Computer-Algebra: Das Ende der Mathematik?

Bruno Buchberger
RISC (Research Institute for Symbolic Computation)
Johannes-Kepler-Universität, A4040 Linz, Österreich
Bruno.Buchberger@RISC.Uni-Linz.ac.at

10. April 2000

Mathematische Software-Systeme wie Mathematica, Maple, Derive etc. basieren wesentlich auf enormen Fortschritten in dem Gebiet der Mathematik, das man „Computer-Algebra" oder „Symbolisches Rechnen" nennt. Faktisch alles, was man in den Gymnasien und in den ersten Semestern der Mathematik-Ausbildung lernt, ist in diesen Systemem heute „auf Knopfdruck" zur Verfügung. Wird Mathematik damit überflüssig? In den drei Abschnitten dieses Aufsatzes beantworten wir diese Frage für Nicht-Mathematiker, für Mathematiker und für (zukünftige) Studierende der Mathematik.

1 Computer-Algebra: Mathematik auf Knopfdruck

Viele von uns haben den Mathematikunterricht als etwas Belastendes in Erinnerung: Drill von Dingen, die man eigentlich nie ganz verstanden hat! Oder besonders hinterhältig: Aufgaben, zu deren Lösung man einen „Trick" wissen musste. Wer ihn herausfand, war der Kaiser, die anderen waren die Dummen. Und dazu immer die Frage: Werden wir das jemals brauchen? Wer von uns, die wir das Abitur gemacht haben, musste jemals in seinem Leben eine Funktion differenzieren oder gar integrieren? Nicht einmal das Wurzelziehen kommt später wirklich vor und sollte es vorkommen, haben wir den Taschenrechner! Wieviele von uns haben die Aufgaben aus dem Mathematikunterricht ("zwei Züge fahren mit Geschwindigkeit soundso von A nach B, ...") im späteren Leben je gestellt bekommen? Nicht nur, dass viele Menschen Mathematik nie brauchen, viele einflussreiche und erfolgreiche Menschen sind stolz darauf, dass sie in der Schule schlecht in Mathematik waren und dass sie es „trotzdem" geschafft haben. (Ich erlebe das zum Beispiel sehr oft, wenn Wirtschaftsdelegationen, Firmenvertreter, Politiker und andere den von unserem Institut RISC gegründeten und bestens florierenden Software-Park in Hagenberg besuchen: Die meisten sind beeindruckt von der Wirtschaftsdynamik, die aus der Verbindung von mathematischer Forschung und Wirtschaft entsteht, viele „outen" sich aber gleich bei der Begrüßung - mit verlegenem oder überlegenem Lächeln -, dass Mathematik für sie immer unverständlich oder uninteressant war.)

Die Lage ist inzwischen noch viel extremer geworden: Es gibt jetzt nicht nur Taschenrechner, mit denen alles, was man bis zum vierzehnten Lebensjahr im „Rechnen” lernt, durch Drücken von Knöpfen erledigt werden kann, sondern es gibt nun auch Software-Systeme (wie Mathematica, Maple, Macsyma, Derive, u.v.a.), mit denen alles, was man im Gymnasium oder in den Mathematikvorlesungen in den Ingenieurswissenschaften lernt, aber auch fast alles, was in den ersten zwei Jahren eines regulären Mathematikstudiums geboten wird, - und noch einiges darüberhinaus - auf Knopfdruck zur Verfügung steht. Auch haben diese Systeme heute Benutzeroberflächen, die den Umgang mit diesen Systemen für jedermann ganz leicht machen. Es können weiters hunderte fertige Software-Pakete, die auf der Basis dieser mathematischen Software-Systeme programmiert sind, für eine Vielzahl von Anwendungen aus allen Bereichen der Naturwissenschaft, Technik, Medizin, Wirtschaft etc. rasch über das Netz geladen und dann am Computer zu Hause ausgeführt werden.

