Promotionen in der Computeralgebra

Maximilian Boy: On the Second Class Group of Real Quadratic Number Fields
Betreuer: Gunter Malle (Kaiserslautern)
Zweitgutachter: Jürgen Klüners (Paderborn)
Februar 2012
`https://kluedo.ub.uni-kl.de/frontdoor/index/index/docId/2885`

Zusammenfassung:

This thesis generalizes the Cohen-Lenstra heuristic for the class groups of real quadratic number fields to higher class groups. A "good part" of the second class group is defined. In general this is a non abelian proper factor group of the second class group. Properties of those groups are described, a probability distribution on the set of those groups is introduced and proposed as generalization of the Cohen-Lenstra heuristic for real quadratic number fields. The calculation of number field tables which contain information about higher class groups is explained and the tables are compared to the heuristic. The agreement is close. A program which can create an internet database for number field tables is presented.

Christian Eder: Signature-based algorithms to compute standard bases
Betreuer: Gerhard Pfister (Kaiserslautern)
Zweitgutachter: Vladimir Gerdt (Dubna)
April 2012
`http://www.mathematik.uni-kl.de/~ederc`

Zusammenfassung:

Standard bases are one of the main tools in computational commutative algebra. In 1965 Buchberger presented a criterion for such bases and thus was able to introduce a first approach for their computation. Since the basic version of this algorithm is rather inefficient due to the fact that it processes lots of useless data during its execution, active research for improvements of those kind of algorithms is quite important.

In this thesis we introduce the reader to the area of computational commutative algebra with a focus on so-called signature-based standard basis algorithms. We do not only present the basic version of Buchberger's algorithm, but give an extensive discussion of different attempts optimizing standard basis computations, from several sorting algorithms for internal data up to different reduction processes. Afterwards the reader gets a complete introduction to the origin of signature-based algorithms in general, explaining the underlying ideas in detail. Furthermore, we give an extensive discussion in terms of correctness, termination, and efficiency, presenting various different variants of signature-based standard basis algorithms.

Whereas Buchberger and others found criteria to discard useless computations which are completely based on the polynomial structure of the elements considered, Faugère presented a first signature-based algorithm in 2002, the F_5 Algorithm. This algorithm is famous for generating much less computational overhead during its execution. Within this thesis we not only present Faugère's ideas, we also generalize them and end up with several different, optimized variants of his criteria for detecting redundant data.

Being not completely focussed on theory, we also present information about practical aspects, comparing the performance of various implementations of those algorithms in the computer algebra system SINGULAR over a wide range of example sets.

In the end we give a rather extensive overview of recent research in this area of computational commutative algebra.

Berichte von Konferenzen

1. **Symbolic Computation and its Applications**

   Aachen, 17.–20. Mai 2012

   `http://www.computeralgebra.de/SCA2012`

The second conference "Symbolic Computation and its Applications" was organized by Lehrstuhl D für Mathematik, RWTH Aachen. This conference, as well as the first one which was held in Maribor, Slovenia in 2010, was designed to discuss new developments in the theory of symbolic and symbolic-numeric computation, algorithms and software oriented to enhancing their applicability to modern problems of science and engineering.

Among the 32 speakers, there were 8 speakers from Germany, 6 from France, 5 from Spain, 3 from Austria, 2 from Russia, and one each from Canada, Emirates, Japan, Slovenia, Sweden, UK, Ukraine, and USA.

16 talks presented at the conference were devoted to investigation and improvement of computer algebra algorithms for symbolic summation, primary decomposition of polynomial ideals, construction of solutions to polynomial systems, ordinary differential and difference equations, partial differential equations, integro-differential operator equations, for matrices whose entries are Ore polynomials, for fuzzy ideals over non-commutative rings, for Lie algebras. In 3 talks, the latest versions of computer algebra software systems Maple 16 and Sage as well as the Maple package Isolde for solving linear functional systems were presented and their new features were discussed. In 8 talks, the applications of computer algebra methods, algorithms and software were given for solving real problems in biology, applied dynamical systems, nonli-

near and non-commutative problems in mathematical physics, in fuzzy logic and in numerical analysis. In 5 talks, there were presented and discussed some unsolved computational problems in the theory of D-modules, algebraic analysis, non-commutative algebra, theory of Lie groups, detection of the Hopf bifurcations and oscillations in multidimensional dynamical systems.

