Infinite objects in constructive mathematics

Thierry Coquand

Mar. 24, 2005

Goal of this presentation

Introduction to some recent developments in constructive algebra and abstract functional analysis

This approach can be seen as an application of some basic results in proof theory: the main one being the completeness of cut-free provability

It can be seen also as a partial realisation of Hilbert's program and uses the idea of "replacing" an infinite object by a syntactical one: a logical theory which describes this object

It has close connections with formal topology: cut-elimination can be expressed as forcing/topological model over a formal space

Content of the talks

The first part will explain the method and contains basic examples in algebra, finite combinatorics and functional analysis

The second part shows how this approach can lead to

-new concept (notion of boundary of element in a ring)

-new simple proof of classical result (*Kronecker's theorem* about algebraic subsets of $\mathbb{C}^n$)

-new mathematical results in algebra: nonNoetherian version of *Serre's splitting-off theorem* (1958) and *Forster-Swan's theorem* (1964-67), improving slightly on breakthrough results of Heitmann (1984)

Constructive mathematics

Compared to Bishop: alternative approach to infinite objects (reals, continuous functions, linear functional, . . .)

Compared to Richman/Kronecker: work without requiring a factorisation algorithm (cf. T. Mora "The Kronecker-Duval Philosophy")

but we will see that we get a notion of formal "solutions" of system of equations quite close to the one of Kronecker (notion that was forgotten in more recent development of constructive mathematics)

Basic example

Let R be a commutative ring.

Theorem: *The intersection of all prime ideals is the set of nilpotent elements*

This theorem does not hold in constructive mathematics if we undertand as prime ideal a subset of R satisfying the usual properties

There are effective non trivial rings with *no* effective prime ideals

Solution (in constructive mathematics): to replace prime ideals by their syntactical description

Classically this gives a way to eliminate the use of Zorn's lemma

Basic example

We introduce new symbols $P(r),\ r \in R$ and we write the following theory of a prime ideal

$P(0)$

$\neg P(1)$

$P(rs) \leftrightarrow [P(r) \vee P(s)]$

$[P(r) \wedge P(s)] \rightarrow P(r+s)$

To say that a belongs to the intersection of all prime ideals is to say that $P(a)$ is a propositional consequence of this theory

Basic example

This is justified classically by the *completeness theorem* of *propositional logic*

More generally, the present approach is justified classically by various completeness theorems (first-order logic, and completeness of infinitary logic)

We change the theorem to the following statement (classically equivalent): $P(a)$ *is a propositional consequence of the theory of a prime ideal if and only if* a *is nilpotent*

Proofs are finite objects (finite trees); prime ideal are infinite (ideal) objects

Basic example

Prime ideals were introduced by Kummer by analogy with chemistry

"These ideal complex numbers are comparable to hypothetical radicals that do not exist by themselves, but only in their combinations."

Kummer gave an example of an element (fluorine) that, at the time, existed only hypothetically comparable to a prime ideal (this element was isolated later)

This notion of prime ideal, as introduced by Kummer, was an important example for Hilbert's program

Hyperresolution and geometrical logic

The axioms for the theory of a prime ideal are of a special form: a conjunction of atomic formulae (facts) implies a disjunction of (conjunction of) atomical formulae. These are known as *geometrical statements*

We see the axioms as *rules* for developping the possible consequences of a finite set of atomic formulae (facts)

This is a natural generalisation of closure for Horn clauses: we explore the consequences of a given set of facts using the rules given by the theory

We may have to do branching since we have disjunction

To each branch is associated a set of facts

The Method of Tree

Here for instance we can explore the consequences of $P(r_1), \ldots, P(r_k)$

A branch may *collapse* if $\bot$ is derivable (for instance $P(r), P(1-r)$ then $P(1)$ and $\bot$ directly derivable)

An atom $P(r)$ is a consequence iff there exists a finite trees where this atom $P(r)$, or a contradiction $\bot$, appear at all leaves

