The Abdus Salam
International Centre for Theoretical Physics

Automated theorem proving in Simplicial Topology with ACL2

Mirian Andrés
Universidad de la Rioja
Departamento de Matematicas y Computacion
La Rioja, Spain

Abstract:
The talk presents an approach to formally analyze concepts and algorithms in the mathematical domain of Simplicial Topology. Our aim is twofold. Firstly, to sketchs a methodology for using ACL2 to increase the reliability of a previously existing symbolic computation system for Simplicial Topology, written in Common Lisp. Secondly, to show by means of an elementary example, that it can be feasible, and even natural, to undertake that formalization in ACL2, since most of the theorems in Simplicial Topology can be seen as theorems about list manipulation. It is also worth pointing out how this example can be also proved reusing some previously proved results about abstract reduction systems.

The Abdus Salam
International Centre for Theoretical Physics

Efficient computation with Dedekind reals
(joint work with Paul Taylor)

Andrej Bauer
FMF
Ljubljana, Slovenia

Abstract:
Cauchy's construction of reals represent real numbers as sequences of rational approximations. Most implementations of exact real arithmetic follow this idea and represent reals as streams of digits, or sequences of nested intervals.

We present a novel way of computing with exact real numbers which is based on the construction of reals as Dedekind cuts in Abstract Stone Duality. Reals are described by their lower and upper cuts rather than as limits of sequences, and properties of reals are expressed as logical formulae which determine open sets. We have developed a prototype language, Marshall, which has a distinct flavor of logic programming. Nevertheless, Marshall computes with real numbers robustly and efficiently.

The Abdus Salam
International Centre for Theoretical Physics

A coinductive approach to digital computation

Ulrich Berger
Department of Computer Science
University of Wales Swansea
Singleton Park
Swansea SA2 8PP
UK

Abstract:
We study digit systems and their coinductively defined morphisms as an abstract approach to digital computation. A digit system is a set X together with a set D of functions, from X to X. The elements of D are called digits. A standard example of a digit system is the compact real interval I = [-1,1] together with the functions av_i : I -> I (i = -1,0,1) defined by av_i(x) = (x+i)/2. This digit system corresponds to the well-known binary signed digit representation of real numbers in [-1,1] which has been extensively studied in exact real number computation, type theory and domain theory.

Our approach contains two novelties:

1. We define coinductively a set of morphisms between digit systems which, in the standard cases, coincides with the set of uniformly continuous functions.

2. We use the proof-theoretic technique of program extraction to automatically synthesise from constructive proofs lazy algorithms for these morphisms.

We show how constructive analysis and corresponding certified algorithms can be developed in this approach.

Structures similar to digit systems are known as iterated function systems in the theory of dynamical systems and fractals. Since our theory has different goals we chose a different name.

The Abdus Salam
International Centre for Theoretical Physics

Local structure of the quotient morphism of a G_a-action on a factorial variety

M'hammed El Kahoui
Université Cadi Ayyad
Faculté des Sciences - Semlalia
Marrakech, Morocco

Abstract:
"Let K be a commutative field of characteristic zero and A be a K-UFD endowed with an irreducible locally nilpotent K-derivation X. We describe in this talk the structure of the pair (A,X) in case the ring of constants ker(X) of X is a principal ideal domain. We show in particular that X may be built out of a partial derivative by using a sequence of affine modifications. As an application, we study the local structure of the morphism \pi_{X}:Spec A\longrightarrow Spec(ker(X))} induced by the inclusion ker(X)\subset A above the height one components of the plinth ideal of X."

The Abdus Salam
International Centre for Theoretical Physics

On sign conditions over real multivariate polynomials

Gabriela Jeronimo
Universidad de Buenos Aires
Departamento de Matematicas
Buenos Aires, Argentina

Abstract: We will present a probabilistic algorithm to find a finite set of points intersecting the closure of each connected component of the realization of every sign condition over a family of real polynomials defining regular hypersurfaces that intersect transversally. We will also show how this set enables the determination of all feasible sign conditions over the given polynomials.

Finally, we will describe extensions of our results to the bivariate case and to sets defined by equalities and non-strict inequalities over arbitrary real multivariate polynomials.

The Abdus Salam
International Centre for Theoretical Physics

Walking in the Quarter Plane

Manuel Kauers
Johannes Kepler University
Institut of Computational Mathematics
Linz, Austria

Abstract: We consider some combinatorial questions about the number of certain lattice walks in the plane that are restricted to the first quadrant. We will show how a long-standing open conjecture of Ira Gessel about these walks was recently proven with computer algebra, in a joint effort together with Doron Zeilberger and Christoph Koutschan. We will also report on large-scale computations done together with Alin Bostan, which indicate that a much stronger assertion than Gessel's original conjecture might be true.