Wollen Sie z.B. ausrechnen, wie ein Roboter, dessen Plattform mit 6 Stäben gesteuert wird, auf Verschiebungen der Stäbe reagiert? Oder die Qualität von Finanzprodukten vergleichen? Oder die Brechung in komplizierten optischen Linsensystemen berechnen? Oder studieren, wie sich einfachste zellulare Strukturen über tausende Generationen hinweg entwickeln? Und dies alles mit graphischer Ein- und Ausgabe und animierten Illustrationen? Sie brauchen dazu nur die Homepage der gängigen mathematischen Software-Systeme zu besuchen (z.B. www.wolfram.com für Mathematica), sich eines dieser Systeme über das Netz herunterzuladen (wofür Sie - Gott sei Dank!- einen Obolus entrichten müssen) und durch die Anwendungspages zu navigieren. Sie werden in vielen Fällen ein fertiges Software-Paket für Ihre Anwendung vorfinden, sich selbst an interaktiven Einführungsbeispielen in die fachgerechte Benutzung des geeigneten Pakets einschulen können und sich gegebenenfalls aus den vorhandenen Funktionalitäten des Anwendungspakets rasch neue Funktionalitäten zusammenbauen können, die ganz auf Ihre Bedürfnisse zugeschnitten sind. Ein Beispiel einer solchen Anwendung sehen Sie in Anhang 1.

Das qualitativ Neue der heutigen mathematischen Software-Systeme - gegenüber Sammlungen „numerischer Algorithmen” [1] von vor zwanzig Jahren - ist, dass inzwischen Methoden entwickelt worden sind, mit denen man im Computer „wie ein Mensch rechnen kann”. Das heißt, man kann im Computer jetzt nicht nur mit (Näherungs-)zahlen arbeiten, sondern mit „Formeln”, „symbolischen Ausdrücken”, „sprachlichen Gebilden”, die die behandelten mathematischen Probleme exakt darstellen und dann auch „exakt”, „in geschlossener Form”, „analytisch”, „symbolisch” zu lösen gestatten. Viel von dem, was vor zwanzig oder dreißig Jahren von den Mathematikern noch selbst mühsam und mit viel Überlegung „mit Papier und Bleistift” entwickelt werden musste, bevor man überhaupt darangehen konnte, ein Computer-Programm für die (numerische) Lösung eines gegebenen Problems zu schreiben, kann man heute mit den Methoden der „symbolischen Mathematik” (oder wie man auch sagt, der „Computer-Algebra”) durch den Computer durchführen lassen. Die Computer-Algebra hat den wesentlichen Beitrag dazu geleistet, dass sich jetzt innerhalb weniger Jahre die Situation bezüglich der Benutzbarkeit des vorhandenen mathematischen Wissen und der mathematischen Problemlösetechniken radikal dahingehend geändert hat, dass faktisch die

[1] „Numerische Mathematik”: Alle mathematischen Probleme werden durch approximative, „endliche” Probleme ersetzt. Die Ersatzprobleme werden dann mit gerundeten Zahlen näherungsweise gelöst.

gesamte Mathematik, die man in der Schule und in den ersten Semestern an der Universität lernt - einschließlich der Schritte, wo man „denken" musste, - bereits „am Computer zur Verfügung steht".

Im Beispiel im Anhang 1 bedeutet dies, dass nicht nur vorgelegte Bilder mit einem System von Wavelets z.B. für die schnelle Übertragung komprimiert werden können, sondern dass auch das Erfinden von brauchbaren Systemen von Wavelets - eine Aufgabe, die noch bis vor kurzem von Mathematikern „nicht-numerisch", „mit Papier und Bleistift" gelöst wurde, *bevor* ein Bildkompressionsverfahren auf einem solchen Wavelet-System aufsetzen konnte - heute mit Methoden der Computer-Algebra (in diesem Fall mit der Methode der sogenannten Gröbner-Basen [1]) am Computer gemacht werden kann, siehe [2].

Wenn die Methoden der Mathematik nun für jedermann auf Knopfdruck zur Verfügung sind, ja sogar die „Papier- und Bleistift-Arbeit" des Mathematikers durch die Methoden der Computer-Algebra „vom Computer" übernommen werden, wenn faktisch jeder auch ohne spezielle mathematische Ausbildung komplizierteste mathematische Probleme lösen kann, ja sogar solche, die stolz darauf sind, dass sie „in Mathematik immer schlecht waren", spielerisch wie in einem Video-Game die hochgestochenste mathematische Maschinerie in Bewegung setzen können, was bleibt dann eigentlich noch für die Mathematik zu tun? Ist die Computer-Algebra das Ende der Mathematik?

