05021 Abstracts Collection
Mathematics, Algorithms, Proofs
— Dagstuhl Seminar —

Thierry Coquand[1], Henri Lombardi[2] and Marie-Françoise Roy[3]

[1] Chalmers - Göteborg, SE
coquand@cs.chalmers.se
[2] Université de Franche-Comté, FR
henri.lombardi@univ-fcomte.fr
[3] Université de Rennes, FR
Marie-Francoise.Roy@univ-rennes1.fr

Abstract. From 09.01.05 to 14.01.05, the Dagstuhl Seminar 05021 "Mathematics, Algorithms, Proofs" was held in the International Conference and Research Center (IBFI), Schloss Dagstuhl. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

Keywords. Constructive mathematics, computer algebra, proof systems

05021 Executive Summary – Mathematics, Algorithms, Proofs

Thierry Coquand (Chalmers - Göteborg, S)

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.

Keywords: Constructive mathematics, computer algebra, proof systems

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/438

Translating nonstandard proofs to constructive ones

Jeremy Avigad (CMU - Pittsburgh, USA)

I will describe a mechanical translation which takes proofs using nonstandard arithmetic and analysis to standard (and even constructive) ones. By way of illustration, I will explain how the translation is helpful in finding the "constructive content" of a theorem due to Steinhaus: if A and B are sets of reals with positive Lebesgue measure, then the sumset A + B includes an interval.

Strong normalization for lambda calculi with recursion

Ulrich Berger (University of Wales - Swansea, GB)

We consider the untyped lambda calculus with constructors and recursively defined constants. We show that if a term does not denote the bottom element in a suitable strict domain-theoretic model and satisfies some additional condition, then it is strongly normalizing.

We transfer this result to extensions of Goedel's system T and system F extended by various forms of bar recursion for which strong normalization was hitherto unknown.

Heitmann dimension

Thierry Coquand (Chalmers - Göteborg, S)

In 1958, Serre presented a purely algebraic theorem, directly motived by geometrical considerations (given a vector fiber bundle, if the dimension of the fibers are $>$ dimension of the base, then there is a non vanishing question). This can be formulated concretely as a general theorem about idempotent matrices over a commutative ring.

The proof needed the ring to be Noetherian and it was natural to look for a nonNoetherian generalisation.

A breakthrough was obtained by a paper of Heitmann in 1984, but the generalisation of Serre's theorem was still missing. We present such a generalisation, with a constructive and elementary proof, that was obtained by giving a purely first-order formulation of Serre's theorem.

Joint work of: Lombardi, Henri; Quitté, Claude

Towards Diagrammatic Specifications of Symbolic Computation Systems

César Domínguez (Universidad de la Rioja, E)

The aim of this work is to present an ongoing project to formalize, in the framework of diagrammatic logic (due to Dominique Duval and Christian Lair) some data structures appearing in Sergeraert's symbolic computation systems Kenzo and EAT. More precisely, we intend to translate into the diagrammatic setting a previous work based on standard algebraic specification techniques. In particular, we give hints on the reason why an important construction (called imp construction) in the specification of the systems can be understood as a freely generating functor between suitable categories of diagrammatic realizations. Even if very partial, these positive results seem to indicate that this new kind of specification is promising in the field of symbolic computation.

Keywords: Specification, symbolic computation, sketches, diagrammatic logic

Joint work of: Dominguez, César; Duval, Domonique; Lamban, Laureano; Rubio, Julio

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/292

Diagrammatic logic and effects: the example of exceptions

Dominique Duval (Université de Grenoble, F)

For dealing with computational effects in computer science, it may be helpful to use several logics: typically, a logic with implicit effects for the language, and a more classical logic for the user.