The Abdus Salam
International Centre for Theoretical Physics

Proof Interpretations, "Hard Analysis" and Ergodic Theory

Ulrich Kohlenbach
Technische Hochschule Darmstadt
Fachbereich Mathematik
Darmstadt, Germany

Abstract: Building upon pioneering ideas of G. Kreisel, going back to the 50's, a new applied form of proof theory emerged during the last 20 year. Here the emphasis is on applications of so-called proof interpretations to concrete mathematical proofs with the aim of extracting effective bounds as well as new uniformity results from prima facie ineffective proofs.
This has led to new results in number theory, approximation theory, nonlinear analysis, geodesic geometry and ergodic theory as well as the development of logical metatheorems that explain these results as instances of general logical phenomena. Specialized to the examples discussed in T. Tao's recent essay "Soft analysis, hard analysis, and the finite convergence principle" the logical machinery yields very much the type of quantitative finitary versions of analytical theorems as considered by Tao. We will argue that such logical methods based on appropriate functional interpretations provide a systematic approach to Tao's program of "hard analysis".

We will also give a recent application (joint work with L. Leustean) of proof mining to ergodic theory.

The Abdus Salam
International Centre for Theoretical Physics

Constructive commutative algebra and families of algebraic identities

Henri Lombardi
Université de Franche-Comté
UMR-CNRS 6623
Besançon, France
Henri.Lombardi@univ-fcomte.fr
page web http://hlombardi.free.fr/

Abstract:

We compare classical constructive algebra, à la Gauss and Kronecker, with some recent constructive decipherings of abstract existence theorems in modern commutative algebra. We find many similarities. This is probably due to the fact that "en dernière analyse", many abstract existence theorems assert the existence of special kinds of families of algebraic identities.

The Abdus Salam
International Centre for Theoretical Physics

Fast computation of a rational point of a variety over a finite field

Guillermo Matera
Universidad Nacional de General Sarmiento
Instituto de Desarrollo Humano
Buenos Aires, Argentina

This talk will be concerned with the computation of a rational point in an algebraic variety defined over a finite field. We shall comment on estimates on the number of rational points. Then we shall present algorithms for computing a rational point of an absolutely irreducible variety defined over a finite field, and extensions to more general situations.

The Abdus Salam
International Centre for Theoretical Physics

Certification of Numerical Analysis Programs

Micaela Mayero
Université Paris-Nord
LIPN-UMR-CNRS 7030
Villetaneuse, France
Micaela.Mayero@lipn.univ-paris13.fr
http://www-lipn.univ-paris13.fr/~mayero/

Abstract:

I will present you a project which aims at developing and applying methods which allow us to formally prove the soundness of programs from numerical analysis. In particular, we are interested in programs which often appear in the resolution of critical problems. Many critical programs come from numerical analysis, but few people have ever tried to apply formal methods to this kind of programs. The main reason is that real numbers (floating-point) are greatly used in numerical programs, whereas formal methods tend to handle integers, or more generally discrete structures.
I will present our experimentation on a case study. It consists in proving the correctness of a 1 dimension wave equation program (written in C). We have to check on 2 kinds of errors : method error and floating-point error. To deal with the first one, it is necessary to formalise the problem (in fact the algorithm) and the error in a proof system (in our case, we use Coq). To deal with the second one, we have to work on the C program itself and we use Caduceus. The C program has to be annoted w.r.t. the properties we want to be preserved. These annotations generate some proof obligations for several proof systems. The methods developed in this project may be applied to a large variety of problems in environments intended to produce numerical code, which is safe and correct w.r.t. its formal specification.

The Abdus Salam
International Centre for Theoretical Physics

New perspectives in algebraic systems theory

Alban Quadrat
INRIA Sophia Antipolis, APICS project
2004 Route des Lucioles,
BP 93, 06902 Sophia Antipolis Cedex, France,
Alban.Quadrat@sophia.inria.fr

Keywords. Algebraic systems theory, algebraic analysis, behavioural approach, multidimensional and infinite-dimensional linear systems, module theory, homological algebra, constructive algebra, symbolic computation.