Example: we can derive $\bot$ from $P(1-a), P(b^2a), P(1-b)$

The Method of Tree

That this method of proof is complete is exactly the completness of *hyperresolution*

We can use this special form of deduction to prove that $P(r)$ is a consequence of $P(r_1), \ldots, P(r_k)$ iff a power of r is in the ideal $<r_1, \ldots, r_k>$

Tree induction

This method of proofs ("logic without logic") is described in detail in

Coste Lombardi Roy
"Effective Methods in Algebra, Effective Nullstellensätze", JPAA 155 (2001)

The Method of Tree

Each proof tree of $P(r)$ from $P(r_1), \ldots, P(r_k)$ can be decorated by algebraic identities (Nullstellensatz identities)

Example: we can derive $\perp$ from $P(1-a), P(b^2a), P(1-b)$

Tree induction proceeds from the leaves to the top of the tree

$$1 = b + (1 - b)$$
$$1 = b^2 + (1 + b)(1 - b)$$
$$1 = a + (1 - a)$$
$$1 = ab^2 + b^2(1 - a) + (1 + b)(1 - b)$$

The Method of Tree

Theorem: *The facts* $P(r_1), \ldots, P(r_k)$ *are inconsistent iff* $1 \in <r_1, \ldots, r_k>$

We can read an algebraic identity $1 = u_1 r_1 + \cdots + u_k r_k$ from any tree derivation of $P(r_1) \wedge \cdots \wedge P(r_k) \rightarrow \bot$

The Method of Tree

Whiteley's slogans:

"*Nullstellensatz identities grow on trees*"

"*A logical proof guarantees an algebraic proof*"

Cf. "Invariant computations for analytic projective geometry" Journal of Symbolic Computation 11, 1991

An application

Theorem: *If* $(\Sigma a_i Y^i)(\Sigma b_j Y^j) = \Sigma c_k Y^k$ *we have the* Gauss-Joyal *equivalence*

$$(\wedge P(a_i)) \vee (\wedge P(b_j)) \leftrightarrow \wedge P(c_k)$$

This is clear if we think of $P(u)$ as meaning u is in a generic prime ideal P, simply because, since $A = R/P$ is integral, $A[Y]$ is an integral ring

Say that $\Sigma u_i Y^i$ is *primitive* iff $1 \in <u_i>$

Corollary: *The product of primitive polynomials is primitive*

We get a *constructive* proof of this theorem which is similar in structure to the classical proof which uses prime ideals

An application

In the case $n = m = 1$ we have

$c_0 = a_0b_0,\ c_1 = a_0b_1 + a_1b_0,\ c_2 = a_1b_1$

Given u_0, u_1, v_0, v_1 such that

$u_0a_0 + u_1a_1 = 1 \qquad v_0b_0 + v_1b_1 = 1$

we have to produce w_0, w_1, w_2 such that

$w_0c_0 + w_1c_1 + w_2c_2 = 1$

The method reduces the use of prime ideals to algebraic identities like

$(a_0b_1)^2 = a_0b_1c_1 - c_0c_2 \qquad (a_1b_0)^2 = a_1b_0c_1 - c_0c_2$

Other example

If K is a field, a *valuation ring* is a subring V such that for all $x \neq 0$ we have $x \in V$ or $x^{-1} \in V$

The atoms are $V(x)$, $x \in K$ and the theory is

$V(x) \wedge V(y) \to V(x+y) \wedge V(xy)$

$\to V(x) \vee V(x^{-1})$ if $x \neq 0$

Theorem: *The implication*

$$V(a_1) \wedge \cdots \wedge V(a_n) \to V(a)$$

holds iff a *is integral over* $a_1, \ldots, a_m$

Other example

Application: *If* $c_k = \Sigma_{i+j=k} a_i b_j$ *then each* $a_i b_j$ *is integral over* $c_0, \ldots, c_{n+m}$

This is known as Dedekind's Prague theorem, fundamental in his theory of ideals (and was actually proved before by Kronecker)