Hence, the study of computational effects should take place in a framework where distinct logics can be related. In this paper, such a framework is presented: it is a category, called the category of propagators. Each propagator defines a kind of logic, called a diagrammatic logic, which is endowed with a deduction system and a sound notion of models. Morphisms of propagators provide the required relationships between diagrammatic logics. The category of propagators has been introduced by Duval and Lair in 2002, it is based on the notion of sketches, which is due to Ehresmann in the 1960's. Then, the paper outlines how Duval and Reynaud in 2004 used the category of propagators for dealing with the computational effect of raising and handling exceptions. Another application of diagrammatic logic is presented by Dominguez et al. in the same conference

Keywords: Specifications, Semantics, Exceptions, Sketches, Diagrammatic Logic, Extensive Categories, Monads

Joint work of: Duval, Dominique; Reynaud, Jean-Claude

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/293

Introduction to My Book "Essays in Constructive Mathematics"

Harold M. Edwards (Courant Institute - New York, USA)

The talk will describe the overall approach and the major topics of the book, recently published by Springer.

Keywords: Constructive Mathematics, Galois Theory, Genus of a Curve

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/280

Abel and the Concept of the Genus of a Curve

Harold M. Edwards (Courant Institute - New York, USA)

This talk is about the treatement of the Genus of a Curve by Abel, following the book "Essays in Constructive Mathematics".

Keywords: Constructive Mathematics

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/277

Generalized metatheorems on the extractability of uniform bounds in functional analysis

Philipp Gerhardy (TU Darmstadt, D)

Recently U.Kohlenbach proved general metatheorems for the extraction of (uniform) bounds from classical proofs in functional analysis. The proof was based on a combination of Gödel's functional interpretation and Bezem's strong majorization relation. We present a generalization of the majorization relation which allows to generalize Kohlenbach's metatheorems significantly. Finally, we will discuss some examples which are now covered by the new metatheorems.

This is joint work with Ulrich Kohlenbach.

Keywords: Proof mining, majorization

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/431

Introduction to the Flyspeck Project

Thomas C. Hales (University of Pittsburgh, USA)

This article gives an introduction to a long-term project called Flyspeck, whose purpose is to give a formal verification of the Kepler Conjecture. The Kepler Conjecture asserts that the density of a packing of equal radius balls in three dimensions cannot exceed *pi/sqrt*18. The original proof of the Kepler Conjecture, from 1998, relies extensively on computer calculations. Because the proof relies on relatively few external results, it is a natural choice for a formalization effort.

Keywords: Certified proofs, Kepler conjecture

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/432

Agda and Computer Algebra

Daisuke Ikegami (Research Center for Verification & Semantics, J)

Agda is one of proof systems which has been developped by Chalmers university. Currently CVS laboratory of AIST Japan also develops Agda in cooperation with Chalmers.

In this talk I will introduce a plug-in interface to connect between Agda and Computer Algebra System. A short demonstration about Euler phi function of natural numbers will be given, for discussing the performance checking the definition with Agda vs computing with computer algebra systems.

This research was supported in part by Japan Science and Technology Agency, CREST projects.

Keywords: Agda, Computer Algebra, plug-in interface, Proof System

Executing Extracted Programs

Pierre Letouzey (Universität München, D)

It is a well-known fact that algorithms are often hidden inside mathematical proofs. If these proofs are formalized inside a proof assistant, then a mechanism called extraction can generate the corresponding programs automatically. In previous work, it has been explained how a program has been (with difficulty) produced from a formalization of the Fundamental Theorem of Algebra inside the Coq proof assistant. This program theoretically allows one to compute approximations of polynomial roots. But there is currently quite a gap between theory and practice. In this sequel work, we focus on studying the complexity of this program, and tried to analyze the reasons of its inefficiency by looking at selected sub-problems, like computation of series giving values of Euler constant e or $\sqrt{2}$.

Joint work of: Letouzey, Pierre; Cruz-Filipe, Luís

Approximate fixed points of nonexpansive functions in product spaces

Laurenţiu Leuştean (TU Darmstadt, D)

In this talk, we present another case study in the general program of proof mining in fixed point theory. Thus, we generalize results obtained by W. Kirk in the theory of approximated fixed points of nonexpansive mappings in product spaces.

