $\sigma^n(y) + \lambda_{n-1}\sigma^{n-1}(y) + \ldots + \lambda_0 y = 0$ defines a difference algebraic subgroup of the additive group $\mathbb{G}_a$.

In this thesis many fundamental results about difference algebraic groups are established, e.g., finiteness theorems, existence and good properties of quotients, a dimension theorem, a Jordan-Hölder type theorem. Several numerical invariants for difference algebraic groups are introduced and studied. Many constructions are inspired by well-known constructions from algebraic groups. The employed tools range from algebraic geometry and the theory of group schemes to commutative algebra and difference algebra. An important special class of difference algebraic groups analogous to étale algebraic groups is studied in great detail and a structure theorem is provided for these groups.

Berufungen

Prof. Dr. Alice Niemeyer hat zum 1. September 2015 eine Professur für Algebra an der RWTH Aachen angetreten. Ihr Arbeitsgebiet ist die algorithmische Gruppentheorie.

Hans-Wolfgang Henn; Andreas Filler
Didaktik der Analytischen Geometrie und Linearen Algebra

Springer Spektrum 2015, 391 Seiten, ISBN 978-3-662-43434-5, €24,99 (als e-book: €19,99)

Der erste Eindruck: Dieses Buch ist von zwei erfahrenen Didaktikern sowohl für die tägliche Unterrichtspraxis als auch für die Lehrerausbildung geschrieben worden. Zahlreiche motivierende realitätsnahe und problemorientierte Aufgabenbeispiele werden ergänzt durch didaktische Analysen und weiterführende Gedanken der beiden Autoren. Es ist zudem eine lohnende Fundgrube für jeden erfahrenen Mathematiklehrer, die weit mehr Beispiele enthält, als man in einem Unterrichtsgang zu dieser Thematik mit einem Oberstufenkurs je behandeln kann. Auf den zweiten Blick bietet dieses Buch jedoch weit mehr!
Die Kapitel des Buches orientieren sich an der typischen Unterrichtsgenese in den Themen Lineare Algebra und Analytische Geometrie: Einer allgemeinen Einführung in die didaktischen Leitgedanken und Ausführungen der Autoren zum Fachanspruch des Buches schließen sich sechs Kapitel über Lineare Gleichungssysteme, dem Vektorbegriff, der Analytischen Geometrie, dem Kontext Matrizen und ein besonders lesenswerter Ausblick an. Durchgängig werden Möglichkeiten für einen sinnvollen Computereinsatz anhand verschiedener Programme aufgezeigt, die kostenlos für alle üblichen Betriebssysteme im Internet erhältlich sind.
Das Kapitel Lineare Gleichungssysteme greift typische Beispiele der Sekundarstufe I auf, erläutert deren Fortführung in die Sekundarstufe II, liefert diesbezüglich viele weitere Kontexte die insbesondere eine Verallgemeinerung auf höhere Dimensionen ermöglichen. Bereits hier verdeutlicht und konkretisiert sich der Anspruch der Autoren, wie Beziehungen zwischen der algebraischen und geometrischen Darstellung von Gleichungen (mit Hilfe von Technologie) aufgezeigt werden können und welche Grundvorstellungen notwendig sind, damit Lernende diesem Anspruch gerecht werden können.
Im Kapitel Vektoren werden verschiedene Auffassungsmöglichkeiten des Vektorbegriffs (z.B. Pfeilklasse oder n-Tupel) analysiert und die Berechtigungen dieser Auffassungen anhand von Beispielen konkretisiert. Ergänzt wird dieses Kapitel durch den Nutzen von Vektoren für Beweise geometrischer Sätze und eine sehr lesenswerte kritische Auseinandersetzung mit dem Begriff „Ortsvektor“.
In den Kapiteln Analytische Geometrie und Vertiefungen und Anwendungen der analytischen Geometrie werden ausgehend von einem historischen Rückblick verschiedene Darstellungs- bzw. Herleitungsmöglichkeiten und Lagebeziehungen von Objekten des dreidimensionalen Raumes diskutiert. Dem Leser sei hier besonders der kritische Blick der Autoren auf Abituraufgaben und die von den Autoren vorgestellten Kontexte unter Einbeziehung von 3D-Computergrafik empfohlen.
Wurden Matrizen bislang nur als Schreibfigur für lineare Gleichungssysteme behandelt, so zeigt das Kapitel Matrizen und affine Abbildungen Kontexte für arithmetische und geometrische Zugänge auf, die das Rechnen mit ihnen motivieren und sie als eigenständige mathematische Objekte rechtfertigen. Besonders gelungen sind hier die reichhaltigen computergestützten Beispiele zu affinen Abbildungen – umso bedauernswerter, dass diese bundesweit in Lehrplänen immer seltener vorkommen.
Im letzten Kapitel Ausblick erhält der Leser Anregungen zum selbständigen Weiterarbeiten und - mit kritisch-historischem Blick auf die nicht aufhörende Diskussion um mathematische Bildung - Anspruch der Autoren an ein den zukünftigen Ansprüchen gerecht werdendes Lehramtsstudium.

In jedem Kapitel zeigen die Autoren mit diesem Buch sehr gelungen auf, wie mit weniger Kalkül und mehr inhaltlich orientierter Analyse des uns umgebenden Raumes die Bereiche Lineare Algebra und Analytische Geometrie in Schule und Hochschule anhand interessante Problemstellungen oder ansprechender geometrischer Objekte vermittelt werden können. Insbesondere das Spiralprinzip und die Herausarbeitung von Beziehungen der Analytischen Geometrie unter Ausnutzung von Methoden der Linearen Algebra sind Leitgedanken, die in diesem Buch gut nachvollziehbar sind und jeden Lehrer sicher zur Nachahmung motivieren.

Jan Hendrik Müller (Plettenberg)

Berichte von Konferenzen

1. **CAPP - Computer Algebra and Particle Physics**

   DESY, Hamburg, 23.03.2015 – 27.03.2015

   `indico.desy.de/conferenceDisplay.py?confId=10282`

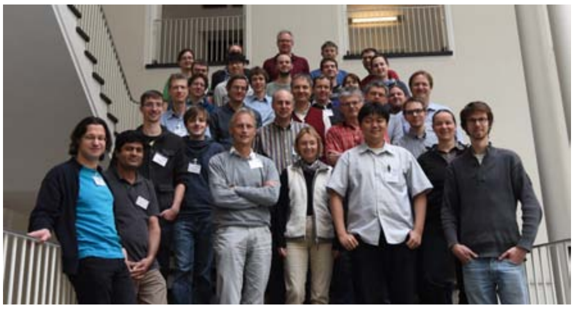
   In March 2015 the 'Computer Algebra and Particle Physics' (CAPP) school took place for one week at the DESY research centre in Hamburg, Germany. About 40 graduate and PhD students participated in this school about calculational tools related to elementary particle physics. A repetition of theoretical basics as well as a short introduction to state-of-the-art trends in this special area of research was given. Computer algebra programs and algorithms were presented as standard tools to deal with the complicated mathematical expressions arising in perturbative calculations within the Standard Model of particle physics and beyond. The lectures given by Sven Moch, Jos Vermaseren, Thomas Hahn, and Peter Marquard introduced different computer algebra programs in an excellent way and demonstrated how these programs can be used to solve the complex tasks which arise in daily particle physics calculations. In addition, the students had the possibility to apply their new knowledge in well-matched exercises.

