05021 Summary - Mathematics, Algorithms, Proofs

T. Coquand, H. Lombardi, M.-F. Roy
09.01.-14.01.05

General Presentation

This workshop was the third MAP meeting, a continuation of the seminar "Verification and constructive algebra" held in Dagstuhl from 6 to 10 January 2003. The goal of these meetings is to bring together people from the communities of formal proofs, constructive mathematics and computer algebra (in a wide meaning). The special emphasis of the present meeting was on the constructive mathematics and efficient proofs in computer algebra. We were honored to have as invited speakers Helmut Schwichtenberg, proof theorist who is now working on extraction of programs from proofs, Harold Edwards, specialist of the work of Kronecker, and Fred Richman, the specialist of constructive algebra. A sub-theme was on formalization of mathematics, especially on the flyspec project, lead by Thomas C. Hales, and we were fortunate that most people working on this, in particular, besides Hales himself, Jeremy Avigad and Robert M. Solovay were present at the workshop.

Once again, we would like to thank the team of Schloss Dagsthul. The exceptional working condition we enjoyed there played an important part in the success of this meeting.

Summary of the meeting

extraction of programs from proofs

H. Schwichtenberg explained modified realizability which provides a logically sound way to extract programs from (constructive) proofs. In practice some new features, such as uniform quantification, introduced by U. Berger, should be introduced to get reasonable programs. The talk of P. Letouzey was on the tentative extraction of a program from a proof of the "fundamental theorem of algebra". A work that started at the workshop was a comparison between several systems on the extraction of a normalization algorithm from Tait's proof of normalization for simply typed lambda calculus (by Letouzey in the Coq system, Schwichtenberg in the minlog system, and Berghofer in the Isabelle system).

computational content from ineffective proofs

This is a related theme. J. Avigad presented how to use ideas from non standard analysis to analyze a measure theoretic theorem of Steinhaus (if A and

B are sets of reals with positive Lebesgue measure, then the sum set A + B includes an interval). There were several talks connected to the general program of U. Kohlenbach of extracting computation information (and even new proofs) by a combination of Dialectica interpretation and Howard's monotone functionals. It is interesting to compare this approach to modified realizability as presented by H. Schwichtenberg and P. Oliva presented a survey of different form of functional interpretation in an elegant parametrised form. L. Leustean gave concrete applications of Kohlenbach's method in analysis. P. Gerhardy presented a generalization of the majoration relation (used in the definition of monotone functionals) motivated by concrete examples in analysis.

Flyspec

The goal of the Flyspec project is to formalize completely, using interactive proof systems, the proof by T. Hales of the Kepler conjecture. This is a large enterprise. T. Hales himself presented a formalized proof of Jordan curve theorem, done in the system HOL light. T. Nipkow and S. Obua presented some parts of the verification for the Kepler conjecture in the system Isabelle. It is interesting that S. Obua found convenient for this to use the concept of lattice-ordered rings. R. Zumkeller's presentation was about inequalities between reals in the Coq system, also motivated by the verification of T. Hales' proof of the Kepler conjecture.

Computer algebra

P. Paule and C. Schneider presented some elegant applications of the use of computer algebra systems in proving mathematical theorems. There is a "feedback process": experiments on mathematical problems suggest, not only possible proofs, but also new conjectures.

V. Weispfenning described algorithms for the study of univariate p-adic constraints, implemented in the system REDUCE. A. Mahboubi's talk was about Cylindrical Algebraic Decomposition, and its possible representation in the proof system system Coq.

The talks by J. Rubio, D. Duval, C. Dominguez and F. Sergeraert were more general in nature and about the problem of representation of algorithms in computer algebra and their correctness proofs. V. Prevesto showed how this is handled in the focal system.

A. Quadrat showed how problem from mathematical physics and control theory can be expressed using algebraic analysis, leading for instance in problems about testing if a given module is free or projective, and how this can then represented in computer algebra system (for instance in the Maple package OreModules).

Constructive topology

E. Palmgren talked about the problem of defining quotient in formal topology while B. Spitters talk illustrated how ideas from formal topology can served as guide for a constructive approach to measure theory.

Constructive algebra

H. Edwards gave two talks. One was a general presentation of his new book on constructive mathematics. He explained the problem of constructive existence of the splitting fields, and how this was solved through the work of Galois and Kronecker. It is very interesting to compare this solution to the solution using dynamical methods. His second talk was about a particular chapter of this book, which is an analysis of the notion of genus as it appears in Abel's paper. He insisted on the fact that this approach was purely algebraic, without any mention of complex numbers. There also it would be very interesting to connect this to more recent approaches on constructive algebra.

F. Richman's talk was about a general technique to prove independence result in constructive algebra, for instance to build a discrete ring with a finitely generated ideal for which one cannot decide if it contains the unit or not. (It can be noted that the same technique is used when showing that the axiom of choice implies the law of excluded middle).

H. Perdry, P. Schuster, Th. Coquand presented concrete results in constructive algebra. H. Lombardi gave a presentation of the constructive dynamic theory of Dedekind rings. M.F. Roy gave an elementary algebraic proof providing an explicit sum of square for the subdiscrimants of a symmetric matrix. I. Yengui gave an elegant application of dynamical methods for solving the "Kronecker's problem": a decision procedure for the ideal membership problem for $\mathbb{Z}[X_1, \ldots, X_n]$ giving an example of "dynamical" or "comprehensive" computation of Gröbner's basis.