Keywords: Proof mining, fixed point theory, approximated fixed points, nonexpansive functions, product spaces

Joint work of: Kohlenbach, Ulrich; Leuştean, Laurenţiu

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/433

A constructive view of Dedekind domains

Henri Lombardi (Université de Franche-Comté, F)

We present a basic constructive theory for Prüfer rings and Dedekind rings.

Due to the lack of general factorisation algorithms, in order to deal with integral extensions, we allow zero-divisors.

Similarly, our general setting for Dedekind rings does not include complete factorisation of invertible ideals.

We use partial coprime factorisation bases for finite families of invertible ideals, since they always do exist constructively (in the noetherian case).

Many classical results are obtained in the weaker settings of Prüfer coherent rings (= semihereditary rings) or of dimension one Prüfer coherent rings.

Keywords: Dedekind domains, Arithmetical rings, Prüfer rings, Coprime bases, Partial factorisation, Constructive algebra

Joint work of: Ducos, Lionel; Lombardi, Henri; Quitté, Claude; Salou, Maimouna

Programming and certifying a CAD algorithm in the Coq system

Assia Mahboubi (INRIA - Sophia Antipolis, F)

A. Tarski has shown in 1948 that one can perform quantifier elimination in the theory of real closed fields. The introduction of the Cylindrical Algebraic Decomposition (CAD) method has later allowed to design rather feasible algorithms. Our aim is to program a reflectional decision procedure for the Coq system, using the CAD, to decide whether a (possibly multivariate) system of polynomial inequalities with rational coefficients has a solution or not. We have therefore implemented various computer algebra tools like gcd computations, subresultant polynomial or Bernstein polynomials.

Keywords: Computer algebra, Bernstein polynomials, subresultants, CAD, Coq, certification

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/276

Towards a Verified Enumeration of All Tame Plane Graphs

Tobias Nipkow (TU München, D)

In his proof of the Kepler conjecture, Thomas Hales introduced the notion of tame graphs and provided a Java program for enumerating all tame plane graphs. We have translated his Java program into an executable function in HOL ("the generator"), have formalized the notions of tameness and planarity in HOL, and have partially proved that the generator returns all tame plane graphs. Running the generator in ML has shows that the list of plane tame graphs ("the archive") that Thomas Hales also provides is complete. Once we have finished the completeness proof for the generator.

In addition we checked the redundancy of the archive by formalising an executable notion of isomorphism between plane graphs, and checking if the archive contains only graphs produced by the generator. It turned out that 2257 of the 5128 graphs in the archive are either not tame or isomorphic to another graph in the archive.

Joint work of: Nipkow, Tobias; Bauer, Gertrud

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/434

Proving Bounds for Real Linear Programs in Isabelle/HOL

Steven Obua (TU München, D)

Linear programming is a basic mathematical technique for optimizing a linear function on a domain that is constrained by linear inequalities.

We restrict ourselves to linear programs on bounded domains that involve only real variables. In the context of theorem proving, this restriction makes it possible for any given linear program to obtain certificates from external linear programming tools that help to prove arbitrarily precise bounds for the given linear program. To this end, an explicit formalization of matrices in Isabelle/HOL is presented, and how the concept of lattice-ordered rings allows for a smooth integration of matrices with the axiomatic type classes of Isabelle.

As our work is a contribution to the Flyspeck project, we demonstrate that via reflection and with the above techniques it is now possible to prove bounds for the linear programs arising in the proof of the Kepler conjecture sufficiently fast.

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/435

Unifying Functional Interpretations

Paulo Oliva (Queen Mary College - London, GB)

The purpose of this article is to present a parametrised functional interpretation. Depending on the choice of the two parameters one obtains well-known functional interpretations, among others Gödel's Dialectica interpretation, Diller-Nahm's variant of the Dialectica interpretation, Kreisel's modified realizability, Kohlenbach's monotone interpretations and Stein's family of functional interpretations. We show that all these interpretations only differ on two basic choices, which are captured by the parameters, namely the choices of (1) "how much" of the counter-examples for A becomes witnesses for the negation of A, and of (2) "how much" information about the witnesses of A one is interested in.