All talks were well attended and intensively discussed by the participants of the conference.

Vladimir P. Gerdt (Dubna, Russia)

2. WMC 2012 – Workshop on Mathematical Cryptography und SCC 2012 – Third Int. Conference on Symbolic Computation and Cryptography

Castro-Urdiales, Spanien, 9.–13. Juli 2012

`http://scc2012.unican.es`

Direkt im Anschluss an den *Workshop on Mathematical Cryptology* vom 9.-11.7.2012 fand am International Center for Mathematical Meetings (CIEM) in Castro-Urdiales (Spanien) die nach Beijing 2008 und Egham 2010 dritte Ausgabe der Konferenz *Symbolic Computation and Cryptography (SCC)* statt.

Mit ca. 60 Teilnehmern und insgesamt 36 Vorträgen deckte die Workshop/Konferenz Kombination ein weites Spektrum der mathematischen Kryptologie ab: die Themen reichten von Methoden der diskreten Mathematik (Gitter, Learning with Errors, Codes) über die bekannten zahlentheoretischen Ansätze (RSA, hyperelliptische Kurven, diskreter Logarithmus) bis hin zur Computeralgebra (multivariate PKC, algebraische Angriffe, Fehlerangriffe).

Ein besonderes Highlight war der Vortrag "Untangling Attribution: Understanding the Requirements for Network Attribution" von Susan Landau, in dem die politische und rechtliche Dimension der Kryptographie am Beispiel der Anonymität im Internet aufgezeigt und an realen Fällen aus der Praxis lebhaft illustriert wurde. Weitere Hauptvorträge wurden von Nadia Heninger (Microsoft Research), Éric Schost (London/Ontario) und Damien Stehlé (ENS Lyon) gehalten.

Die Konferenz war von Jean-Charles Faugère (Inria/Frankreich) und dem lokalen Team um Jaime Gutierrez (Santander/Spanien) hervorragend organisiert, und auch das etwas wechselhafte Wetter lenkte nicht von der inhaltsreichen Tagung ab. Ein Tagungsband wird in einem speziellen Heft des *Journal of Symbolic Computation* erscheinen.

Martin Kreuzer (Passau)

3. 37th International Symposium on Symbolic and Algebraic Computation (ISSAC)

Grenoble, Frankreich, 22.–25. Juli 2012

`http://www.issac-conference.org/2012`

Die diesjährige ISSAC-Konferenz wurde vom 22. bis zum 25. Juli in Grenoble abgehalten und stand unter der organisatorischen Leitung von Joris van der Hoeven (General Chair), Mark van Hoeij (Program Committee Chair) und Jean-Guillaume Dumas (Local Arrangement Chair). Unterstützt wurde die Tagung von mehreren Sponsoren, von denen insbesondere die französische Organisation INRIA für ihren besonders großzügigen Beitrag hervorgehoben werden sollte. Im Anschluss an die Konferenz wurden zwei weitere Workshops angeboten, nämlich MaGiX am 26.–27. Juli und CaCoS am 26. Juli.

Traditionell wurde die Tagung mit einem Tutorientag eröffnet, welcher diesmal von Agnes Szanto (North Carolina State University) organisiert wurde. Es sprachen Pascal Koiran (ENS de Lyon) über "Upper bounds on real roots and lower bounds for the permanent", Seth Sullivant (North Carolina State University) über "Algebraic statistics" und der Autor dieser Zeilen über "Elements of computer algebraic analysis". Alle Tutorien waren gut besucht und liefen in einer diskussionsfreundlichen Atmosphäre ab.

Die Höhepunkte der drei folgenden Konferenztage bildeten jeweils die Vorträge der drei eingeladenen Sprecher: Frits Beukers (University of Utrecht) trug über "Hypergeometric functions: computational aspects" vor, Volker Strassen (emeritiert) über "Asymptotic spectrum and matrix multiplication", sowie Marie-Françoise Roy (University of Rennes) über "Complexity of deciding connectivity in semi-algebraic sets: recent results and future research directions".