Für Benutzer der heutigen Computer-Algebra-basierten mathematischen Software-Systeme mag es genügen zu wissen, dass sie jetzt die Potenz einer Mathematik, die auch die besten Mathematiker nicht annähernd in ihrem Kopf haben, ohne Denkanstrengung auf Knopfdruck „in ihren Händen" zur Verfügung haben. Für sie ist die Frage nach dem Ende der Mathematik wahrscheinlich irrelevant. Viel wichtiger mag es sein, dass die Botschaft möglichst rasch an die „breite Öffentlichkeit" hinüberkommt, dass Mathematik auf Knopfdruck jetzt von jedermann/frau benutzt werden kann.

Für die Mathematiker selbst klingt die Frage nach dem Ende der Mathematik aber vielleicht beunruhigend. Werden wir uns bald selbst wegrationalisiert haben? Werden wir bald ehrlich gestehen müssen, dass unsere Institute zu groß, die für die Universitätsmathematik verwendeten öffentlichen Gelder zu reichlich und die Anzahl der Mathematikstunden in den Schulen und auch in den Universitäts-Curricula, in denen Mathematik nur Hilfswissenschaft ist, weit überproportional sind? Dürfen wir junge Menschen ehrlicherweise noch motivieren, Mathematik zu studieren oder Mathematiklehrer zu werden? Sollten wir uns nicht lieber „inhaltlichen" Dingen zuwenden, die „echte Kreativität" brauchen (wie z.B. Politikwissenschaften oder Biotechnik), nachdem anscheinend auch die kreativen Dinge in der Mathematik schon „vom Computer" gemacht werden?

2 Computer-Algebra: Triviale oder trivialisierte Mathematik?

Die Antwort auf diese Fragen müsste für die Mathematiker eigentlich einfach und natürlich sein. Es ist dennoch erstaunlich, wieviele Mathematiker (darunter auch viele „reine" Mathematiker und vor allem auch viele Mathematiklehrer) sehr diffuse Vorstellungen davon haben, was die heutige Situation in bezug auf die Automatisierung der Mathematik eigentlich für die Mathematik selbst bedeutet. Es gibt zwei große Gruppen mit anscheinend unvereinbaren Ansichten zu diesen Fragen:

- Die *Puristen*: Sie glauben, dass das, was heute in den mathematischen Software-Systemen mit numerischen und Computer-Algebra-Methoden gemacht wird, nur „triviale" Mathematik ist. Man sollte und müsste sich als „echter" Mathematiker nicht mit diesen Dingen abgeben und man sollte diese Systeme am besten den Anwendern oder solchen Mathematikern, die zur „echten" Mathematik nicht fähig sind, überlassen. Die Puristen unter den Mathematikern befassen sich mit dem Computer höchstens, um e-mails zu lesen, Literatursuche am Web zu betreiben oder eine Arbeit in LaTeX zu tippen. Aus dem Mathematikunterricht sollte man nach ihrer Meinung die neuen Software-Systeme am besten verbannen, damit die Schüler und Studenten nicht „verdorben" werden.

- Die *Populisten*: Sie glauben tatsächlich, dass man die Teile der Mathematik, die heute in mathematischen Software-Systemen verfügbar sind, nicht mehr oder nur mehr als „Black-Box" zu unterrichten braucht. Man habe dann den „Kopf frei für die kreativen Teile der Mathematik" und ihrer Anwendungen, was immer das dann ist. Extreme Vertreter dieser Ansicht glauben sogar, dass in der Mathematik auch die Zeit des Beweisens vorbei ist und zwar in dem Sinn, dass man, um neue mathematischen Resultate zu entwickeln, besser am Computer - wie ein Physiker - mit vorhandenen Systemen „experimentiert", als die Resultate mit der „altmodischen" Methode des Beweisen abzusichern.

Ich halte beide Ansichten für grundfalsch und meine demgegenüber Folgendes:

- Mathematik ist charakterisiert durch die Methode des Beweisens. Obwohl natürlich das Experimentieren mit Beispielen (heute: das Experimentieren in mathematischen Software-Systemen) fundamental ist für das Gewinnen neuer Vermutungen und auch Beweisideen typischerweise aus der Betrachtung von Beispielen entstehen, ist die Methode des Beweisens letztlich das, was Mathematik zur Mathematik macht.