Keywords: Functional interpretation, modified realizability, Dialectica interpretation, intuitionistic logic

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/291

Coequalisers of formal topology

Erik Palmgren (Uppsala University, S)

We give a predicative construction of quotients of formal topologies. Along with earlier results on the match up between of continuous functions on real numbers (in the sense of Bishop's constructive mathematics) and approximable mappings on the formal space of reals, we argue that formal topology gives an adequate foundation for constructive algebraic topology, also in the predicative sense. Predicativity is of essence when formalising the subject in logical frameworks based on Martin-Löf type theories.

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/436

Special Functions and Computer Algebra

Peter Paule (University of Linz, A)

Along selected examples from special functions (i.e., identities involving integrals and sums) the role of recently developed computer algebra algorithms in the process of mathematical discovery and proving is illustrated.

Henselian local rings

Hervé Perdry (Università di Pisa, I)

I shall outline an elementary and effective construction of the Henselization of a local ring (which could be implemented in some computer algebra systems) and an effective proof of several classical results about Henselian local rings.

Keywords: Local rings, henselian local rings

Joint work of: Lombardi, Henri; Alonso, M.E.

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/437

Certified mathematical hierarchies: the FoCal system

Virgile Prevosto (MPI für Informatik, D)

The focal language (formerly Foc) allows a programmer to incrementally build mathematical structures and to formally prove their correctness. focal encourages a development process by refinement, deriving step-by-step implementations from specifications. This refinement process is realized using an inheritance mechanism on structures which can mix primitive operations, axioms, algorithms and proofs. Inheritance from existing structures allows to reuse their components under some conditions, which are statically checked by the compiler.

In this talk, we first present the main constructions of the language. Then we show a shallow embedding of these constructions in the Coq proof assistant, which is used to check the proofs made in Focal. Such a proof can be either an hand-written Coq script, made in an environment set up by the Focal compiler, or a Coq term given the zenon theorem prover, which is partly developped within Focal. Last, we present a formalization of focal structures and show that the Coq embedding is conform to this model.

Keywords: Specifications, proofs, inheritance, refinement, types, Focal, Coq, computer algebra, mathematics

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/274

An introduction to constructive algebraic analysis

Alban Quadrat (INRIA - Sophia Antipolis, F)

Algebraic analysis has been developed in the middle of the sixties by B. Malgrange, I. N. Bernstein, M. Kashiwara, V. P. Palamodov [1, 2, 5, 6] in order to study general systems of linear partial differential equations with constant or variables coefficients (e.g., polynomial, rational coefficients). The purpose of this talk is to give a short introduction to some constructive algorithms of algebraic analysis [4, 8], discuss an implementation of those algorithms in the Maple package OreModules [3] and show some of their applications in mathematical physics and control theory [4, 7, 8, 9, 10].

References:

[1] J. E. Bjork, Rings of Differential Operators, North Holland, 1979.
[2] A. Borel et al., Algebraic D-Modules, Perspectives in Mathematics, Academic Press, 1987.
[3] F. Chyzak, A. Quadrat, D. Robertz, OreModules project, http://wwwb.math.rwth-aachen.de/OreModules/, 2003.
[4] F. Chyzak, A. Quadrat, D. Robertz, Effective algorithms for parametrizing linear control systems over Ore algebras, INRIA report 5181, available at http://www.inria.fr/rrrt/index.fr.html, submitted for publication, 2004.
[5] M. Kashiwara, Algebraic Study of Systems of Partial Differential Equations, Mťemoires de la Sociťetťe Mathťematiques de France 63, 1995.
[6] V. P. Palamodov, Linear Differential Operators with Constant Coefficients, Grundlehren der mathematischen Wissenschaften 168, Springer-Verlag, 1970.
[7] J.-F. Pommaret, A. Quadrat, Algebraic analysis of linear multidimensional control systems, IMA Jounal of Control and Information, 16 (1999), 275-297.
[8] A. Quadrat, An introduction to algebraic theory of linear systems of partial differential equations, submitted for publication.
[9] J. Wood, Modules and behaviours in nD systems theory, Multidimens. Systems Signal Process., 11 (2000), 11-48.
[10] E. Zerz, Topics in Multidimensional Linear Systems Theory, Lecture Notes in Control and Information Sciences, Springer, 2000.