The purpose of this talk is to present the algebraic analysis approach to mathematical systems theory developed in recent years. Algebraic analysis, pioneered by B. Malgrange and the Japanese school of M. Sato, is a mathematical theory which studies linear systems of partial differential equations based on module theory, homological algebra and sheaf theory. Ideas, techniques and results of algebraic analysis have recently been extended to different classes of linear systems such as discrete systems, differential time-delay systems, multidimensional systems or infinite-dimensional systems.
The module-theoretic approach to linear systems developed within algebraic analysis gives a unified mathematical framework (common concepts, techniques, results, algorithms and implementations) for the study of the structural properties of different classes of multidimensional linear systems and infinite-dimensional linear systems and for the study of synthesis problems (e.g., optimal control, stabilization problems). In particular, the module characterizations of the structural properties developed in this approach are intrinsic in the sense that they do not depend on particular representations of the linear system (e.g., state-space or input-output representations for 1D linear systems, Roesser or Fornasini-Marchesini models for multidimensional systems). Within algebraic analysis, the behavioural approach to linear systems can be found again and more intrinsically developed. Using powerful tools of homological algebra, we can then obtain general characterizations for the module properties corresponding to the system properties. Finally, using constructive algebra (e.g., non-commutative Gröbner or Janet bases) and symbolic computation, those homological characterizations can be made constructive over certain classes of multidimensional systems (e.g., differential time-delay systems, under-determined systems of partial differential or difference equations) and can be implemented in dedicated symbolic computation packages (e.g., OreModules, OreMorphisms, JanetOre, QuillenSuslin, Stafford).

The Abdus Salam
International Centre for Theoretical Physics

A constructive theory of classes and sets

Giuseppe Rosolini
Università di Genova
D.I.S.I.
Genova, Italy

Abstract: We compare Algebraic Set Theory of A. Joyal and I. Moerdijk [3] with the original theory of classes of Goedel and Bernays [2], adapting some previous works by C. Butz [1] and by A. Simpson[4], and discuss some of the advantages obtained with the former. In particular, we shall analyze how to build internal models.

References

[1] C. Butz, Bernays-Goedel type theory, JPAA 178 (2003) 1-23

[2] K. Goedel, The consistency of the axiom of choice and of the generalized continuum hypothesis with the axioms of set theory, Annals of maathematics studies, vol.3, 1904

[3] A. Joyal & I. Moerdijk, Algebraic Set Theory, Cambridge, 1995

[4] A. Simpson, Elementary axioms for categories of classes, 14th LiCS, 1999, 77 85

The Abdus Salam
International Centre for Theoretical Physics

Certificates of positivity on a simplex in the multivariate Bernstein basis

Marie-Françoise Roy
IRMAR
Université de Rennes 1
Campus de Beaulieu
35042 Rennes Cedex
France

Abstract:
The Bernstein polynomials of degree d on a simplex V form a basis of the polynomials of degree at most d and are visibly positive on V. A classical result by Bernstein states that if a polynomial P is positive on V it can be written as a positive combination of Bernstein polynomials of degree D on V: this is a certificate of positivity i.e. an expression for P making clear that P is positive on V. In this talk we propose to subdivide the simplex without increasing the degree, which improves the size of the certificates of positivity. In the univariate case, we obtain a certificate with size polynomial in the degree and bitsize of P.

The univariate part is a joint work with Fatima Boudaoud and Fabrizio Caruso. The multivariate part is based on the Ph D thesis of Richard Leroy and a paper with Saugata Basu and Richard Leroy (both in preparation).

The Abdus Salam
International Centre for Theoretical Physics

Spectral Schemes as Ringed Lattices
(joint work with Thierry Coquand and Henri Lombardi)

Peter Schuster
Mathematisches Institut, Universität München,
Theresienstraße 39,
80333 München, Germany;
Peter.Schuster@mathematik.uni-muenchen.de

Abstract: A partial realisation of Hilbert's programme has proved successful in commutative algebra [1]. One of the key tools is Joyal's point-free version of the Zariski spectrum as a distributive lattice. Extending this to algebraic geometry requires to reformulate Grothendieck's language of schemes with, in Hilbert's sense, finite methods. It turns out that distributive lattices even suffice for all the schemes whose underlying topological spaces are spectral. This includes pivotal cases such as the projective spectrum of a graded ring [2], and simplifies the preceding approach undertaken in formal topology [3, 4, 5].

References

[1] T. Coquand, H. Lombardi, A logical approach to abstract algebra. Math. Struct. in Comput. Science 16 (2006), 885–900.

[2] T. Coquand, H. Lombardi, P. Schuster, The projective spectrum as a distributive lattice. Cah. Topol. G´eom. Diff´er. Cat´eg. 48 (2007), 220–228.

[3] N. Gambino, P. Schuster, Spatiality for formal topologies. Math. Structures Comput. Sci. 17 (2007), 65–80.

[4] P. Schuster, Formal Zariski topology: positivity and points. Ann. Pure Appl. Logic 137 (2006), 317–359.

[5] P. Schuster, The Zariski spectrum as a formal geometry. Theoret. Comput. Sci. (2008), doi:10.1016/j.tcs.2008.06.030

The Abdus Salam
International Centre for Theoretical Physics

Helmut Schwichtenberg
University of Munich
Munich, Germany

Title: Decorating proofs

Abstract: If a formula contains existential quantifiers in strictly positive positions, then -- according to Brouwer, Heyting and Kolmogorov -- it can be viewed as a computational problem. A proof then provides a solution to this problem, and one can machine extract (via a realizability interpretation) this solution in the form of a lambda calculus term involving recursion operators, which can be seen as (and translated into) a functional program. We concentrate on the question how to control at the proof level the complexity of the extracted programs. It is shown that every proof admits an optimal decoration with uniform (U. Berger 2005) or non-computational variants of universal quantifiers and implications. (Joint work with Diana Ratiu).