   Cyril Pietsch (München)

2. **Experimental Methods in Computational Algebra**

   Leibniz Universität Hannover,
   26.05.2015 – 29.05.2015

   `www.icm.tu-bs.de/ag_algebra/Workshop-NTH-II`

   In der Pfingstwoche 2015 fand an der Leibniz Universität Hannover die Tagung 'Experimental Methods in Computational Algebra' statt. Organisiert mit dem Ziel, die Kommunikation zwischen verschiedenen Feldern der algorithmischen und experimentellen Algebra und angrenzender Gebiete zu intensivieren, umfaßte der Workshop 15 Vorträge zu aktuellen Forschungsthemen von Gruppentheorie über Algebraische Geometrie bis hin zu Kryptographie und algebraischer Systemtheorie. Dabei legten alle Vortragenden großen Wert darauf, sich auch an die Nicht-Fachleute im Publikum zu wenden gleichzeitig aktuelle Ergebnisse zu präsentieren. Dank der finanziellen Unterstützung durch den DFG-Schwerpunkt 1489 war es den Organisatoren Bettina Eick, Claus Fieker und Anne Frühbis-Krüger dabei möglich, auch internationale Experten nach Hannover einzuladen, wodurch dieser Workshop im Vergleich zum Vorjahr deutlich mehr Resonanz fand.

   Anne Frühbis-Krüger (Hannover)

3. **ISSAC 2015 – International Symposium on Symbolic and Algebraic Computation**

   University of Bath, 06. – 09.07.2010

   `http://www.issac-conference.org/2015`

   Die ISSAC-Konferenz 2015 fand vom 6. bis zum 9. Juli 2015 im Chancellor's Building auf dem Campus der University of Bath in England statt. Die Leitung lag in den Händen von James Davenport (Local Arragements) und Steve Linton (General Chair). Der Vorsitzende des Programmkomitees war Kazuhiro Yokoyama.

   Konferenzort Chancellor's Buiding auf dem Bath Campus

   Die Konferenz hatte ca. 120 Teilnehmer. Von 74 eingereichten Papers wurden 43 auf der Tagung vorgestellt, ferner gab es 12 Poster und 6 Software Demos. Die Titel aller Präsentationen finden sich auf der Webseite der Konferenz.

   Die Proceedings gab es diesmal nur als USB-Stick, der Erwerb der gedruckten Ausgabe musste trotz der hohen Tagungsgebühren gesondert bezahlt werden; dies wurde dann auch nur von 19 Teilnehmern in Anspruch genommen. Die Artikel stehen auch in der ACM Digital Library zur Verfügung.

   Eingeladene Vorträge wurden von Erika Ábrahám, Éric Schost und Lihong Zhi präsentiert:

   Erika Ábrahám (RWTH Aachen University): Building Bridges between Symbolic Computation and Satisfiability Checking

   Éric Schost (University of Western Ontario, Canada): Algorithms for Finite Fields Arithmetic

   Lihong Zhi (MMRC, Chinese Academy of Sciences, China): Optimization Problems over Noncompact Semialgebraic Sets

   Ferner gab es folgende Tutorials:

   Ankur Moitra (MIT, USA): Nonnegative Matrix Factorization: Algorithms, Complexity and Applications

   Clément Pernet (Grenoble, France): Exact Linear Algebra Algorithmic: Theory and Practice

   Veronika Pillwein (RISC-Linz, Austria): An Introduction to Finite Element Methods

   Die SIGSAM und die Fachgruppe Computeralgebra prämierten die besten Tagungsbeiträge. Die Gewinner des *ISSAC 2015 Distinguished Paper Award* der SIGSAM waren Jean-Guillaume Dumas, Clément Pernet und Ziad Sultan für ihr Paper *Computing the Rank Profile Matrix*, der Gewinner des *ISSAC 2015 Distinguished Student Author Award* der SIGSAM war Sébastien Maulat für *Formulas for Continued Fractions: An Automated Guess and Prove Approach*, einer gemeinsamen Arbeit mit Bruno Salvy.

Distinguished Student Author Award für Sébastien Maulat

Auch die Fachgruppe stellte diesmal wieder einige Preise zur Verfügung. Für die *Beste Software-Demonstration* wurde Bruno Grenet mit *Lacunaryx: Computing Bounded-degree Factors of Lacunary Polynomials* ausgezeichnet. Die Auswahl wurde getroffen von einem Komitee bestehend aus Ernst Mayr und Bill Hart (Fachgruppe Computeralgebra) sowie Bernard Mourrain (Software Presentation Committee Chair) und Steve Linton (General Chair).

Bruno Grenet erhält den Fachgruppenpreis von Ernst Mayr

Als *Beste Poster Presentation* wurde das Poster von Luca De Feo, Christophe Petit und Michael Quisquater zum Thema *Deterministic Root Finding in Finite Fields* ausgewählt. Den Preis nahm Luca de Feo in Empfang. Die Auswahl wurde getroffen von einem Komitee bestehend aus Wolfram Koepf und Ernst Mayr (Fachgruppe Computeralgebra) sowie Yang Zhang (Mitglied des Poster Presentation Committees) und Steve Linton (General Chair).

Luca de Feo mit dem Fachgruppenpreis sowie Wolfram Koepf und Jürgen Gerhard (Maplesoft)

Die beiden Software- und Postersieger erhielten von der Fachgruppe Computeralgebra ein Preisgeld in Höhe von jeweils 250 € und außerdem eine Maple-Lizenz von der Firma Maplesoft. Wir haben das preisgekrönte Poster auf S. 34 abgedruckt.

Das Conference Banquet fand in der Guild Hall im City Centre von Bath statt. Wie immer wurden auf dem Bankett in festlichem Rahmen die Preise vergeben.

Bankett in The Pump Rooms der Guild Hall

Außerdem berichtete James Davenport über die lange Geschichte von Bath. Die City of Bath, die zum Weltkulturerbe `http://whc.unesco.org/en/list/428` gehört, war um 50 v. Chr. von den römischen Eroberern gegründet worden, die die heißen Naturquellen als Thermalbäder nutzten.