- Mathematik war immer darauf ausgerichtet, durch *eine* gute Theorie, *eine* neue Einsicht, *einen* neuen Satz, *einen* neuen Beweis, *eine* neue Methode *unendlich viele* Instanzen eines Problems zu „erschlagen". In dem Augenblick, wo durch einen nicht-trivialen Satz nebst nicht-trivialem Beweis mit einer darauf aufbauenden Methode die unendlich vielen Instanzen eines Problems behandelt werden können, ist der betreffende Problembereich der Mathematik „trivialisiert". Das Computer-Zeitalter unterscheidet sich von früheren Zeiten der Mathematik nur dadurch, dass der Begriff der „Methode", mit welcher die unendlich vielen Instanzen eines Problems erschlagen werden, eine viel konkretere, nämlich extreme Bedeutung hat: Eine auf einem Computer ausführbare Methode für ein Problem erschlägt das Problem so vollständig, dass bei der Anwendung der Methode auf eine Instanz des Problems keine wie immer geartete Kreativität mehr notwendig ist. Also: Mathematik ist dazu da, um durch einmal gründliches Nachdenken (Arbeiten auf einer „grundlegenden" Ebene) *unendlich oftmaliges* Nachdenken auf der Ebene der Instanzen eines Problems unnotwendig zu machen. Mit anderen Worten: Mit nicht-trivialer Mathematik auf einer Ebene A wird ein ganzer Bereich von Mathematik auf Ebene B „trivialisiert". (*Beispiel*: Ebene A: Liouville-Theorie der notwendigen Körpererweiterungen für die Darstellung elementarer transzendenter Funktionen; Ebene B: Problem des Integrierens elementarer transzendenter Funktionen mit dem Risch-Algorithmus. *Einfaches Beispiel*: Ebene A: Sätze über die Invarianz der Lösungsräume von linearen Systemen gegenüber Zeilenoperationen. Ebene B: Lösen von linearen Systemen, die durch Matrizen gegeben sind, mit dem Gauss'schen Algorithmus.)

- Je mehr man sich in der Mathematik darauf ausrichtet, Probleme nicht nur „irgendwie", sondern mit computer-exekutierbaren Algorithmen zu lösen, umso schwierigere Mathematik (d.h. umso feinere Theorien, umso tiefere Sätze, umso schwierigere Beweise) sind notwendig, um die Lösung möglich zu machen. Das ist deshalb so, weil es natürlich viel schwieriger ist (mehr Denkarbeit benötigt), ein gegebenes Problem mit genau begrenzten Reduktionsmethoden (z.B. Rekursion, endliche Schleifen) auf genau begrenzte Grundbausteine (z.B. auf bereits verfügbare Algorithmen) zurückzuführen als mit mächtigen Reduktionskonstrukten (z.B. Mengenbildungsquantor, Mengenvereinigungsquantor) auf mächtige axiomatisch vorausgesetzte „Black-Boxes"(z.B. das Auswahlaxiom). (Ein Beispiel dazu findet sich im Anhang 2.) Mit anderen Worten: Das, was wir heute in den mathematischen Software-Systemen zur Verfügung haben, ist nicht *triviale* Mathematik, sondern *durch höchst nicht-triviale Mathematik trivialisierte Mathematik*!

- Für die „Soziologie der Mathematik" hat das folgende Konsequenz. Nicht diejenigen Mathematiker, die zur „echten" („reinen") Mathematik nicht das rechte Zeug haben, sollten sich mit algorithmischer Mathemik (z.B. Computer-Algebra) befassen, sondern gerade umgekehrt: Die algorithmische Mathematik braucht die besten mathematischen Köpfe. Oder anders formuliert: „Reine" Mathematiker, die bisher den Computer nur vom e-mail her kennen, mögen sich einmal ernsthaft mit der Algorithmisierung ihres Gebiets beschäftigen und sie werden eine Fülle neuer, interessanter, mathematisch äußerst schwieriger Fragen und Anregungen erhalten, die nur durch eine gewaltige Vertiefung der mathematischen Theorie beantwortet werden können.

