Lehrstuhl für Symbolic Computation

Prof. Dr. **Martin Kreuzer**

Sekretariat:
Nathalie Vollstädt

Wiss. Mitarbeiter:
Martina Kraupner
Bilge Sipal
Thomas Stadler

Doktoranden:
Samina Batul
Rashid Ali
Ehsan Ullah

Nanu? Ein neuer Lehrstuhl?

Nicht ganz. Seit Oktober 2007 heißt der Lehrstuhl für Mathematik mit dem Schwerpunkt Algebra jetzt Lehrstuhl für Mathematik mit dem **Schwerpunkt Symbolic Computation.**

Wie bitte? Symbolic Computation? Was ist denn das schon wieder?

Das kennen Sie eigentlich bereits aus der Schule, nur heißt es dort **„Rechnen mit Buchstaben“**, also zum Beispiel Formeln wie $(x+y) \cdot (x-y) = x^2 - y^2$. Natürlich lassen wir hier an der Universität den Computer für uns rechnen.

Und wozu soll das gut sein?

Symbolic Computation hat viele Anwendungen, innerhalb und außerhalb der Mathematik. Häufig lassen sich in **Naturwissenschaft und Technik** die betrachteten Vorgänge durch Polynomgleichungen beschreiben.
Eine der wichtigsten Anwendungen symbolischer Berechnungen ist das **Lösen algebraischer Gleichungssysteme**, d.h. von Gleichungssystemen der Form

$$f_1(x_1, \ldots, x_n) = 0$$
$$f_2(x_1, \ldots, x_n) = 0$$
$$\ldots$$
$$f_s(x_1, \ldots, x_n) = 0$$

mit Polynomen $f_1, \ldots, f_s$ in den n Unbestimmten $x_1, \ldots, x_n$.

Sollte man die Lösungen solcher Gleichungssysteme nicht besser näherungsweise mit numerischen Methoden bestimmen?

Das kann man manchmal gar nicht. Denken Sie zum Beispiel an einen Ingenieur, der ein Maschinenteil entwerfen muss. Er möchte gewisse **Designparameter** unbestimmt lassen, seine Gleichungen in Abhängigkeit von den Parametern lösen und diese dann so wählen, dass die Lösung schöne Zusatzeigenschaften besitzt. Oder betrachten Sie die Gleichungssysteme in der **algebraischen Kryptographie**, die wir weiter unten besprechen. Bei denen sucht man die Lösungen in so genannten endlichen Körpern, wo es keine Näherungswerte gibt.

Was? Endlicher Körper? Sind nicht alle Körper endlich? Meiner auf jeden Fall schon.

In der Mathematik versteht man unter einem Körper einen Zahlbereich, in dem die vier Grundrechenarten existieren und die üblichen Rechenregeln gelten. Ein endlicher Körper wäre zum Beispiel die Menge F2 = {0,1} versehen mit der Arithmetik modulo 2, die in der Informatik eine große Rolle spielt. Die rationalen Zahlen und die reellen Zahlen bilden unendliche Körper.

Und in solchen Körpern rechnen Sie herum?

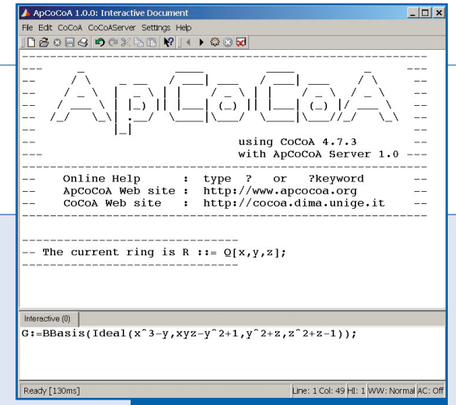
Nicht wirklich. Wir verwenden die Körperelemente nur als Koeffizienten für Polynome, denen unsere eigentliches Interesse gilt. Denn mit Polynomen und Polynomidealen kann man in viel allgemeineren Zahlbereichen, sogenannten Ringen, Moduln und Algebren, explizite Berechnungen durchführen.

All dies sind doch wieder nur fantastische Theorien von Elfenbeinturm-Mathematikern. Wenn man diese Methoden in der Praxis implementieren würde, wären sie bestimmt unbrauchbar.

Ganz und gar nicht. Alle Algorithmen werden von den Studenten und Mitarbeitern am Lehrstuhl im Computeralgebrasystem **ApCoCoA** (das bedeutet „Applied Computations in Commutative Algebra“) implementiert und für konkrete Industrieprojekte verwendet.

Aha. Und ich dachte, dies wäre ein Lehrstuhl für reine Mathematik.