Bei jeder ISSAC-Tagung wird ein ISSAC Business Meeting abgehalten, zu welchem alle Teilnehmer herzlich eingeladen und Beschlüsse zur Tagungsreihe getroffen werden.

Manuel Kauers leitete als letzte Amtshandlung die Sitzung des ISSAC Business Meetings. Seine Amtszeit als Chair des ISSAC Steering Committees endete mit der Tagung.

Nach dem Dinner gab es Kaffee in The Roman Baths

Als neues Mitglied des ISSAC Steering Committees wurde in einer sehr knappen Wahl von den Anwesenden Daniel S. Roche (University of Waterloo) gewählt, gegen den Frédéric Chyzak (INRIA) angetreten war.

Das Plenum diskutierte die Vergabe von Preisen für beste Software- und Poster-Präsentationen durch die Fachgruppe Computeralgebra. Das Engagement und Angebot der Fachgruppe wurde begrüßt, und es wurde beschlossen, das ISSAC Steering Committee damit zu beauftragen, sich einen Modus zu überlegen, wie dies im Detail gehandhabt werden soll.

Für die Durchführung der Konferenz ISSAC 2017 hatten sich Kaiserslautern sowie die Jilin University Changchun aus China beworben. Die Wahl durch die Anwesenden lieferte ein sehr deutliches Votum für Kaiserslautern. Herzlichen Glückwunsch! Damit wird also 2017 die ISSAC wieder in Deutschland stattfinden.

Als Veranstaltungsort für die ISSAC 2016 war bereits im letzten Jahr die Wilfrid Laurier University Waterloo, Kanada, ausgewählt worden. Diese Tagung wird vom 20.–22. Juli 2016 stattfinden.

Wolfram Koepf (Kassel)

4. Hyperplane arrangements and reflection groups

Leibniz Universität Hannover, 10.08.2015 – 12.08.2015

`www.iazd.uni-hannover.de/~hoge/arr2015`

Vom 10.-12. August fand in Hannover ein Workshop zum Thema 'Hyperplane arrangements and reflection groups' statt. Organisiert wurde die Tagung von Michael Cuntz (Hannover), Torsten Hoge (Hannover) und Gerhard Röhrle (Bochum).

Die Teilnehmer kamen aus Schweiz, USA, Japan, Frankreich und Deutschland. Die Vorträge konzentrierten sich auf geometrische, kombinatorische und rechentechnische Aspekte von Hyperebenenarrangements und Spiegelungsgruppen.

Die Vorträge waren sehr stark miteinader verzahnt. Ein Beispiel dafür waren die aufeinanderfolgenden Vorträge von Paul Mücksch und Takuro Abe. Paul Mücksch berichtete von der Klassifikation der rekursiv freien komplexen Spiegelungsarrangements, welche eine Vermutung von Takuro Abe bewies.

Torsten Hoge (Hannover)

5. The 17th International Workshop on Computer Algebra and Scientific Computing (CASC 2015)

Aachen, September 14–18, 2015

`http://www.casc.cs.uni-bonn.de/`

(Conference photo CASC 2015 in the main building of RWTH Aachen hosting the conference; Photo: Christian Schilli)

The ongoing progress both in theoretical computer algebra and in its expanding applications has caused a need in forums bringing together both the scientists working in the area of computer algebra methods and systems and the researchers who apply the tools of computer algebra for the solution of problems in scientific computing in order to foster new and closer interactions. This need has led to the series of CASC (Computer Algebra in Scientific Computing) Workshops, which started in 1998 and since then has been held annually.

This year the seventeenth CASC conference took place in Aachen (Germany) from September 14–18, and was very well organized by the CASC 2015 local organizing committee at RWTH Aachen University, headed by Eva Zerz and Viktor Levandovskyy. Computer algebra in Aachen has a long and a fruitful history. A brief overview of this history is given in the preface to the proceedings, see `http://link.springer.com/content/pdf/bfm%3A978-3-319-24021-3%2F1.pdf`.

In the conference thirty-three full papers submitted to the workshop by the participants, accepted by the program committee after a thorough reviewing process, and printed in the proceedings were presented. Additionally, two invited talks were given. Moreover, four talks related to (commercial) systems were given—giving news on established systems MAPLE, MATHEMATICA, or introducing novel developments CLOUDMATH, and SWMATH.

Polynomial algebra, which is at the core of computer algebra, was represented by contributions devoted to the computation of resolutions and Betti numbers with the aid of a combination of Janet bases and algebraic discrete Morse theory, automatic reasoning in reduction rings using the THEOREMA software system, estimation of the complexity of a new algorithm for recognizing a tropical linear variety, conversion of a zero-dimensional standard basis into a standard basis with respect to any other local ordering, simplification of cylindrical algebraic decomposition formulas with the aid of a new multi-level heuristic algorithm, solving polynomial systems with polynomial homotopy continuation, implementation of solvable polynomial rings in the object oriented computer algebra system JAS (Java Algebra System), explicit construction of the tangent cone of a variety using the theory of regular chains, computation of the limit points of the regular chain quasi-component by using linear changes of coordinates, obtaining new bounds for the largest positive root of a univariate polynomial with real coefficients, real root isolation by means of root radii approximation, application of the algebra of resultants for distance evaluation between an ellipse and an ellipsoid.

Among the many existing algorithms for solving polynomial systems, perhaps the most successful numerical ones are the homotopy methods. The number of operations that these algorithms perform depends on the condition number of the roots of the polynomial system. Roughly speaking the condition number expresses the sensitivity of the roots with respect to small perturbation of the input coefficients. The invited talk by E. Tsigaridas dealt with the problem of obtaining effective bounds for the condition number of polynomial systems with integer coefficients. The provided bounds depend on the number of variables, the degree and the maximum coefficient bitsize of the input polynomials. Such bounds allow one to estimate the bit complexity of algorithms like the homotopy algorithms that depend on the condition number for solving polynomial systems.

Two talks dealt with the solution of difference systems: hypergeometric solutions of first-order linear difference systems with rational-function coefficients; computation of regular solutions of linear difference systems with the aid of factorial series.

The topics of two further talks were related to problems in linear algebra and the theory of matrices: in one of them, it was proposed to perform a randomized preprocessing of Gaussian elimination with no pivoting with the aid of circulants; the other talk a new form of triangular decomposition of a matrix, which was termed the LDU-decomposition, has been proposed.

Several talks were devoted to using computer algebra for the investigation of various mathematical and applied topics related to ordinary differential equations (ODEs): obtaining the algebraic general solutions of first order algebraic ODEs, obtaining the analytic-form solutions of two-point boundary problems with one mild singularity with the aid of the Green's function and the THEOREMA software system, investigation of quasi-steady state phenomena arising in the solutions of parameter-dependent ODE systems, in particular, for reaction networks, symbolic computation of polynomial first integrals of systems of ODEs, homotopy analysis of stochastic differential equations with maxima.

