Promotionen in der Computeralgebra

Ehsan Ullah: New Techniques for Polynomial System Solving
Betreuer: Martin Kreuzer (Passau)
Zweitgutachter: Lorenzo Robbiano (Genua)
Juli 2012
http://www.opus-bayern.de/uni-passau/volltexte/2012/2681/

Zusammenfassung:

In den letzten Jahren ist es in der algebraischen Kryptoanalyse immer wichtiger geworden, spezielle Systeme polynomialer Gleichungssysteme zu lösen: der Grundkörper ist endlich, es gibt i.A. genau eine Lösung, und diese ist über dem Grundkörper definiert. In dieser Dissertation entwickelt, implementiert und analysiert der Autor eine Reihe von Methoden, um auch große Beispiele solcher Gleichungssysteme zu lösen. Er verwendet dabei Techniken, die aus verschiedenen Gebieten der Mathematik stammen.

(1) Methoden aus der linearen Algebra basieren auf den Techniken von J. de Loera und anderen, bei der das polynomiale Gleichungssystem durch immer größere lineare Gleichungssysteme approximiert und jeweils nur die Lösbarkeit untersucht wird. Diesen Ansatz kombiniert der Autor geschickt mit der Idee der *Mutants* von J. Ding.

(2) Methoden aus der diskreten Optimierung, insbesondere Integer Programming (IP), Mixed Integer Programming (MILP) und Mixed Integer Non-Linear Programming (MINLP) werden anwendbar, indem man das Gleichungsysstem in eine Menge linearer Ungleichungen über $\mathbb{Z}$ umwandelt. Hierzu werden eine Reihe von Konversionsalgorithmen entwickelt und miteinander verglichen. Wie zu erwarten haben sie einen großen Einfluß auf das Laufzeitverhalten der verwendeten IP-Solver.

(3) Weitere betrachtete Methoden sind die Umwandlung in ein SAT-Problem und anschließende Verwendung eines SAT-Solvers, Umwandlung in ein lineares Diophantisches Gleichungssystem über $\mathbb{Z}$ mit Berechnung der Smith Normalform, und die Umwandlung in ein relles oder komplexes Gleichungssystem mit Verwendung von Methoden aus der numerischen Analysis, insbesondere der Newton-Methode und der Homotopie-Fortsetzungsmethoden.

Die Arbeit hat einen erheblichen Umfang und wird durch eine Vielzahl an Implementationen und Timings expliziter Beispiele aus der Kryptoanalyse ergänzt.

Xingqiang Xiu: Non-Commutative Gröbner Bases and Applications
Betreuer: Martin Kreuzer (Passau)
Zweitgutachter: Gerhard Rosenberger (Hamburg)
Juli 2012
http://www.opus-bayern.de/uni-passau/volltexte/2012/2682/

Zusammenfassung:

Während die Algorithmen zur Berechnung von Gröbner-Basen für Ideale im kommutativen Polynomring hochentwickelt und weitgehend optimiert sind, ist die Situation für zweiseitige Ideale im nicht-kommutativen Polynomring (also in der freien assoziativen Algebra) weit weniger erfeulich. Es gibt kein Standardlehrbuch für die theoretischen Grundlagen, es gibt nur wenige, oft nicht sehr zugängliche Implementationen, und mögliche Optimierungen der Buchberger-Prozedur sind nur ansatzweise untersucht worden. Die Dissertation von X. Xiu versucht hier etwas Abhilfe zu schaffen. Nachdem die Grundlagen ausführlich entwickelt werden, untersucht und optimiert der Autor die Buchberger-Prozedur. Dazu werden die Obstruktionen (also die nicht-kommutativen Analoga der kritischen Paare) sorgfältig minimiert und es werden nicht-kommutative Analoga der Gebauer-Möller Kriterien zur Paarvermeidung entwickelt. Auch die Art und Anzahl der notwendigen Interreduktionen wird eingeschränkt, so dass sich eine stark optimierte, performante Version der Buchberger-Prozedur ergibt.

In weiteren Kapiteln werden Anwendungen auf Berechnungen für Untermoduln freier zweiseitiger Moduln, eine nicht-kommutative Version des F4-Algorithmus, Gröbner-Basisberechnugnen in Restklassenringen nicht-kommutativer Polynomringe (z. B. in Gruppenringen) und Methoden zur Bestimmung der Gelfand-Kirillov Dimension sowie der nicht-kommutativen Hilbert-Funktion beschrieben.

Der Autor hat alle Algorithmen effizient in einem C++ Paket für das Computeralgebrasystem ApCoCoA implementiert, das frei verfügbar ist. Die Dissertation enthält auch viele mit diesem Paket berechnete Beispiele und Timings.

Stephan Ritscher: Degree Bounds and Complexity of Gröbner Bases of Important Classes of Polynomial Ideals
Betreuer: Ernst W. Mayr (TUM Informatik)
Gutachter: Gregor Kemper (TUM Mathematik), Chee Yap (New York University)
Oktober 2012
http://mediatum.ub.tum.de/doc/1006213/1006213.pdf

Zusammenfassung:

Polynomial ideals have been intensely studied by computer scientists. The method of Buchberger allows to effectively solve the membership problem to which a variety of other interesting problems can be reduced. Mayr and Meyer showed, that these computations are very expensive in the worst case. As a consequence, special ideal classes have to be identified for which the membership problem can be solved more efficiently. As previous results show, the complexity of the membership problem is mainly related to the degrees of the representation problem and Gröbner bases. Thus the first part of the thesis studies degree bounds for various ideal classes. The main contributions are upper and lower bounds for Gröbner bases depending on the ideal dimension and some results for toric ideals. In the second part, these findings are applied to questions of complexity. The presentation comprises an incremental space-efficient algorithm for the computation of Gröbner bases, an algorithm in polylogarithmic space for the membership problem in toric ideals and the space-efficient computation of the radicals of low-dimensional ideals.