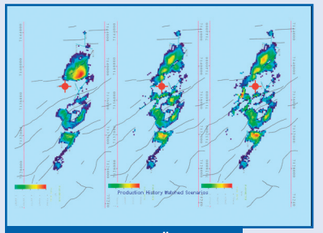
Auch reine Mathematik kann anwendungsorientiert sein. Eines unserer **Hauptforschungsgebiete** ist zum Beispiel die **Theorie der Randbasen**. Sie stellen eine Verbesserung der bekannten **Gröbner-Basen** dar, welche ja im Zentrum fast jeder symbolischen Computerberechnung stehen. Randbasen sind für Anwendungen aber noch geeigneter als Gröbner-Basen: sie erhalten die in der Problemstellung vorhandenen Symmetrien besser und sind numerisch stabiler, d.h. weniger anfällig für Störungen der Ausgangsdaten.



Cas ApCoCoA Begrüßungsbildschirm

Soll das heißen, dass die Ausgangsdaten auch echte Messdaten sein können? Kann man die exakten Berechnungen der Computeralgebra denn tatsächlich in einer industriellen Anwendung einsetzen?

Durch die gestiegene Leistungsfähigkeit der Computer und unserer Algorithmen ist dies tatsächlich möglich. Das größte diesbezügliche Projekt am Lehrstuhl hat den bezeichnenden Namen **Algebraisches Erdöl**.



Entwicklung eines Ölfelds

Algebraisches Erdöl

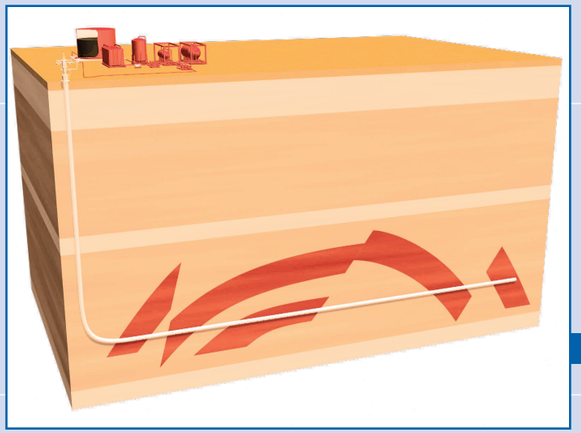
Das soll wohl ein Witz sein, nicht wahr?

Absolut nicht. Es geht um nichts Geringeres als den **Schutz der Umwelt** und die **Sicherung der Energieversorgung** der ganzen Welt.

Und wie soll das funktionieren?

Wussten Sie, dass am Ende der Lebensdauer eines Ölfelds mehr als 70 % des ursprünglich vorhandenen Rohstoffs immer noch in der Erde sind? Unser Ziel ist es, die **Gesamtausbeute** deutlich zu erhöhen. Dann bräuchte man nicht in ökologisch sensiblen Gegenden wie in Alaska zu bohren. Auch die Tatsache, dass seit Jahren kein neues großes Erdölfeld mehr gefunden wurde, wäre weniger beunruhigend.

Das müssen Sie mir jetzt schon genau erklären. Wie wollen Sie denn diese Gesamtausbeute mit Hilfe von symbolischen Berechnungen verbessern? Das klingt wie ein Hirngespinst.



Schematischer Aufbau eines Ölfelds im Laufe der Zeit

Das ist es aber ganz und gar nicht. Es sind auch keine rein symbolischen Berechnungen, sondern so genannte **symbolisch-numerische Berechnungen**. Die Approximate Computational Algebra ist ein noch sehr junges und aufstrebendes Gebiet.

Ja, ja, aber wie soll das nun wirklich gehen?

Basierend auf den **Messdaten der Ölquellen und Förderpunkte** eines Felds (z.B. Drücke und Temperaturen der Phasen Öl, Gas und Wasser) stellen wir Modellgleichungen für die einzelnen Quellen und für die Gesamtproduktion auf. Aus der Aufteilung der Gesamtproduktion auf die einzelnen Förderpunkte können wir Rückschlüsse darüber ziehen, wie sich die verschiedenen Quellen gegenseitig beeinflussen wenn sie gleichzeitig produzieren.

Und wozu soll diese Information gut sein?