Two talks dealt with applications of symbolic and symbolic-numeric computations for investigating and solving partial differential equations (PDEs) in mathematical physics: partial analytical solution of a PDE system from Kirchhoff's rod theory, symbolic-numeric solution of boundary-value problems for the Schrödinger equation.

Among the numerical methods to approximately solve partial differential equations on complicated domains, finite element methods are often the preferred tool. The invited talk by V. Pillwein showed how symbolic computations can be used in the construction of higher-order finite element methods. The analysis and construction methods range from Gröbner basis computations and cylindrical algebraic decomposition to algorithms for symbolic summation and integration.

(Scenic Monschau; Photo: Ernst-W. Mayr)

Applications of symbolic and symbolic-numeric algorithms in mechanics and physics were represented by the following themes: investigation of the stability of relative equilibria of oblate axisymmetric gyrostat by means of symbolic-numerical modeling, investigation of the influence of constant torque on stationary motions of satellite, investigation of invariant manifolds and their stability in the problem of motion of a rigid body under the influence of two force fields, development of a symbolic algorithm for generating irreducible bases of point groups in the space of $\mathrm{SO}(3)$ group for its application in molecular and nuclear physics, analysis of reaction network systems using tropical geometry, approximate quantum Fourier transform and quantum algorithm for phase estimation.

The remaining topics included the use of resultants and cylindrical algebraic decomposition for the symbolic determination of the topology of a plane algebraic curve, the solution of the problem of interpolating the reduced data in cases when the interpolation knots are unknown, safety verification of hybrid systems using certified multiple Lyapunov-like functions.

The CASC 2015 workshop was supported financially by a generous grant from Deutsche Forschungsgemeinschaft (DFG). Further financial support was obtained from the sponsors Additive, Dr. Hornecker Software-Entwicklung and IT-Dienstleistungen, and Maplesoft.

The program of the CASC 2015 may be found at the web site `http://www.casc.cs.uni-bonn.de/index.php/schedule`

The scientific program of the CASC 2015 workshop was combined by the local organizers in an excellent way with the cultural program including an exciting excursion to Monschau.

The online version of the Proceedings (LNCS 9301) is available at `http://link.springer.com/book/10.1007%2F978-3-319-24021-3`

Wolfram Koepf (Kassel)
Werner M. Seiler (Kassel)
Andreas Weber (Bonn)

6. Jahrestagung der DMV

Hamburg, 21.09.2015 – 25.09.2015

www.math.uni-hamburg.de/DMV2015

Under the umbrella of the DMV Jahrestagung in Hamburg, several Minisymposia were also held, in particular symposia about Algebraic Aspect of Cryptography (organised by Benjamine Fine (Fairfield, USA), Anja Moldenhauer (Hamburg) and Gerhard Rosenberger (Hamburg)) and Computer Algebra and Applications (organised by Mohamed Barakat, Janko Böhm and Claus Fieker, all Kaiserslautern).

The symposium on cryptography with a total of 10 talks covered mainly non-standard cryptography, such as ideas based in group theory, meta-analysis and even hardware based.

The symposium on computer algebra showed the full bandwidth of flavours of current computer algebra from number theory to group theory and (tropical) geometry to name a few topics.

Claus Fieker (Kaiserslautern)

7. Jahrestagung DFG SPP 1489

Osnabrück, 28. September - 02. Oktober 2015

https://www.spptagung.uni-osnabrueck.de/

Die diesjährige Jahrestagung des Schwerpunktprogramms „Algorithmic and experimental methods in Algebra, Geometry and Number Theory“ fand dieses Jahr an der Universität Osnabrück statt. Die Tagung wurde hervorragend von W. Bruns und R. Sieg inclusive Rahmenprogramm organisiert. So fand ein gemeinschaftlicher Ausflug nach Kalkriese, dem Ort der berühmten Varus-Schlacht, statt.

Das Schwerpunktprogramm läuft noch bis 2016 und wird mit der Abschlusstagung in der zweiten Hälfte 2016 beendet. Ein Konferenzband ist in Planung.

In mehreren Vorträgen wurde die Weiterentwicklung von Computeralgebra–Systemen und deren Vernetzung thematisiert. Im Folgenden liste ich die Vorträge in der Reihenfolge auf, in der sie gehalten wurden. Die Folien der meisten Vorträge sind erhältlich unter: https://www.spptagung.uni-osnabrueck.de/program/schedule/

Derenthal: Strong approximation and descent. **Margolis:** Torsion Units in Integral Group Rings. **Hampe:** Realizing graphs of genus 4 as skeleta of tropical space curves. **Gutsche/Posur:** Cap — Categories, algorithms, and programming. **Netzer:** Proving Kazhdan's Property (T) with Semidefinite Programming. **Varbaro:** Dual graphs of projective schemes. **Toman:** The Complexity of the Radical Word Problem for Binomial Ideals. **T. Markwig:** How to compute tropical varieties over the p-adic numbers? **Stoll:** Chabauty without the Mordell-Weil group. **Spreckels:** On the order of abelian varieties over finite prime fields. **Thiel:** Computational aspects of rational Cherednik algebras. **Keicher:** Computing automorphisms of graded algebras and Mori dream spaces. **Fieker:** Software Development Within the SPP1489: Number Theory. **Kemeny:** Syzygies of curves via K3 surfaces. **Pieropan:** Generalized Cox rings over nonclosed fields. **Rossmann:** Computing representation zeta functions of unipotent groups. **Börner:**.The functional equation for L-functions of hyperelliptic curves. **Decker:** Software Development Within the SPP1489. **Centeleghe:** Computing integral Frobenius for Modular Abelian Surfaces. **Eick:** Nilpotent associative algebras and coclass theory. **King:** Algorithmic isomorphism classification of modular cohomology rings of finite groups. **Boehm:** Modular Techniques in Computational Algebraic Geometry. **Söger:** Better triangulations in Normaliz 3.0. **Eder:** Improved Parallel Gaussian Elimination for Groebner Bases Computations in Finite Fields. **Steenpaß:** Gröbner Bases over Algebraic Number Fields. **Gutsche:** Dockerimage für Schwerpunktssoftware. **S. Müller:** Quadratic Chabauty. **Naskrecki:** Generalized Fermat equations $x^2+y^3=z^p$ — a progress report. **Tsaknias:** Generalizations of Maeda's Conjecture. **Rahm:** Novel techniques for group homology calculation, and applications to Bianchi modular forms.

Jürgen Klüners (Paderborn)

Jahrestagung DFG SPP 1489

Deterministic root finding in finite fields

Luca De Feo[1], Christophe Petit[2] and Michaël Quisquater[1]

[1]Université de Versailles – Saint-Quentin-en-Yvelines, [2]University College London

Root finding problem

- Let q be a prime power, $n \geq 1$ and $\mathbb{F}_{q^n}$ a field with q^n elements,
- f a polynomial in $\mathbb{F}_{q^n}[X]$ of degree d.