- Die Algorithmisierung der Mathematik ist niemals abgeschlossen. Man braucht also niemals Angst zu haben, dass die Algorithmisierung der Mathematik das Ende der Mathematik bedeutet. Höhere und höhere Problembereiche der Mathematik werden algorithmisch erschlossen werden können, wozu immer tiefere und tiefere Mathematik notwendig sein wird. In diesem Sinne ist trotz der gewaltigen Fortschritte der Computer-Algebra erst die Oberfläche der Algorithmisierung angekratzt. Relativ zu dem, was in der Mathematik noch nicht verstanden, durchdrungen, algorithmisiert, trivialisiert ist, wird das, was man bereits „am Computer geht", *immer* ein ein winziger

Bruchteil bleiben. Die Unmöglichkeit, die Algorithmisierung der Mathematik zu einem Ende zu führen, ist nicht nur eine praktische Erfahrung aller, die sich mit dem Gebiet beschäftigen - weil sich jedesmal, wenn wieder ein Stück Mathematik algorithmisiert ist, neue unendliche Horizonte auftun -, sondern eine inhärente Eigenschaft der Mathematik, die beweisbar (!) ist und eine praktische Erscheinungsform des Gödelschen Unvollständigkeitssatzes darstellt.

- Für die Didaktik der Mathematik hat das alles folgende Konsequenz: Es ist einerseits sehr naiv, den Computer heute aus der Mathematik auszuschließen. Im Gegenteil, er ist nicht nur ein Hilfswerkzeug, sondern Anlaß und eine treibende Kraft für die konsequente Weiterführung des Grundanliegens der Mathematik, durch mehr Denken schwierige Probleme systematisch, ja sogar automatisch lösbar zu machen. Es war und ist auch „politisch" ein schwerer Fehler, die Beschäftigung mit dem Computer, d.h. mit dem algorithmischen Lösen von Problemen, aus der Mathematik abtriften zu lassen und sich um das weggelegte Kind „Informatik" nicht zu kümmern. Andererseits ist es genauso naiv, „den Computer" als Black-Box dort einzusetzen, wo erst Verständnis geschaffen werden muss, was das Problem ist und was die zugrundeliegenden mathematischen Konzepte, Einsichten und Begründungen sind. Es gibt keine absolute Antwort auf die Frage, in welchen Teilen der Mathematikausbildung „der Computer" eingesetzt werden soll. Vielmehr ist es so, dass für ein vorgegebenes Thema in der Phase, wo die neuen Konzepte, Einsichten und Begründungen erarbeitet werden müssen, das unverstandene Verwenden der vorhandenen Algorithmen sinnlos ist - „White-Box-Phase des Unterrichts" -, während es andererseits in der Phase, wo die Erarbeitung der Grundlagen abgeschlossen ist, genauso sinnlos wäre, die Verwendung der fertigen Algorithmen auszuschließen - „Black-Box-Phase des Unterrichts". Für eine detaillierte Beschreibung dieses „White-Box / Black-Box-Prinzips" siehe [3].

3 Computer-Algebra: Schlüsseltechnologie der Informationsgesellschaft

Natürlich ist die Mathematik nicht am Ende, sondern so dynamisch wie noch nie. Gerade auch wegen der explosionartig fortschreitenden Algorithmisierung der Mathematik müssen wir vielmehr von einem neuen Anfang der Mathematik sprechen. In der Selbstanwendung der Mathematik auf sich selbst, die gerade durch die neuen mathematischen Software-Systeme eine neue Dimension erreicht hat, liegt enorme Schubkraft und eine noch nie dagewesene Dynamik in der mathematischen Forschung, Lehre und Anwendung:

- In allen Bereichen der mathematischen Forschung ist es jetzt möglich, sich theoretische Anregungen durch ausgedehntes und einfaches Experimentieren mit den bereits algorithmisierten Teilen der Mathematik zu beschaffen.

- Das Anliegen der Algorithmisierung immer weiterer Teile der Mathematik in immer effizienterer Form stellt für die mathematische Forschung eine Fülle neuer Fragestellungen und Probleme, zu deren Beantwortung und Lösung völlig neue oder vertiefte Ideen, Begriffe und Theorien entwickelt werden müssen.

- Die mathematische Ausbildung in den Disziplinen, in denen Mathematik nur Hilfswissenschaft ist, wird sich völlig verändern und einem großen Kreis von Menschen ein viel umfassenderes und reichhaltigeres Bild von der Problemlösekraft der Mathematik vermitteln.