We reason in the field $\mathbb{Q}(a_i, b_j)$ and we show that

$V(c_0) \wedge \cdots \wedge V(c_{n+m}) \to V(a_i b_j)$

Actually we have

$[\wedge_k V(c_k)] \leftrightarrow [\wedge_{i,j} V(a_i b_j)]$

Any Proof Tree can be decorated by an algebraic identities

Other example

For $n = m = 2$ a proof certificate of $V(c_0) \wedge \cdots \wedge V(c_4) \to V(a_0 b_1)$ is

$$(a_0 b_1)^6 = p_1(a_0 b_1)^5 + p_2(a_0 b_1)^4 + p_3(a_0 b_1)^3 + p_4(a_0 b_1)^2 + p_5(a_0 b_1) + p_6$$

where

$$p_1 = 3c_1, \quad p_2 = -3c_1^2 - 2c_0c_2, \quad p_3 = c_1^3 + 4c_0c_1c_2$$
$$p_4 = -c_0^2c_1c_3 - 2c_0c_1^2c_2 - c_0^2c_2^2 + 4c_0^3c_4$$
$$p_5 = c_0^2c_1^2c_3 + c_0^2c_1c_2^2 - 4c_0^3c_1c_4$$
$$p_6 = -c_0^3c_1c_2c_3 + c_0^4c_3^2 + c_0^3c_1^2c_4$$

The Method of Tree

This method has been also investigated in finite combinatorics

Matijasevitch "The application of the methods of the theory of logical derivation to graph theory", 1972

A simple application gives an elegant proof of König's theorem: a graph cannot be two-coloured iff it contains a cycle of odd length

Finite combinatorics

We consider the theory, for i, j, k distincts in a given finite set

$R(i,j) \wedge R(j,k) \wedge R(k,i) \rightarrow$

$R(i,j) \rightarrow R(i,k) \vee R(k,j)$

We prove by Tree Induction that the facts F are contradictory iff F contains a cycle of odd length

König's theorem is a corollary of this remark: interpret $R(i,j)$ as that i and j does not have the same colour

Finite combinatorics

For the pigeon-hole theory, given two finite sets P and H

$R(p, h_1) \wedge R(p, h_2) \rightarrow \bot$

$R(p_1, h) \wedge R(p_2, h) \rightarrow \bot$

$\rightarrow \vee_{h \in H} R(p, h)$

When is $\{R(p, h) \mid (p, h) \in X\},\ X \subseteq P \times H$ a consequence of this theory?

We prove by tree induction that this holds iff X contains a rectangle $P_1 \times H_1$ with $|P| < |P_1| + |H_1|$

We retrieve in this way Rado's proof of Hall's theorem (the "Mariage Lemma")

First-order formulation

Whiteley (1971) and Scarpellini (1969) gives a first-order formulation of these results. In the first-order theory of rings, the terms are polynomials, and the only predicate is $Z(x)$. The axioms for rings are

$Z(0)$

$Z(x) \wedge Z(y) \rightarrow Z(x+y)$

$Z(x) \rightarrow Z(xy)$

This is a *direct* theory (no branching) and $Z(u)$ follows from $Z(u_1), \ldots, Z(u_k)$ iff $u \in <u_1, \ldots, u_k>$

First-order formulation

We can add the axioms

$Z(xy) \to [Z(x) \vee Z(y)]$ for *integral rings*

$Z(x) \vee \exists y.Z(1 - xy)$ for *fields*

$\exists x.Z(x^n + a_{n-1}x^{n-1} + \cdots + a_0)$ for *algebraically closed fields*

The method of tree extends to this case: one may have to introduce new parameters for the existential quantifications

First-order formulation

For all these theories $Z(u)$ follows from $Z(u_1), \ldots, Z(u_k)$ iff some power of u is in $<u_1, \ldots, u_k>$

This is proved by Tree Induction

In particular $Z(u_1), \ldots, Z(u_k)$ are incompatible iff $1 \in <u_1, \ldots, u_k>$

This is a simple proof of consistency of the theory of algebraically closed fields and of Hilbert's Nullstellensatz