Problem: find (one/all) the roots of f in $\mathbb{F}_{q^n}$.

Complexity: We count the number of $(+, \times, \div)$ operations in $\mathbb{F}_{q^n}$.

Best algorithms (average case complexities)

We suppose that f is *squarefree* and *splits completely* in $\mathbb{F}_{q^n}$ (easy deterministic reduction by taking the gcd with $X^{q^n} - X$).

Non-deterministic

- Cantor-Zassenhaus [2]. $O(n\mathsf{M}(d)\log d \log(dq))$

Deterministic (worst case still polynomial)

- Berlekamp's Trace Algorithm [1] (**BTA**), $O(n\mathsf{M}(d)\log q \log d + q\mathsf{M}(d)\log^2 d)$
- Affine Refinement Method [4, 7] (**ARM**), $O(n^2 \log q + n\mathsf{M}(d)\log q + q\mathsf{M}(d)\log^2 d)$
- Successive Resultants Algorithm [6] (**SRA**), $O(n^2 \log q + (n - \log d)q\mathsf{M}(d)\log d)$

Conditionally deterministic

- Subgroup Refinement Method [5, 4] (**SRM**), $O(S(q^n - 1)\mathsf{M}(d)\log^2 d)$
- Subgroup+Affine Refinement Method, $O(n^2 \log q + n\mathsf{M}(d)\log q + S(q-1)\mathsf{M}(d)\log^2 d)$

where $S(x) =$ largest prime divisor of x. Our contributions in red.

Subgroup Refinement Method

Suppose $f(X) \mid (X^D - 1)$. For example, $D = q^n - 1$.
Let ω be an element of $\left(\mathbb{F}_{q^n}\right)^*$ of order D, let $t|D$.

$$X^D - 1 = \prod \begin{cases} X^{D/t} - \omega^{D/t} \\ \vdots \\ X^{D/t} - \omega^{(t-1)D/t} \\ X^{D/t} - 1 \end{cases} \quad \overset{\text{gcd}}{\longleftrightarrow} \quad \begin{matrix} g_1(X) \\ \vdots \\ g_{t-1}(X) \\ g_t(X) \end{matrix} \Bigg\rangle \prod = f(X)$$

- Roots of g_t are D/t-th roots of unity $\rightarrow$ apply recursively.
- Roots of g_i are in $\omega^i \mu_{D/t}$ $\rightarrow$ shift by ω^{-i} and apply recursively.

Complexity

- Requires a primitive generator of $\mathbb{F}_{q^n}$ (non-deterministic in general),
- then uses only gcd's and (t-points) polynomial evaluation (deterministic).
- Dominated by $S(q^n - 1)$, largest factor of $q^n - 1$.

Affine Refinement Method

- Let $v_1, \ldots, v_n$ be an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ and $V_i = \operatorname{span}(v_1, \ldots, v_i)$,
- $L_i(X)$ the (linearized) polynomial vanishing on V_i (e.g. $L_n = X^{q^n} - X$).

$$L_{i+1}(X) = \prod \begin{cases} L_i(X) \\ L_i(X - c_1 v_{i+1}) \\ \vdots \\ L_i(X - c_{q-1} v_{i+1}) \end{cases} \quad \overset{\text{gcd}}{\longleftrightarrow} \quad \begin{matrix} g_0(X) \\ g_1(X) \\ \vdots \\ g_{q-1}(X) \end{matrix} \Bigg\rangle \prod = f(X)$$

c_i running through the elements of $\mathbb{F}_q$.

- The L_i's are independent of f, and computed by a recursion formula.
- Roots of g_0 are in the subspace V_i $\rightarrow$ apply recursively.
- Roots of g_j are in $V_i + c_j v_{i+1}$ $\rightarrow$ shift by $-c_j v_{i+1}$ and apply recursively.

Subgroup+Affine Refinement Method

Unifies SRM and ARM:

- Let ω be a generator of $(\mathbb{F}_q)^*$, let $D = q - 1$ and $t|D$,
- let $v_1, \ldots, v_n$ be an $\mathbb{F}_q$ basis of $\mathbb{F}_{q^n}$.

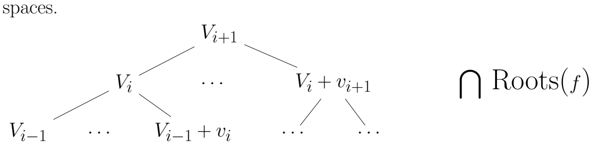
$$\frac{L_{i+1}(X)}{L_i(X)} = L_i(X)^D - L_i(v_{i+1})^D = \prod \begin{cases} L_i(X)^{D/t} - \left(\omega L_i(v_{i+1})\right)^{D/t} \\ \vdots \\ L_i(X)^{D/t} - \left(\omega^{t-1} L_i(v_{i+1})\right)^{D/t} \\ L_i(X)^{D/t} - L_i(v_{i+1})^{D/t} \end{cases}$$

Apply recursively on $L_i(X)^{D/t} - L_i(v_{i+1})^{D/t}$.

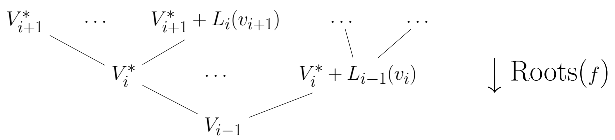
- Dominated by $S(q-1)$ rather than $S(q^n - 1)$.
- Requires primitive generator of $\mathbb{F}_q$ rather than $\mathbb{F}_{q^n}$ (e.g., deterministic under GRH if q is prime).

Successive Resultants Algorithm

ARM finds the roots of f by intersecting with progressively smaller affine spaces.



Define the dual space V_i^* as the image space of L_i. SRA is formally the *dual* of ARM: it projects the roots of f onto progressively smaller subspaces.



- Projections computed (recursively) by $\operatorname{Res}_X\left(L_i(X) - Y_i,\ f(X)\right)$,
- Descent stopped when space is small enough for exhaustive search.

More about root finding

Find more on `https://github.com/defeo/root_finding`

- Optimizations for: worst case, composite n,
- NTL/Python implementation and comparison with state of the art.

Open questions:

- Make the complexity of ARM and SRA linear in n.
- Is it possible to combine SRA with SRM? With [3]?

References

[1] E. R. Berlekamp. Factoring Polynomials over Large Finite Fields. *Math. Comp.*, 24:713–735, 1970.

[2] David G Cantor and Hans Zassenhaus. A New Algorithm for Factoring Polynomials over Finite Fields. *Mathematics of Computation*, pages 587–592, 1981.