- Die Ausbildung der neuen Generation von Mathematikern wird sich ebenfalls drastisch verändern. Es wird möglich sein, grundlegende mathematische Gedanken in viel umfassenderer, gründlicherer Weise in kürzerer Zeit zu erfassen und damit rascher an die aktuellen Themen der Forschung heranzukommen. Die neue Generation von Mathematikern wird also in sehr viel kürzerer Zeit in die Lage versetzt werden, an der Front der mathematischen Forschung weiterzuarbeiten.

- Gerade in der Algorithmisierung abstrakter Bereiche der Mathematik ist ein hohes Maß an formaler Bildung Voraussetzung. Die Mathematik wird sich also gerade durch die Algorithmisierung in ihrem Abstraktheitsgrad noch erhöhen, denn Automatisierung von Gedanken setzt deren vollständige Formalisierung und einwandfreie formale Durchdringung voraus.

Die Denktechnologie der Mathematik - das Arbeiten in abstrakten Modellen - ist der Kern des technologischen Forschritts auf der Basis der Naturwissenschaften. Algorithmische Mathematik und insbesondere die abstrakteste Ausprägung der algorithmischen Mathematik in Form des Symbolic Computation (Computer-Algebra) hat die Automatisierung des Arbeitens in abstrakten Modellen zum Ziel. Der gesamte technische Fortschritt zielt auf die Automatisierung des Problemlösens in allen Bereichen. Computer-Mathematik zielt auf die Automatisierung des Kernbereichs der technologischen Entwicklungsspirale, auf die Automatisierung der Denktechnologie. *Damit sollte es klar sein, dass Computer-Mathematik eine, wenn nicht* die *Schlüsseltechnologie der heutigen Informationsgesellschaft ist.*

Diese einfache, doch nur wenigen wirklich klar bewusste Tatsache, möchte ich hier aus den folgenden Gründen so betonen:

- Es wird den jungen Menschen heute vielfach eingebläut und vorgelebt, dass der technologische Fortschritt und die darauf aufbauende Wirtschaft das Ergebnis des Schaltens und Waltens derer ist, die in der Politik, in der Finanzwelt, im Marketing, im Management tätig sind. Ohne die Beiträge all dieser Bereiche herunterspielen zu wollen, muss doch die einfache innere Logik des technologischen und wirtschaftlichen Fortschritts klargestellt werden, damit sie nicht in Vergessenheit gerät. Die treibende Kraft des Erfolgs kommt aus der Kreativität der technischen Disziplinen. Wer heute Technik und insbesondere Mathematik studiert, befindet sich im „Auge des Hurrikans" der modernen Entwicklung und nicht irgendwo in einem Hinterzimmer. Es ist heute so motivierend wie noch nie, sich als junger Mensch auf das Abenteuer Mathematik-basierter Technik einzulassen.

- Gerade die algorithmische Mathematik hat eine ungeheure Spannbreite, die die Verbindung der besten Techniken aus der Logik, Mathematik und Informatik erfordert. Sie hat theoretische Tiefe und praktische Schlagkraft. Sie lebt in der Welt der internationalen akademischen Forschung genauso wie in der Welt der heißesten Informations- und Kommunikationstechnologie-Firmen. Gerade die besten Studenten sollten sich deshalb motiviert fühlen, sich in diesem Gebiet ihre Karriere aufzubauen.

- Den politisch Veranwortlichen muss klar werden, wo die Kraftquelle für technologischen Fortschritt und wirtschaftliche Entfaltung sitzt. Es muss deshalb alles getan werden, um den Jugendlichen die Türen zu einem modernen Verständnis der Mathematik zu öffnen und den Bildungs- und Forschungseinrichtungen, die für diesen grundlegenden Bereich des technologischen und wirtschaftlichen Gefüges verantwortlich sind, die besten Voraussetzungen zu schaffen.

- Es ist in den letzten Jahren modern geworden, in den Forschungsförderungsprogrammen die Anwendungen zu entdecken. So wichtig dies als Reaktion auf das Elfenbeinturm-Gehabe mancher Wissenschafter war, wird heute der Bogen mancherorts gefährlich überspannt (siehe z.B. das fünfte Rahmenprogramm der EU). Die treibende Kraft im „Auge des Hurrikans"des technologischen und wirtschaftlichen Fortschritts ist und bleibt das immer feinere Verständnis der Struktur der Natur und die immer wirkungsvollere Beherrschung der wissenschaftlichen Denktechnologie, deren Konzentrat die Mathematik und heute die sich selbst automatisierende Mathematik ist.