Aber auch das weitere Programm war mit insgesamt 46 Vorträgen, 8 Software-Präsentationen, Präsentationen von Industriepartnern und mehreren Slots für Posterpräsentationen reichlich gefüllt und interessant.

Das Konferenzdinner gab der Veranstaltung einen angemessenen Rahmen, angefangen mit einer Gondelfahrt zur Burg Bastille, welche auf dem gleichnamigen Berg über Grenoble mit den Flüssen Isère und Drac thront. Das Abendessen mit vielen Spezialitäten aus der Region wurde anschließend im Restaurant du Téléphérique serviert. Die Preisverleihungen waren ein Höhepunkt des Abends und trugen zur gemütlichen Atmosphäre bei.

Es wurde beschlossen, dass die ISSAC 2014 in Kobe, Japan, stattfinden soll, und sie wurde bereits als Satellitenkonferenz zum International Congress of Mathematicians (ICM 2014, 13.–21. August 2014, Seoul, Südkorea) gemeldet. Die nächste ISSAC-Tagung 2013 wird an der Northeastern University in Boston, USA, abgehalten.

Viktor Levandovskyy (Aachen)

4. Computer Algebra in Scientific Computing (CASC 2012)

Maribor (Slowenien), 3.–6. September 2012

`http://www14.in.tum.de/konferenzen/CASC2012/`

Vom 3. bis zum 6. September 2012 fand der *14. International Workshop on Computer Algebra in Scientific Computing* in Maribor in Slowenien statt, in hervorragender Weise vor Ort organisiert von Prof. V. Romanovski vom Center for Applied Mathematics and Theoretical Physics (CAMTP) der Universität Maribor, zusammen mit M. Petkovšek (Ljubljana) und M. Robnik (Maribor). Maribor ist übrigens Kulturhauptstadt des Jahres 2012.

Wie in vergangenen Jahren deckte die Tagung, die einer besonderen Zusammenarbeit zwischen Staaten der ehemaligen Sowjetunion (GUS) und Deutschland entsprang und

eigentlich abwechselnd in GUS-Ländern bzw. in Deutschland stattfindet, dieses Mal aber, mit Blick auf die rege einschlägige Forschungsaktivität am CAMTP, ausnahmsweise in Slowenien geplant wurde, einen weiten Themenbereich ab.

Die Tagung umfasste 28 reguläre Vorträge, zwei eingeladene Präsentationen und eine kleine Poster Session.

Wie schon bei früheren CASC-Tagungen lag ein klarer Schwerpunkt bei Differential- und Differenzengleichungen bzw. Dynamischen Systemen mit Anwendungen in der Physik. Eine Reihe von Vorträgen befasste sich mit der Untersuchung und Lösung von durch (gewöhnliche) Differentialgleichungen modellierten Problemen, z. B. für biochemische Reaktionsnetzwerke oder Normalformen der Lösung der Euler-Poisson-Gleichungen, oder etwa der Stabilität „geschalteter" Systeme linearer Differentialgleichungen.

Auch wurden z. B. neue Algorithmen für die Lösung des Randwertproblems für die Schrödinger-Gleichung in zylindrischen Koordinaten oder für Navier-Stokes in 3D gezeigt.

Natürlicherweise spielten Anwendungen symbolischer Berechnung eine große Rolle, etwa bei der Stabilitätsuntersuchung eines (eingeschränkten) 4-Körper-Problems der Himmelsmechanik oder eines Gyroskop-Systems mit vier Freiheitsgraden.

Aber auch klassische Fragestellungen der Computeralgebra kamen zu Wort, mit Themen wie: Berechnung (verschiedener Typen) von Gröbnerbasen, Berechnung der Jacobson-Form von Matrizen oder von Ore-Polynomen, die Inversion on Polynommatrizen, oder innovative Ansätze für so elementare Probleme wie die Berechnung der dritten Potenz einer (sehr großen) natürlichen Zahl oder die effiziente Berechnung der Potenzen eines Polynoms in „dünner" Darstellung.