[3] Bruno Grenet, Joris van der Hoeven, and Grégoire Lecerf. Deterministic root finding over finite fields using graeffe transforms. In *ISSAC'15*. ACM, 2015.

[4] Alfred Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Some Computational Aspects of Root Finding in GF(q^m). In *ISSAC*, volume 358 of *Lecture Notes in Computer Science*, pages 259–270. Springer, 1988.

[5] Robert T. Moenck. On the Efficiency of Algorithms for Polynomial factoring. 31(137):235–250, 1977.

[6] Christophe Petit. Finding Roots in GF(p^n) with the Successive Resultant Algorithm. *LMS Journal of Computation and Mathematics*, 8 2014. (to appear).

[7] Paul C. van Oorschot and Scott A. Vanstone. A Geometric Approach to Root Finding in GF(q^m). *IEEE Transactions on Information Theory*, 35(2):444–453, 1989.

Das auf der ISSAC-Konferenz preisgekrönte Poster.

Hinweise auf Konferenzen

1. **III EACA International School on Computer Algebra and its Applications**

   Seville, Spain , 18.01.2016 – 21.01.2016

   The Third EACA International School on Computer Algebra and its Applications will take place at the Faculty of Mathematics and IMUS (University Institute of Mathematics Research) of the University of Seville (Spain) on January 18th-21th, 2016. It is an activity of the Spanish network Red-EACA, Red Temática de Cálculo Simbólico, Álgebra Computacional y Aplicaciones, partially supported by the Ministry of Economy and Competitiveness, under the Acciones de Dinamización "Redes de Excelencia"MTM2014-56142-REDT. This School intends to provide an opportunity for young researchers (namely, Master and PhD students and Postdocs) in Computer Algebra and Symbolic Computation or in its Applications from all over the world, to learn from three internationally recognized lecturers, about recent developments on the area. The School also welcomes experienced researchers interested in these topics. The School will consist on three courses (lectures and tutorials) by experts plus short contributed talks and poster presentations by young researchers. Submissions will be supervised by the School's Scientific Committee. There will be grants partially covering local expenses for young researchers. Candidates will be selected under the supervision of the School's Scientific Committee.

2. **Advanced Computing and Analysis Techniques in physics research (ACAT)**

   Valparaiso, Chile, 18.01.2016 – 22.01.2016

   The 17th edition of ACAT aims to once again bring together computer science researchers and practitioners, and researchers from particle and nuclear physics, astronomy and astrophysics and accelerator science to explore and confront the boundaries of computing, of automated data analysis as well as theoretical calculation technologies. It will create a forum for exchanging ideas among the fields and will explore and promote cutting-edge computing, data analysis and theoretical calculation technologies in fundamental physics research.

3. **COCOA 2016 - International School on Computer Algebra**

   IIT Gandhinagar (Indien), 22.02.2016 – 26.02.2016

   `www.iitgn.ac.in/COCOA-2016`

   Die CoCoA-Schule richtet sich an Diplomanden und Doktoranden aus der ganzen Welt, die an Themen aus der kommutativen Algebra oder algebraischen Geometrie arbeiten und das Computeralgebrasystem
   CoCoA einsetzen wollen. Es wird zwei Kurse mit zugehörigen Tutorien geben:

   (1) Lorenzo Robbiano, Computational Linear and Commutative Algebra (Tutorien: Anna Bigatti)

   (2) Dilip Patil und Martin Kreuzer, Computational Aspects of Burnside Algebras (Tutorien: Martin Kreuzer)

   Die CoCoA Schule findet bereits zum neunten Mal statt, jedoch erstmals in Indien. Neben den Kursen und Tutorien wird auch eine Poster-Session angeboten, in der die Teilnehmer ihre eigenen Arbeiten präsentieren können. Ferner wird die Schule durch Abendvorträge angesehener Mathematiker ergänzt. Details zur Anmeldung und Durchführung sind auf der angegebenen Webseite abrufbar. Anmeldeschluss ist der 25.11.2015.

4. **Gemeinsame Jahrestagung von DMV und GAMM**

   Braunschweig, 7.03.2016 – 11.03.2016

   `www.dmv-gamm-2016.de`

   Nächstes Jahr veranstalten die Deutsche Mathematiker-Vereinigung (DMV) und die Gesellschaft für Angewandte Mathematik und Mechanik (GAMM) eine gemeinsame Jahrestagung vom 7. - 11. März an der TU Braunschweig.

   Zu dieser Konferenz werden mehr als 1.000 nationale und internationale Teilnehmer erwartet. Das wissenschaftliche Programm enthält zehn Hauptvorträge, sieben Minisymposia und 29 Sektionen. Dort wird in mehreren hundert Vorträgen über die neuesten wissenschaftlichen Ergebnisse in einem breiten Spektrum von Disziplinen, das von Mathematik über Numerik und wissenschaftlichem Rechnen bis zur Strömungsmechanik und Mechanik reicht.

   Eines der Minisymposien ist dem Thema Computeralgebra gewidmet, das sich aufgrund seiner Lage im Spannungsfeld zwischen Reiner und Angewandter Mathematik hervorragend für die gemeinsame Jahrestagung von DMV und GAMM eignet. Das Minisymposium wird von Bettina Eick (Braunschweig), Anne Frühbis-Krüger (Hannover), Sandra Klinge (Dortmund) und Eva Zerz (Aachen) organisiert und soll am Dienstag, dem 8. März, stattfinden. Mehrere hochkarätige Vortragende haben ihre Teilnahme bereits zugesagt.

5. **The 7th International Symposium on Symbolic Computation in Software Science**

   Tokyo, Japan , 28.03.2016 – 31.03.2016

   The purpose of SCSS 2016 is to promote research on theoretical and practical aspects of symbolic computation in software science. The symposium provides a forum for active dialog between researchers from several fields of computer algebra, algebraic geometry, algorithmic combinatorics, computational logic, and software analysis and verification.

6. **5th European Seminar on Computing - Smart Applications of Scientific Computing Minisymposium**

   Pilsen, Czech Republic , 05.06.2016 – 10.06.2016

   Nowadays there is a wide variety of mathematical software available: computer algebra systems, technical computing languages, automated deduction systems,... This minisymposium is devoted to practical real-world applications of this software in fields like: transportation engineering, electrical engineering, medicine, knowledge based systems,... (this is not an exhaustive list). The focus will be on advanced and smart applications with a nontrivial mathematical background.

7. **EACA-2016: Meeting on Computer Algebra and Applications**

   Logroño, Spain, 22.06.2016 – 24.06.2016

   The “Encuentros de Álgebra Computacional y Aplicaciones, EACA“ (Meetings on Computer Algebra and Applications) are organized by the Spanish “Red Temática de Cálculo Simbólico, Álgebra Computacional y Aplicaciones“ to provide a meeting frame for researchers in the fields of Computer Algebra and Symbolic Computation, and for those who use these techniques in their research.