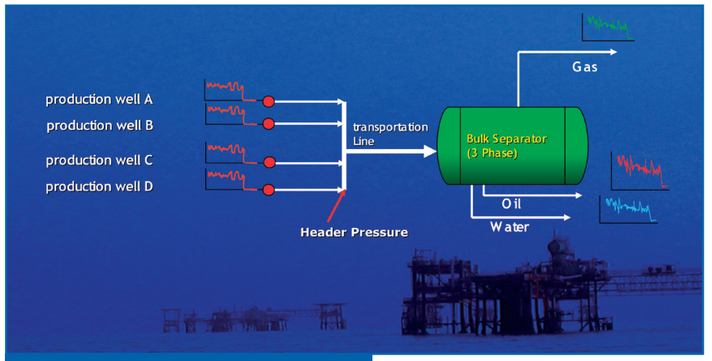
Wenn man Modellgleichungen besitzt, die die Entwicklung eines Ölfelds über längere Zeiträume korrekt vorhersagen, kann man durch eine **gezielte Produktionsstrategie** das Absinken des Öldrucks eines Felds verlangsamen und dadurch die Gesamtausbeute verbessern.

So ein Ölkonzern beschäftigt doch Tausende von Geologen, Physikern und angewandten Mathematikern. Warum haben die denn diese Modellgleichungen nicht schon längst gefunden?

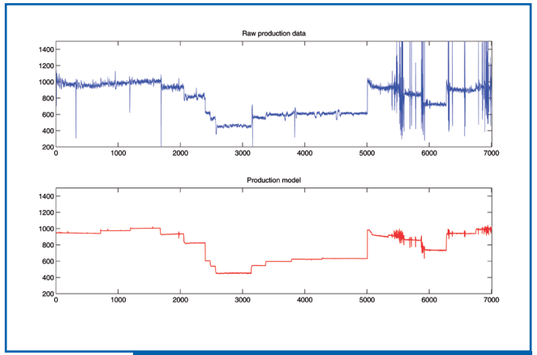
Bei den klassischen Ansätzen versuchte man stets, vorgegebene Gleichungen, z.B. partielle Differentialgleichungen für das Sickern von Öl durch Gestein, an die jeweilige Situation anzupassen. Dies scheitert jedoch daran, dass man die meisten der benötigten Daten wie die Durchlässigkeit der Gesteinsschichten, unterirdische Verwerfungen usw. nicht genau genug kennt.

Aha. Aber wenn man das alles nicht weiß, wie soll man da mit Ihrem Methoden weiterkommen?

Unser Ansatz ist entgegengesetzt: anstatt das physikalische System der Gestalt der Gleichungen, die nur unseren Vorurteilen entspringt, zu unterwerfen, **starten wir zu 100 Prozent mit den Messdaten** und suchen darin nach Modellgleichungen, die approximativ erfüllt sind.



Schematischer Aufbau der Messumgebung



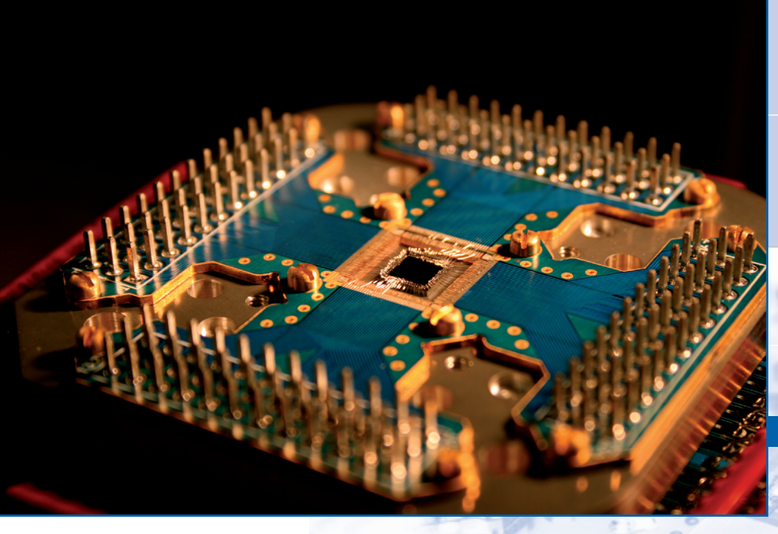
Ein polynominales Modell der Gesamtproduktion

Das ist ja kaum zu glauben. Funktioniert denn dieser Ansatz auch in der Praxis?

Das tut er. In Brunei gelang es uns z.B. bereits, die **Förderung einer Quelle um 10 % zu verbessern**, indem wir die Ingenieure baten, das Ventil des besten Förderpunktes teilweise zu schließen. Das ging zwar völlig wider deren Intuition, wurde uns von unseren Modellgleichungen aber angeraten. Unser Verfahren ist inzwischen für ein **weltweites Patent** angemeldet.

Damit besteht der Lehrstuhl für Symbolic Computation aus einen Haufen von Ölfuzzis, oder?