The Abdus Salam
International Centre for Theoretical Physics

Effective Constructive Algebraic Topology

Francis Sergeraert
Institut Fourier
St. Martin d'Hères
France

Abstract:
Three theoretical solutions are currently available for *Constructive* Algebraic Topology. The main ideas of one of them, the *operadic* solution, have been presented in a lecture series of this Summer School.

Another solution is based over "Effective Homology". This method is quite elementary and it immediately led to concrete computer programs. Many natural computability problems in Algebraic Topology have been so easily solved, and the corresponding Kenzo program produced homology and homotopy groups so far unreachable.

The main ingredients are:
1. A *constructive* version of elementary homological algebra: every existence statement must *be* an algorithm constructing a copy of an object the existence of which is claimed.
2. Standard functional programming.

This talk is an elementary survey of this subject with some quick machine demos.

The Abdus Salam
International Centre for Theoretical Physics

A computer verified, monadic, functional implementation of the integral (joint work with Russell O'Connor)

Bas Spitters
University of Mijmegen
Foundation of Mathematics and Computer Science
Nijmegen, Netherlands

We provide a computer verified exact monadic functional implementation of the Riemann integral in type theory. Together with previous work by O'Connor, this may be seen as the beginning of the realization of Bishop's vision to use constructive mathematics, based on type theory, as a programming language for exact analysis.

The Abdus Salam
International Centre for Theoretical Physics

Merging the procedural and declarative proof styles

Freek Wiedjik
Room HG02.542
Toernooiveld 1
6525 ED Nijmegen
The Netherlands

Abstract:
Proof assistants for the formalization of mathematics currently use two very different proof styles. Declarative systems like Mizar use a textual input format that is close in style to informal mathematics. This input then is only passively checked by the system. Procedural systems like HOL and Coq use an interactive proof style where the system displays proof obligations called "goals", which the user then reduces by executing "tactics". In a procedural proof assistant the scripts that are the "proofs" just consist of sequences of those tactics, and are not readable as normal text.

In the Isabelle proof assistant both the procedural and declarative interaction styles are available in a single system. In Isabelle often the outline of the proof is written declaratively, after which the details are filled in procedurally. However, in Isabelle the two proof styles still are separate.

In this talk an interaction model will be presented in which the declarative and procedural styles have been truly merged. This leads to a proof language that is very portable. Currently existing procedural and declarative proofs both will be automatically convertible to such a system. This even holds for proofs from different proof assistants, and even for proofs from proof assistants based on different foundations.

A proof assistant implementing this merged interaction model is currently being developed on top of John Harrison's HOL Light system. This effort will be described, and the current state of the prototype will be demoed.

The Abdus Salam
International Centre for Theoretical Physics

A Characteristic Set Method for Solving Boolean Equations and Applications in Cryptanalysis of Stream Ciphers

Chung-Ming Yuan
AMSS, China Academy of Sciences
Beijing 100080, China

Abstract:

We present a characteristic set method for solving Boolean equations, which is more efficient and has better properties than the general characteristic set method.

In particular, we give a disjoint and quasi-linear zero decomposition algorithm for the zero set of a Boolean equation system and an explicit formula for the number of solutions of a Boolean equation system. We also prove that a characteristic set can be computed with a polynomial number of multiplications of Boolean polynomials in terms of the number of variables.

As experiments, we use our method to solve equations from cryptanalysis of a class of stream ciphers based on nonlinear filter generators. Extensive experiments show that the method is quite effective.

Keywords: Characteristic set method, Boolean equation, finite field F_2, cryptanalysis, stream ciphers.

The Abdus Salam
International Centre for Theoretical Physics

Solving Polynomial Systems via Symbolic-numeric Elimination Method

Lihong Zhi
Key Laboratory of Mathematics Mechanization, AMSS
Beijing 100190, China
lzhi@mmrc.iss.ac.cn

Abstract: We exploit the well-known correspondence between polynomial systems and systems of constant coefficient linear homogeneous PDE. The polynomial system is written as a PDE system which is brought to a geometric involutive form. Our numerical criterion for out-put involutive form can be checked by computing dimensions of prolonged and projected systems using singular value decomposition. For zero dimensional systems, the criterion is coordinate independent and all isolated solutions are found by applying eigenvalue-eigenvector techniques to a related eigen-problem constructed from the involutive form. For multiple root with limited accuracy, we can refine it to high accuracy by solving the matrix eigen-problem formed from the invoultive form of the truncated polynomial system.