8. **ISSAC 2016**

   Waterloo, Ontario, Canada, 20.07.2016 – 22.07.2016

   `www.issac-symposium.org/2016`

   The International Symposium on Symbolic and Algebraic Computation (ISSAC) is the premier conference for research in symbolic computation and computer algebra. ISSAC 2016 will be the 41st meeting in the series, which started in 1966 and has been held annually since 1981. The conference presents a range of invited speakers, tutorials, poster sessions, software demonstrations and vendor exhibits with a centerpiece of contributed research papers.

9. **INFORMATIK 2016 — 46. Jahrestagung der Gesellschaft für Informatik**

   Klagenfurt, Österreich, 26.09.2016 – 30.09.2016

   `www.informatik2016.de`

   Mit dem Motto „Informatik: von Menschen für Menschen“ ist die Jahrestagung 2016 dieser auf den Menschen zentrierten Sicht gewidmet: das beschleunigte Privat und Arbeitsleben, die Komplexität der Aufgaben und Abläufe sollen im nahtlosen Zusammenwirken zwischen Mensch und Informatiksystemen zu bewältigen sein. Dabei müssen die Systeme beherrschbar, unaufdringlich und verstehbar bleiben, Technik hat sich dem Menschen anzupassen und nicht umgekehrt.

Antrag auf Mitgliedschaft in der Fachgruppe Computeralgebra der GI in Kooperation mit der DMV und GAMM und auf Bezug des Computeralgebra Rundbriefs

Rückfragen: Telefon: + 49 (0)228-302-151/-149 / Telefax: + 49 (0)228-302-167/
E-Mail: mitgliederservice@gi.de / http://www.gi.de
Bitte zurücksenden an: Prof. Dr. Wolfram Koepf, Institut für Mathematik, Heinrich-Plett-Str. 40, 34132 Kassel

Name:	Vorname:
Akadem. Grad:	Geburtsjahr:
Privatanschrift: Straße / Postf.:	PLZ Ort:
Telefon:	Telefax:
Dienstanschrift: Firma / Inst.:	Abteilung:
Straße / Postf.:	PLZ Ort:
Telefon:	Telefax:
E-Mail:	
Gewünschte Postanschrift: ☐ Privatanschrift	☐ Dienstanschrift
Gewünschte Regionalgruppenzuordnung (www.gi.de/regionalgruppen/): Regionalgruppe:	

☐ Ich bin persönliches Mitglied der GI und beantrage die Mitgliedschaft in der Fachgruppe Computeralgebra sowie den Bezug des Rundbriefs

☐ Ich beantrage assoziierte Mitgliedschaft in der GI und Mitgliedschaft in der Fachgruppe Computeralgebra sowie den Bezug des Rundbriefs

☐ ab 1. Januar ☐ rückwirkend zum 1. Januar des laufenden Jahres (bis zum 30. September möglich).

Ich ordne mich folgender Jahresbeitragsklasse zu:

- ☐ 7,50 Euro für Mitglieder von ☐ DMV ☐ GI ☐ GAMM Mitgliedsnummer:
- ☐ 7,50 Euro. Ich beantrage gleichzeitig Mitgliedschaft in ☐ DMV ☐ GI ☐ GAMM und bitte um Zusendung der dazu erforderlichen Unterlagen.
- ☐ 9,00 Euro für Nichtmitglieder. Ich bitte um Zusendung von Informationen über ☐ DMV ☐ GI ☐ GAMM

☐ Ich bitte lediglich um Aktualisierung meiner Adressdaten sowie meiner Angaben über die Zusendung von Informationen.

Datennutzung

Meine oben angegebenen personenbezogenen Daten werden im Rahmen meiner Mitgliedschaft soweit gesetzlich erlaubt oder aufgrund meiner Einwilligung durch die GI oder durch Dritte nach Weitergabe durch die GI wie folgt genutzt:

- ☐ für alle GI gesellschaftsinternen Aussendungen
- ☐ sowie weitere von der GI gesondert ausgewählte Informationen mit Bezug zur Informatik, wie u.a. Weiterbildungsangebote (z.B. der DIA), Informatik Veranstaltungen oder Kongresse mit und ohne GI-Beteiligung sowie Publikationen mit Informatik-Bezug.

Soweit Sie uns Ihre E-Mail Adresse angegeben haben, wird die oben angegebene Kommunikation soweit möglich elektronisch ausgeführt.

- ☐ Der Nutzung meiner E-Mail Adresse zu Zwecken, die über die satzungsgemäßen Ziele der GI hinausgehen (wie z.B. Werbung, Markt- und Meinungsforschung) stimme ich zu.

Natürlich können Sie Ihre Zustimmung jederzeit widerrufen oder Ihre E-Mail-Adresse in unserem System löschen lassen. Eine kurze Nachricht an mitgliederservice@gi.de, per Post oder Fax genügt.

Ich nehme zur Kenntnis, dass die Aufnahme in die Fachgruppe Computeralgebra zum 1.1. erfolgt und dass die Mitgliedschaft zum 31.12. mit Frist 30.11. schriftlich gekündigt werden kann.

________________________ (Datum) ________________________ (Unterschrift)

Fachgruppenleitung Computeralgebra 2014-2017

Sprecher:
Prof. Dr. Gregor Kemper
Zentrum Mathematik – M11
Technische Universität München
Boltzmannstr. 3, 85748 Garching
089-289-17454, -17457 (Fax)
`kemper@ma.tum.de`
`http://www-m11.ma.tum.de/~kemper`

Fachexperte Redaktion Rundbrief:
Prof. Dr. Michael Cuntz
Institut für Algebra, Zahlentheorie und Diskrete Math.
Leibniz Universität Hannover
Welfengarten 1, 30167 Hannover
0511-762-4252
`cuntz@math.uni-hannover.de`
`http://www.iazd.uni-hannover.de/~cuntz`

Fachreferent CA-Systeme und -Bibliotheken:
Prof. Dr. Claus Fieker
Fachbereich Mathematik
Technische Universität Kaiserslautern
Gottlieb-Daimler-Straße, 67663 Kaiserslautern
0631-205-2392, -4427 (Fax)
`fieker@mathematik.uni-kl.de`
`http://www.mathematik.uni-kl.de/~fieker`

Fachexperte Physik:
Dr. Thomas Hahn
Max-Planck-Institut für Physik
Föhringer Ring 6, 80805 München
089-32354-300, -304 (Fax)
`hahn@feynarts.de`
`http://wwwth.mppmu.mpg.de/members/hahn`

Fachreferent Schwerpunktprogramm 1489:
Prof. Dr. Jürgen Klüners
Mathematisches Institut der Universität Paderborn
Warburger Str. 100, 33098 Paderborn
05251-60-2646, -3516 (Fax)
`klueners@math.uni-paderborn.de`
`http://www2.math.uni-paderborn.de/people/juergen-klueners.html`