Anhang 1: Wavelet-Transformation eines Ultraschald-Bildes

Das *erste Bild* ist ein Schnitt aus einem dreidimensionalen Ultraschall-Datensatzes eines Embryos. Das Bild braucht ca. 16 MB Speicher und die Übertragung der vielen hundert Schnitte braucht eine entsprechend große Zeit. Das *zweite Bild* zeigt denselben Schnitte nach Kompression und nachheriger Dekompression mit der neuen, auf Gröbner-Basen basierenden Wavelet-Methode. Das komprimierte Bild braucht nur 1/25 des Originalbildes! Damit sinkt auch die Übertragungszeit auf 1/25. Das dekomprimierte Bild ist mit freiem Auge nicht vom Original zu unterscheiden. Das *dritte Bild* zeigt die - zwölffach verstärkte - Unterschiedsmenge und demonstriert, dass zwischen dem Original und dem dekomprimierten / komprimierten Original tatsächlich kaum ein Unterschied besteht.

In zeitkritschen Anwendungen wie der Medizin kann also mit dieser Methode die Übertragungsleistung drastisch gesteigert werden, ohne dass die Qualität der Information leidet.

Anhang 2: Inkonstruktiver Beweis der Existenz von Gröbner-Basen

Sei $\mathbf{P}$ die Menge der multivariaten Polynomen über einem Körper. Für $F \subseteq \mathbf{P}$ ist $\mathrm{I}(F) := \{\sum_{i=1}^{m} h_i f_i \mid h_i \in \mathbf{P}, f_i \in F\}$ (das von F erzeugte Ideal). Für Mengen T von Potenzprodukten sei $\mathrm{I}(T)$ die Menge aller Vielfachen von Elementen in T. Ferner sei $\mathrm{L}(f)$ das höchste Potenzprodukt, das im Polynom f vorkommt (in einer fixen zulässigen Ordnung der Potenzprodukte), entsprechend $\mathrm{L}(F)$ die Menge aller höchsten Potenzprodukte von Polynomen in F. Die Menge F heißt Gröbner-Basis, wenn $\mathrm{I}(\mathrm{L}(F)) = \mathrm{L}(\mathrm{I}(F))$. Das Problem bestehe darin, zu jeder gegebenen Polynommenge F eine Polynommenge G zu finden so, dass $\mathrm{I}(G) = \mathrm{I}(F)$ und G eine Gröbner-Basis ist. Dieses Problem ist in der Tat sehr wichtig, denn man kann zeigen, dass sich viele fundamentale Probleme in der kommutativen Algebra (algebraischen Geometrie) algorithmisch lösen lassen, wenn man für das betrachtete Polynomideal nicht nur irgendeine Basis, sondern eine Gröbner-Basis zur Verfügung hat. Die Konstruktion von Gröbner-Basen ist also eine Art Schlüsselproblem für die algebraische Geometrie.

Eine erste „Lösung“ des Problems besteht darin, $G := \mathrm{I}(F)$ zu setzen. Der Beweis, dass diese Lösung die geforderten Eigenschaften hat, ergibt sich unmittelbar aus den Definitionen und einfachen Eigenschaften von Idealen. Diese Lösung hat die drei Eigenschaften, die böse Zungen als die drei charakteristischen Eigenschaften von mathematischen Aussagen bezeichnen: Sie ist prompt und korrekt aber „völlig nutzlos“. In unserem Fall ist die Lösung nutzlos in dem Sinne, dass die Definition der Funktion I den Mengenbildungsquantor verwendet, der in diesem Fall einen unendlichen, algorithmisch nicht ausführbaren Prozess beschreibt.