In den beiden eingeladenen Vorträgen behandelte zunächst K. Yokoyama das Problem der effizienten Berechnung von Operationen auf Polynomidealen mittels modularer Methoden, insbesondere die Berechnung von Gröbnerbasen und von (reduzierten) Normalformen von Polynomen. Der zweite eingeladene Vortrag, von G. Kemper, gab einen interessanten Überblick über Invariantentheorie mit Anwendungen in Bereichen wie Graphentheorie, Computer Vision und Kodierungstheorie, und er diskutierte auch den aktuellen Stand der Algorithmenentwicklung in diesem Querschnittsgebiet.

Das gesamte Programm der Tagung ist auf der Webseite
`http://www14.in.tum.de/konferenzen/CASC2012/program.html`
zu finden, die Online-Version der Proceedings (LNCS 7442) steht auf
`http://www.springerlink.com/content/978-3-642-32972-2/`
zur Verfügung.

Ernst W. Mayr (München)

5. Herbsttagung des Arbeitskreises Mathematikunterricht und Informatik 2012 und Tagung „Computeralgebra in Lehre, Ausbildung und-Weiterbildung" der Fachgruppe Computeralgebra

Soest, 28.–30. September 2012

`http:didaktik-der-mathematik.de/ak/mui`

Vom 28. bis zum 30. September fand die Herbsttagung des Arbeitskreises Mathematikunterricht und Informatik (AK MU&I) der Gesellschaft für Didaktik der Mathematik wie in den letzten Jahren gemeinsam mit der Tagung „Computeralgebra in Lehre, Ausbildung und Weiterbildung" der Fachgruppe Computeralgebra in Soest statt. Die Tagung des Arbeitskreises dient jenen, die sich mit der Rolle der Informatik im Mathematikunterricht und speziell dem Einsatz von digitalen Werkzeugen im Mathematikunterricht sowie den entsprechenden Auswirkungen in methodischen, didaktischen, mathematischen und auch politischen Bereichen befassen. Die Tagung feierte in diesem Jahr ihr dreißigstes Jubiläum, und man stellte sich aus diesem Anlass die Frage „Quo vadis?". Einige Teilnehmer erinnerten auch in Vorträgen an die Anfänge des Arbeitskreises und die Entwicklung im Laufe der vergangenen Jahre. Prof. Dr. Jochen Ziegenbalg hielt den ersten Hauptvortrag zum Thema Informatik-affine Themen in der Didaktik der Mathematik und gab darin eine kurze historische Skizze des Arbeitskreises. Er erinnerte auch an fundamentale Ideen und Prinzipien und stellte die Frage, was speziell an Informatik-Themen bildungsrelevant ist. Hierbei fasste er das Programmieren weit und stelle es auch als Ziel des Mathematikunterrichts heraus. Im zweiten Hauptvortrag [Mehr als] 30 Jahre AK MU&I – Mathematik? Unterricht? Informatik? gaben Hans-Jürgen Elschenbroich und Henning Körner eine persönliche Rückschau auf ihren Einstieg und die Zeit im AK MU&I und erinnerten sich daran, dass die Frage nach den Grundfertigkeiten in Mathematik auch ein Thema des AK MU&I ist, obwohl man sie auf den ersten Blick nicht mit Informatik oder Werkzeugeinsatz in Verbindung bringt. Prof. Dr. Reinhard Oldenburg (Frankfurt) blickte im Hauptvortrag Informatik – Auch das noch?! Ein Reiseführer in die Zukunft des AK MU&I der Zeit voraus. Er unterschied einerseits zwischen Mediendidaktik und Medienkunde, differenzierte andererseits den Computer als „Numerikmaschine", „Symbolikmaschine" und „Funktionsmaschine". Am Beispiel der Behandlung des Heron-Algorithmus mithilfe der Software Scratch zeigte er die mögliche zukünftige Anwendung von Computern im Mathematikunterricht auf. Neben weiteren interessanten Sektionsvorträgen fand eine Podiumsdiskussion statt, in der die Hauptvortragenden engagiert teilnahmen. Die Diskussionsrunde wurde geleitet von Christoph Drösser (Die Zeit), der neben der Moderation auch selbst einen kompetenten Einblick in die Mathematik und die Thematik des Arbeitskreises zeigte.

Hannes Stoppel (Münster)