Fachreferent Themen und Anwendungen:
Prof. Dr. Martin Kreuzer
Fakultät für Informatik und Mathematik
Universität Passau
Innstr. 33, 94030 Passau
0851-509-3120, -3122 (Fax)
`martin.kreuzer@uni-passau.de`
`http://www.fim.uni-passau.de/~kreuzer`

Fachreferent Schule und Didaktik:
OStR Jan Hendrik Müller
Rivius-Gymnasium der Stadt Attendorn
Westwall 48, 57439 Attendorn
02722-5953 (Sekretariat)
`jan.mueller@math.uni-dortmund.de`
`www.mathebeimueller.de`

Stellvertretender Sprecher:
Prof. Dr. Florian Heß
Carl-von Ossietzky Universität Oldenburg
Institut für Mathematik, 26111 Oldenburg
0441-798-2906, -3004 (Fax)
`florian.hess@uni-oldenburg.de`
`http://www.staff.uni-oldenburg.de/florian.hess`

Fachreferentin Themen und Anwendungen:
Prof. Dr. Bettina Eick
Institut Computational Mathematics
Fachbereich Mathematik und Informatik
Technische Universität Braunschweig
Braunschweig
0531-391-7525, -7414 (Fax)
`beick@tu-bs.de`
`http://www.icm.tu-bs.de/~beick/`

Fachreferentin Publikationen und Promotionen:
Prof. Dr. Anne Frühbis-Krüger
Institut für Algebraische Geometrie
Welfengarten 1, 30167 Hannover
0511-762-3592
`fruehbis-krueger@math.uni-hannover.de`
`http://www.iag.uni-hannover.de/~anne`

Fachreferentin Computational Engineering, Vertreterin der GAMM:
Prof. Dr.-Ing. Sandra Klinge
Institute of Mechanics
TU Dortmund
Leonhard-Euler-Str. 5, D-44227 Dortmund
0231-755-5790
`sandra.klinge@tu-dortmund.de`
`http://www.im.mb.tu-dortmund.de/typo3/en/institute`

Vertreter der DMV:
Prof. Dr. Wolfram Koepf
Institut für Mathematik
Universität Kassel
Heinrich-Plett-Str. 40, 34132 Kassel
0561-804-4207, -4646 (Fax)
`koepf@mathematik.uni-kassel.de`
`http://www.mathematik.uni-kassel.de/~koepf`

Vertreter der GI:
Prof. Dr. Ernst W. Mayr
Lehrstuhl für Effiziente Algorithmen
Fakultät für Informatik
Technische Universität München
Boltzmannstraße 3, 85748 Garching
089-289-17706, -17707 (Fax)
`mayr@in.tum.de`
`http://www.in.tum.de/~mayr/`

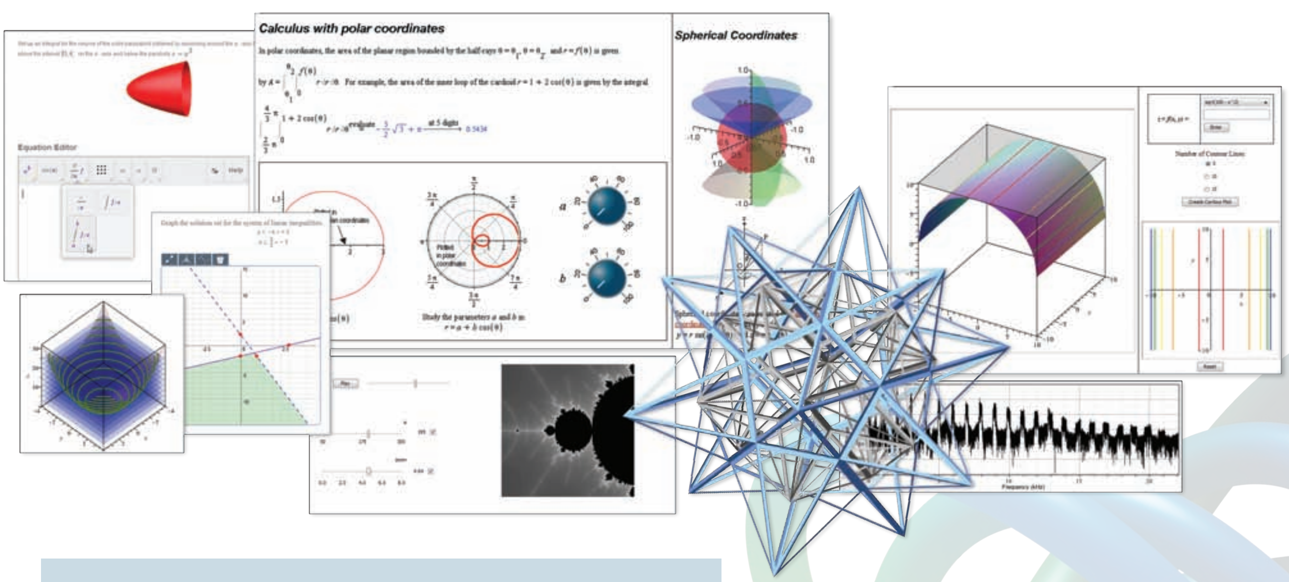
Fachreferentin CA an der Hochschule:
Prof. Dr. Eva Zerz
Lehrstuhl D für Mathematik
RWTH Aachen
Pontdriesch 14/16, 52062 Aachen
0241-80-94544, -92108 (Fax)
`eva.zerz@math.rwth-aachen.de`
`http://www.math.rwth-aachen.de/~Eva.Zerz/`

Herausforderungen und Lösungen für MINT-Programme

Wie kann Technologie die größten Herausforderungen in **MINT-Programmen** lösen und das Verständnis, die Merkfähigkeit und den Erfolg der Studierenden fördern?

Maple und MapleSim sind faszinierende Werkzeuge zur Visualisierung von MINT-Konzepten und zur Erkundung von Problemen. Maple T.A. ermöglicht es den Studierenden, ihre Fähigkeiten zu trainieren und gibt Ihnen ein Werkzeug an die Hand, um die Leistung der Studierenden in den MINT-Fächern zu bewerten.

Das Webinar „**Herausforderungen und Lösungen für MINT-Programme**" bespricht die Herausforderungen der heutigen Zeit und untersucht die benutzerfreundlichen technologischen Lösungen von Maplesoft.



Maple T.A. ist jetzt auf Deutsch verfügbar!

Sehen Sie sich das Webinar „Herausforderungen und Lösungen für MINT-Programme" an:

www.maplesoft.com/MINT

www.maplesoft.com | info@maplesoft.com • Tel: +49 241 980919 30