Eine zweite Lösung kann man wie folgt „konstruieren“: Man definiert zunächst

$$\mathrm{M}(F) := \{s \in \mathrm{L}(\mathrm{I}(F)) \mid \nexists t \in \mathrm{L}(\mathrm{I}(F))(t \neq s \wedge \ t|s)\}.$$

Auf Grund von Dixons Lemma ist $\mathrm{M}(F)$ immer endlich. Sei nun S eine Auswahlfunktion, die folgende Eigenschaft hat und

$$\forall t \in \mathrm{M}(F)(\mathrm{S}(F,t) \in \mathrm{I}(F) \ \wedge \ t = \mathrm{L}(\mathrm{S}(F,t))).$$

Dann hat

$$G := \{\mathrm{S}(F,t) | t \in \mathrm{M}(F)\}$$

die gewünschten Eigenschaften. Zum Beweis beachte man, dass das höchste Potenzprodukt eines Polynoms $f \in \mathrm{I}(F)$ immer ein Vielfaches des höchsten Potenzprodukts eines Polynoms in G ist. Das Polynom f lässt sich also durch Abziehen eines geeigneten Vielfachen eines

Polynoms in G auf ein Polynom im Ideal mit niedrigerem höchstem Potenzprodukt reduzieren. Weil zulässige Ordnungen noethersch sind, lässt sich f also durch Polynome in G in endlich vielen Schritten auf Null reduzieren.

Diese Lösung des Problems ist immer noch prompt (d.h. in wenigen Denkschritten produzierbar) und auch korrekt, aber schon sehr viel „nützlicher“ in dem Sinne, dass man wenigstens weiß, dass das „konstruierte“ G immer endlich sein muss (was immerhin den Hilbert'schen Basissatz als ein Korollar liefert). Die Lösung ist aber immer noch „nicht wirklich nützlich“, weil selbst im Falle, dass F endlich ist, die Zwischenschritte zur Konstruktion von G etliche „unendliche“ Operationen (die Konstruktion von $\mathrm{I}(F)$, den $\exists$-Quantor mit einem unendlichen Laufbereich und schließlich die Auswahlfunktion S) benutzt, die nicht algorithmisch ausgeführt werden können.

Eine dritte Lösung, die „wirklich nützlich" ist (d.h. die zu beliebigem F ein gewünschtes G in endlich vielen algorithmischen Schritten liefert) braucht einen sehr viel komplizierteren Beweis (also viel mehr Denkschritte) mit zusätzlichen mathematischen Ideen (Begriffen), die im obigen Gerüst nicht vorkommen, siehe [1]. Und erst mit der vollständig algorithmischen Lösung des Problems der Konstruktion von Gröbner-Basen werden dann die vielen anderen fundamentalen Probleme der algebraischen Geometrie (Theorie der Polynomideale) wie z.B. die Konstruktion der Syzygien, die vollständige Lösung algebraischer Gleichungssysteme, das Implizitisierungsproblem, das Invertierungsproblem für polynomiale Abbildungen etc. algorithmisch lösbar. Noch mehr Theorie wird notwendig, wenn man Gröbner-Basen effizient, also mit möglichst wenig Aufwand konstruieren möchte. Es gibt Dutzende Arbeiten darüber. Das heißt: Je algorithmischer und dann je effizienter man mathematische Probleme lösen will, umso *mehr* mathematische Theorie und umso schwierigere Beweise sind nötig und *nicht umgekehrt.*

Literatur

[1] B. Buchberger. An Introduction to Gröbner Bases. In: B. Buchberger, F. Winkler (Hsg.), *Gröbner Bases and Applications.* Cambridge University Press, 1998, pp. 3-31.

[2] Chyzak, F., Paule, P., Scherzer, O., Schoisswohl, A. and Zimmermann, B.: The Construction of Orthonormal Wavelets Using Symbolic Methods and a Matrix Analytical Approach for Wavelets on the Interval. Erscheint in *Experimental Mathematics.*

[3] B. Buchberger. Should Students Learn Integration Rules? *ACM SIGSAM Bulletin*, Vol.24/1, 1990, pp. 10-17.

Danksagung: Diese Arbeit wurde dankeswerter Weise durch den österreichischen Fonds zur Förderung der wissenschaftlichen Forschung (FWF) im Rahmen des Projekts SFB 1302 und durch das Land Oberösterreich im Rahmen des Projekts „Prove" gefördert. Mein Dank gilt außerdem Herrn A. Schoisswohl, Koautor von [2], für die Zurverfügungstellung der Bilder im Anhang 1.