Construction of the splitting field

Problem: to build the splitting field of a given polynomial

This problem is discussed in detail in the recent book of H. Edwards on constructive mathematics

It illustrates well the difference with the usual approach to constructive algebra which requires an algorithm to decide if a polynomial is irreducible or not

Construction of the splitting field

The logical analysis of the problem is that for building a splitting field of a polynomial $x^3 - ax^2 + bx - c$ over a field K we have to show the existence of a prime ideal in $K[x_1, x_2, x_3]$ containing

$$x_1 + x_2 + x_3 - a$$

$$x_1x_2 + x_2x_3 + x_3x_1 - b$$

$$x_1x_2x_3 - c$$

Construction of the splitting field

The prime ideal exists formally because the theory that describes it is *not contradictory*. We show that the ideal

$$I = <x_1 + x_2 + x_3 - a, x_1x_2 + x_2x_3 + x_3x_1 - b, x_1x_2x_3 - c>$$

is proper.

It is easy to see that $K[x_1, x_2, x_3]/I$ is of dimension 6 over K of basis $x_1^{i_1}x_2^{i_2}x_3^{i_3}$ with $i_k < k$ (decomposition algebra)

This formal version of the Nullstellensatz, in the form of logical consistency, and notion of logical consequence of a system of equations, was used in algebra by Kronecker and his followers (Drach, 1898)

Summary

By replacing infinite objects by their syntactical descriptions we can represent in constructive mathematics infinite objects in a satisfactory way

By using completeness of hyperresolution/cut-free provability we can associate nullstellensatz identities to any proof tree directly by Tree Induction

Interpretation of cut-elimination

These remarks about cut-elimination have been discovered several times:

Lewis Carroll (1890) "Symbolic Logic", Part II

Skolem (1919): for lattice theory and projective geometry

Scarpellini (1969): Gentzen cut-elimination

Whiteley (1971): Gentzen cut-elimination

Lifschitz (1980): hyperresolution (inspired by Matijasevich 1971)

S. Negri and J. van Plato (1998): axioms as new sequent rules

Infinitary logics

The same method can be used for objects that are described in a theory that uses infinitary logic

Classically, *as long as we have a completeness theorem*, the syntactical approach is equivalent to the approach with models

Infinitary logics

Example: theory of linear functional of norms ≤ 1

We introduce the axioms $X(a, q)$ for $\lambda(a) < q$

$X(a, 1)$ if $|a| < 1$

$X(a + b, p + q) \rightarrow [X(a, p) \vee X(b, q)]$

$X(a, p) \wedge X(-a, -p) \rightarrow$

$X(a, p) \rightarrow \vee_{p' < p} X(a, p')$

We can still apply the Method of Tree

Hahn-Banach

Theorem: *The formula* $X(a_1, p_1) \vee \cdots \vee X(a_k, p_k)$ *is provable iff there is* $1 = \Sigma\alpha_i$ *with* $|\Sigma\alpha_i a_i| < \Sigma\alpha_i p_i$

In particular if we can prove $X(a, p)$ for all $p > 0$ we have $a = 0$

This is a statement of Hahn-Banach theorem

One application is (geometric Hahn-Banach theorem)

Corollary: *If* $X(a, q) \to \vee_i X(a_i, q)$ *for all* $q \in \mathbb{Q}$ *then* a *is in the closed convex hull of the* a_i

Hahn-Banach

In Bishop's development of functional analysis, Hahn-Banach's theorem cannot be proved: a linear functional is presented as a function, and not as a formal object

The present formal approach avoids these problems

Infinitary logic

This formal approach, in the case of infinitary logic, has direct connections with one method used in proof theory to reduce Π^1_1-comprehension to inductive definitions

Infinitary logic

For instance the Π^1_1 statement "the intersection of all positive downward subsets of $\mathbb{Q}$ is $\{q \mid q \leq 0\}$" can be interpreted proof theoretically