Keywords: Linear systems of partial differential equations, over/underdetermined systems, constructive algorithms, non-commutative Gröbner bases, module theory, homological algebra, mathematical physics, control theory

Enabling conditions for interpolated rings

Fred Richman (Florida Atlantic University, USA)

If A is a subring of a ring B, then an interpolated ring is the union of A and b in B : P for some proposition P. These interpolated rings come up frequently in the construction of Brouwerian examples. We study conditions on the inclusion of A in B that guarantee, for some property of rings, that if A and B both have that property, then so does any interpolated ring. Classically, no condition is necessary because each interpolated ring is either A or B. We also would like such a condition to be necessary in the sense that if it fails, and every interpolated ring has the property, then some omniscience principle holds.

Keywords: Brouwerian example, interpolated ring, intuitionistic algebra

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/279

Subdiscriminant of symmetric matrices are sums of squares

Marie-Françoise Roy (Université de Rennes, F)

We present a very elementary algebraic proof providing an explicit sum of squares.

This result generalizes a result on discriminants of symmetric matrices due to Ilyushechkin and proved also by P. Lax.

Keywords: Real algebra, sums of squares, subdiscriminants

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/347

Constructive Proofs or Constructive Statements?

Julio Rubio-Garcia (Universidad de la Rioja, E)

A question raised at previous MAP meetings is the following. Is Sergeraert's "Constructive Algebraic Topology" (CAT, in short) really constructive (in the strict logical sense of the word "constructive")? We have not an answer to that question, but we are interested in the following: could have a positive (or negative) answer to the previous question an influence in the problem of proving the correctness of CAT programs (as Kenzo)?

Studying this problem, we have observed that, in fact, many CAT programs can be extracted from the statements (that is, from the specification of certain objects and constructions), without needing an extraction from proofs. This

remark shows that the logic used in the proofs is uncoupled with respect to the correctness of programs. Thus, the first question posed could be quite irrelevant from the practical point of view. These rather speculative ideas will be illustrated by means of some elementary examples, where the Isabelle code extraction tool can be successfully applied.

Keywords: Program extraction, symbolic computation, constructive logic

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/289

Some Notes On "When is 0.999... equal to 1?"

Carsten Schneider (University of Linz, A)

In joint work Robin Pemantle and I (2004) consider a doubly infinite sum which is not equal to 1, as first suspected, but evaluates to a sum of products of values of the zeta function. Subsequently, I report on this project.

Keywords: Symbolic summation, computer algebra, proofs, harmonic numbers, zeta-relations

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/275

A nilregular element property

Peter Schuster (Universität München, D)

An element or an ideal of a commutative ring is nilregular if and only if it is regular modulo the nilradical. We prove that if the ring is Noetherian, then every nilregular ideal contains a nilregular element. In constructive mathematics, this proof can then be seen as an algorithm to produce nilregular elements of nilregular ideals whenever the ring is coherent, Noetherian, and discrete. As an application, we give a constructive proof of the Eisenbud–Evans–Storch theorem that every algebraic set in n–dimensional affine space is the intersection of n hypersurfaces.

The input of the algorithm is an arbitrary finite list of polynomials, which need not arrive in a special form such as a Gröbner basis.

We dispense with prime ideals when defining concepts or carrying out proofs.

Keywords: Lists of generators, polynomial ideals, Krull dimension, Zariski topology, commutative Noetherian rings, constructive algebra

Joint work of: Coquand, Thierry; Lombardi, Henri; Schuster, Peter

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/278

See also: Arch. Math. (Basel) 85 (2005) 49-54

Program extraction from constructive proofs

Helmut Schwichtenberg (Universität München, D)

We first survey the general theory, that is (modified) realizability. Then the emphasis will be on general principles and concepts to be followed in the formalization of interesting pieces of constructive mathematics, in order to obtain efficient and perspicious extracted programs. This will be exemplified in some case studies: the intermediate value theorem in constructive analysis, and the proof of strong normalization of typed lambda terms by means of strong computability predicates.