Ganz und gar nicht. Wir studieren auch mehr theoretischorientierte Themen wie die **Algebraische Kryptographie.**



Ein 16-bit Quantenprozessor

Algebraische Kryptographie

Was ist das denn schon wieder?

Eine der Hauptaufgaben der Kryptographie ist die **verschlüsselte Übermittlung** von Nachrichten über einen öffentlichen Kanal. Dabei soll ein unberechtigter Empfänger, also jemand der den Geheimschlüssel nicht besitzt, die Nachricht nicht dechiffrieren können.

Das wusste ich schon. Aber wo ist hier der Bezug zur Algebra und zu Symbolic Computation?

Wir beschäftigen uns mit zwei Bereichen der algebraischen Kryptographie. Der eine ist die **Konstruktion neuer Kryptosysteme mit Hilfe von Gröbner-Basen** in nichtkommutativen algebraischen Strukturen.

Wie bitte? Warum denn? Es gibt doch bereits so hervorragende Verschlüsselungsmethoden wie das RSA System.

In der Tat, das **RSA Kryptosystem** ist das mit weitem Abstand in der Praxis am häufigsten angewandte. Aber wie alle anderen praxisrelevanten Kryptosysteme auch hat es zwei gravierende Mankos: zum einen ist die genaue Komplexitätsklasse des zu Grunde liegenden zahlentheoretischen Problems nicht bekannt und zum anderen wurde bewiesen, dass man das RSA System mit einem Quantencomputer brechen kann. Es ist also nur noch eine Frage der Zeit bis die momentan gängigen Kryptosysteme alle unsicher sind.

Heißt das, wenn ich auch weiterhin meine Bankgeschäfte und Einkäufe über das Internet abwickeln möchte, brauche ich neue Verschlüsselungstechniken? Dann erfinden Sie mal ganz schnell etwas.

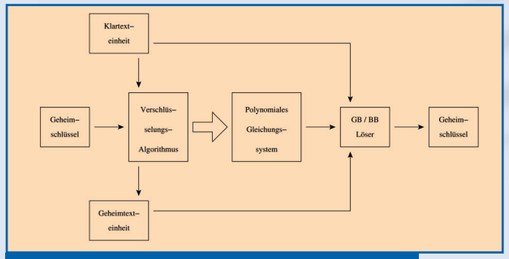
Wir werden unser Bestes tun. Aber bevor wir konkrete Vorschläge machen können, ist hier noch viel theoretische Grundlagenarbeit zu verrichten, da viele der Strukturen, die wir im Auge haben, bezüglich ihrer kryptographischen Verwendbarkeit noch unerforscht sind.

Sie sprachen von zwei Bereichen der algebraischen Kryptographie, in denen der Lehrstuhl aktiv ist.

Nun, es gibt natürlich noch die dunkle Seite der Macht. Hier tritt sie unter der Bezeichnung **Kryptoanalyse** auf. Man kann mit symbolischen Berechnungen auch versuchen, symmetrische Kryptosysteme zu knacken.

Wieder mit diesen Gröbner-Basen? Das klingt aber sehr verdächtig nach einem Allheilmittel.

Ob man am besten Gröbner-Basen, Randbasen oder andere Techniken verwenden sollte, wissen wir noch nicht. Auf jeden Fall entwickeln wir so genannte algebraische Angriffe. Das ist eine spezielle Form von **Known-Plaintext-Angriffen**, bei denen man die Berechnung des Geheimschlüssels zurückführt auf das Lösen eines algebraischen Gleichungssystems über einem endlichen Zahlbereich.



Schematischer Ablauf eines algebraischen Angriffs

Und das funktioniert? Ist jetzt sogar der offizielle Advanced Encryption Standard (AES) unsicher?

So weit sind wir noch nicht. Aber es sind bereits bedeutende kryptographische Herausforderungen mit symbolischen Berechnungen gelöst worden und man sollte jedes neue symmetrische Kryptosystem erst einer **Sicherheitsüberprüfung** gegen algebraische Angriffe unterziehen.

Das ist ja alles kaum zu glauben. Ein Bekannter von mir hat in seiner Firma auch ein mathematisches Problem, bei dem er schon seit längerem nicht weiterkommt. Glauben Sie, dass Sie ihm mit Ihrer „Symbolic Computation“ helfen könnten?

Das weiß ich natürlich nicht. Aber wir hier am Lehrstuhl sind gegenüber Anwendungsmöglichkeiten unserer Theorien und Algorithmen immer sehr aufgeschlossen. Sagen Sie Ihren Bekannten doch einfach, er soll sich bei uns melden. Vielen Dank für das Gespräch und genießen Sie noch die 25-Jahr-Feier!