If $\phi(X) = (\vee_{q>0} X(q)) \wedge \wedge_{q_1 \leq q_2} (X(q_2) \to X(q_1))$ then

$\vdash \phi(X) \to X(r)$ iff $r \leq 0$

This statement replaces the quantification over arbitrary subsets of $\mathbb{Q}$ by a statement that uses only inductive definitions

It is itself provable by Tree Induction

Interpretation of cut-elimination

There is an alternative presentation of cut-elimination which has connection with formal topology and Beth models/forcing

This alternative presentation gives a "semantical" way to prove completeness of hyperresolution and gives an algorithm to transform an arbitrary proof in an hyperresolution proof

One uses a notion of forcing/topological models, where the forcing conditions are finite set of atomic formulae (like in Grzegorczyk's interpretation of intuitionistic logic)

cf. J. Avigad "Forcing in proof theory"
Bulletin of Symbolic Logic, 2004

Interpretation of cut-elimination

We define $X \Vdash \phi$ by induction on ϕ

$X \Vdash p$ iff there is a tree derivation of p from X

$X \Vdash \phi \to \psi$ iff $X \subseteq Y$ and $Y \Vdash \phi$ imply $Y \Vdash \psi$

$X \Vdash \phi \wedge \psi$ iff $X \Vdash \phi$ and $X \Vdash \psi$

$X \Vdash \phi \vee \psi$ iff there is a tree derivation from X of leaves $X_1, \ldots, X_k$ with $X_i \Vdash \phi$ or $X_i \Vdash \psi$ for all i

Theorem: *If* $X \vdash \phi$ *then* $X \Vdash \phi$

In particular if $X \vdash p$ then there is a tree derivation of p from X

Interpretation of cut-elimination

One can look at this forcing relation as defining a topological model: the semantics of a formula ϕ is $\{X \mid X \Vdash \phi\}$

This gives the following interpretation of the present method: it may be impossible to find effectively a model for the predicate X in a standard way, but it is possible to find a topological model for X

This forcing interpretation extends to first-order and infinitary logic

Geometric logic and cut-elimination

In order to apply the method of Tree Induction/Beth model we have to work with axioms of the form

$C \to C_1 \vee \cdots \vee C_k$ or

$C \to \vee_n C_n$ or

$C \to E_1 \vee \cdots \vee E_k$

where C, C_i are finite conjunction of atoms, and E_j existential quantification of conjunction of atoms

Geometric logic and cut-elimination

What is interesting is the intuition from topology/topological models and connection with sheaf models

One aspect of works of C. Mulvey (functional analysis) and G. Wraith (Galois theory) has been precisely to reexpress classical theorems in a geometrical form. (But they did not try to analyse the direct proofs.)

Factorisation of primes

In constructive algebra, as developped by Kronecker, Richman, one insists of effective factorisation in primes

Analogy: to prove $x^2|y^2 \to x|y$ one would use decomposition in prime factors

The primes are like infinite objects, they are best described by their syntactical theories, but they exist in general only ideally

Factorisation of primes

For $x^2|y^2 \longrightarrow x|y$ we can give argument that uses only facts about gcd instead of decomposition in primes

The argument will use only a *partial* factorisation $x = ux_1$ and $y = uy_1$ with $u = gcd(x, y)$

More generally, the algorithms implicit in the arguments that we get using the present formal approach to infinite objects are computationally more reasonable than the ones we get by insisting on prime decompositions. This is the idea of "lazy computations": we don't try to compute a large object but only the relevant part

What do we gain?

For constructive mathematics, we get a more satisfactory representation of infinite objects and avoid to have to decide things like: is a given polynomial irreducible or not? (even if it is possible it may be infeasible and not relevant)

For mathematics, we get a method to express more concretely/simply properties, by Nullstellensatz identities, and to avoid strong assumptions like axiom of choice. For simple statements, we know *a priori* by the logical form of a statement that if it holds, it should hold for simple reasons

One message of Kronecker seems to have been that non only these strong assumptions are not necessary in algebra, but also that we get a *better* treatment by avoiding them