Keywords: Constructive analysis, program extraction

OOP, Structured Programming and Program Proofs.

Francis Sergeraert (Université de Grenoble, F)

Standard program proofs assume a general programming framework roughly described as "Structured Programming". Powerful advanced methods in Object Oriented Programming as they are now available for example under MOP (Meta-Object-Protocol) frequently lead to complex programs with sophisticated implicit gotos. A didactical example is detailed to explain the nature of the problem. Determining a program proof strategy in such a situation is an interesting subject.

Keywords: OOP, Structured Programming, Program Proof, Qualified methods, Initialization

Observational Integration Theory

Bas Spitters (Radboud University of Nijmegen, NL)

In this talk I will present a choice-free and point-free development of parts of Bishop's integration theory, culiminating in an easy algebraic proof of the spectral theorem. This proof is based on Coquand's constructive version of the Stone representation theorem combined with some elementary theory of f-rings.

Constructive algebraic integration theory without choice

Bas Spitters (Radboud University of Nijmegen, NL)

We present a constructive algebraic integration theory. The theory is constructive in the sense of Bishop, however we avoid the axiom of countable, or dependent, choice. Thus our results can be interpreted in any topos. Since we avoid impredicative methods the results may also be interpreted in Martin-Löf type theory or in a predicative topos in the sense of Moerdijk and Palmgren.

We outline how to develop most of Bishop's theorems on integration theory that do not mention points explicitly. Coquand's constructive version of the Stone representation theorem is an important tool in this process. It is also used to give a new proof of Bishop's spectral theorem.

Keywords: Algebraic integration theory, spectral theorem, choiceless constructive mathematics, pointfree topology

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/290

Solving univariate p-adic constraints

Volker Weispfenning (Universität Passau, D)

We describe practical algorithms for the study of univariate p-adic constraints. In analogy with univariate real constraints, we formalize univariate p-adic constraints as boolean combinations of univariate polynomial equations and order comparisons between p-adic values of univariate polynomials.

Our method combines techniques of Presburger arithmetic for integer p-adic values with a detailed analysis of the combined range of p-adic values of a list of univariate polynomials with rational coefficients and p-adic arguments.

We describe an algorithmic test for the solvability of such constraints in the field Q_p of p-adic numbers. If this test has a positive outcome, we also provide a sample solution of the constraint, either as a rational number or as a rational approximation of a uniquely determined algebraic p-adic number.

An implementation of the algorithms by the first author is under way based on the REDLOG-package of REDUCE. First results obtained with this implementation are displayed.

Keywords: Constraints, p-adic, quantifier elimination, decision procedure

Joint work of: Weispfenning, Volker; Sturm, Thomas

A dynamical solution to Kronecker's problem

Ihsen Yengui (Faculté des Sciences - Sfax, TN)

In my talk, I will present a new decision procedure for the ideal membership problem for polynomial rings over principal domains using discrete valuation domains. As a particular case, I solve a fundamental algorithmic question in the theory of multivariate polynomials over the integers called "Kronecker's problem", that is the problem of finding a decision procedure for the ideal membership problem for $\mathbb{Z}[X_1, \ldots, X_n]$. The techniques utilized are easily generalizable to Dedekind domains. In order to avoid the expensive complete factorization in the basic principal ring, I will introduce the notion of "dynamical Gröbner bases" of polynomial ideals over a principal domain. As application, I give an alternative dynamical solution to "Kronecker's problem".

Keywords: Kronecker's problem, Grobner bases

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/288

Verifying inequalities over real numbers in Coq

Roland Zumkeller (Ecole Polytechnique - Palaiseau, F)

The proof of the Kepler conjecture given by Thomas C. Hales in 1998 makes intensive use of computer calculations. In particular, it relies on the correctness of many inequalities over real numbers. For this purpose a formalization of interval arithmetic with some refinements, such as branch-and-bound and monotonicity checks, is presented. As a result we get a (reflectional) Coq tactic for real inequalities and its correctness proof.