Coherent logic

Thierry Coquand

September 1, 2006

How crucial is the use of non effective methods?

Can we develop mathematics with only effective proofs??

Kronecker: in algebra the arguments should be effective "purity of methods": for instance, Abel's theorem is a theorem in algebra (no complex numbers should be involved)

Dedekind, Hilbert: even if one is interested in algorithmic/algebraic results, it can be more elegant to use non effective/analytic arguments

Later non effective arguments were thought essential especially in Analysis

How crucial is the use of non effective methods?

Bishop (1967) showed that a large part of analysis can be developped directly with only effective arguments

Richman did the same in algebra. He stresses that constructive mathematics is *mathematics* developped in *intuitionistic logic*.

A large part of mathematics can be directly developped constructively. This is an elegant way to present algorithms.

BHK interpretation

We prove in *intuitionistic logic* $\forall x.A(x) \to \exists y.B(x,y)$ This can be seen as giving an algorithm which, given an input n *satisfying* A outputs m such that $B(n,m)$ holds

The *proof* can be seen as an *algorithm*, which comes together with its correctness proof (Bishop saw each proofs in his book as *instructions* for humans to carry out some computations)

Constructive algebra should provide an elegant way of developping algorithms together with their proofs of correctness

Constructive algebra

Discrete fields are axiomatised by the two conditions

$a = 0 \vee \exists x.ax = 1$

$0 \neq 1$

So given $a \in K$ we can decide whether $a = 0$ or a has an inverse

We have then $a \neq 0 \leftrightarrow \exists x.ax = 1$

Hence we have $a = b \vee a \neq b$

Constructive algebra

The previous reasonining is done in intuitionistic logic

It has a direct algorithmic content: given a program that decides whether $a = 0$ or a has an inverse, we build a test for equality

But we never talked about algorithms, only did some mathematics using intuitionistic logic

Constructive algebra

What is a local ring? A ring R satisfying

$$(\exists y.xy = 1) \vee (\exists y.(1-x)y = 1)$$

If we read this statement via the BHK interpretation, a local ring R appears to come with a procedure which, given an element $x \in R$ tells whether x or $1-x$ is invertible and produces an inverse

Lemma: *If P is an idempotent matrix over R then P is similar to one canonical idempotent matrix I_k*

A constructive proof gives an algorithm, which using the procedure above and an idempotent matrix P, computes k and an invertible Q such that $QPQ^{-1} = I_k$

Constructive algebra

Example: what is a finitely presented module?

It is given by a finite presentation matrix

A finitely projective projective module is given by a finite idempotent matrix

Theorems about these modules can be interpreted as algorithms on these matrices

Non constructive arguments

This possibility to read a proof as an algorithm (with a proof of correctness) seems *lost* if we allow non constructive arguments

Classically, if K is a field and $P \in K[X]$ there exists $Q \in K[X]$ such that Q is irreducible and Q divides P

The classical proof does not give any algorithm for finding Q (and furthermore there is *no* such algorithm)

Problems in constructive algebra

A factorisation algorithm seems to be needed when we want to build the *splitting field* of a polynomial $f \in k[X]$ or even an extension in which f has a root

It is clear how to do it if f is irreducible: simply takes $k[X]/<f>$ but in general??

MRR contains a clever solution if one can enumerate k.

Classical mathematics use only the ideal existence of such a field but does not require the actual computation

Problems in constructive algebra

The problem of the existence of a splitting field of a polynomial is analysed in detail in the book of Edwards (see also his book on Galois theory)

In particular, he presents a construction of the splitting field in the case $k = \mathbb{Q}(X_1, \ldots, X_n)$ coming originally from Galois and points out an apparent circularity in Galois' construction

Problems in constructive algebra

Maximal ideals exist only in special case: for instance if we can enumerate R and decide if an element belongs to a finitely generated ideal

R is then said to be *strongly discrete*

This construction relies on an *arbitary enumeration* of R does not seem elegant and is probably *useless* computationaly

Problems in constructive mathematics

A similar criticism can be made of several algorithms corresponding to proofs in functional analysis in Bishop-Bridges' book

For instance the proof of the spectral theorem, and hence the corresponding algorithm, uses an arbitrary enumeration of a dense subset of a space

Problems in constructive algebra

Constructive algebra/computer algebra: systems (like MAGMA) can do computations in a splitting field of a polynomial or in an algebraic closure of a field without relying on a factorisation algorithm or an enumeration of the field!

A new approach to constructive mathematics

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

Realisation of Hilbert's program in algebra: we write the *formal theory* of the ideal object (prime ideal, linear functionals, ...) and following a classical argument, we write a proof in this theory

By cut-elimination/normalisation we know that this proof can be rewritten in a simple tree form. In practice it is often *directly* written in this form.

We show how to associate algorithmic informations (often algebraic identities called Nullstellensatz identities) to this tree, proceeding from the leaves to the root

Post systems

As an example theory of rings

$$x + y = y + x, \quad x + (y + z) = (x + y) + z, \quad x + (-x) = 0, \quad x + 0 = x$$

$$x \times (y + z) = x \times y + x \times z, \quad x \times 1 = x, \quad x \times y = y \times x$$

We add the positive diagram of a given ring

$$c_{a+b} = c_a + c_b,\ c_{ab} = c_a \times c_b, 0 = c_0,\ 1 = c_1$$

Proposition $c_{a_1} = 0, \ldots, c_{a_k} = 0 \rightarrow c_a = 0$ *iff* $a \in <a_1, \ldots, a_k>$

Coherent theories

Any coherent formula is equivalent to a conjunction of formulae of the form

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

with $E \ ::= \ C \mid \exists x.E$

One can then develop proofs in this fragment as finitely branching trees

Coherent theories

Theory of fields

$\neg(x = 0) \to \exists y.xy = 1$ is *not* coherent

$x = 0 \vee \exists y.xy = 1$ is coherent (discrete field)

integral domain $xy = 0 \to (x = 0 \vee y = 0)$

Coherent theories

We explore possible ways to map a ring R in a field $R \to K$

For this we write the axioms of discrete fields extended by the positive diagram of R

We shall see that $c_{a_1} = 0, \ldots, c_{a_k} = 0 \to \bot$ is provable in this theory iff $1 \in <a_1, \ldots, a_k>$ in the ring R

Hyperresolution and coherent logic

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

dynamical proof: a dynamical proof is a rooted tree.

A dynamical proof establishes the correctness of an *atomic* formula with reference to some given set of *atomic formulas*

Each node consists of a set of atomic formulas, representing a *state of information*.

The sets increase monotonically along the way from the root to the leaves

Every leaf of a dynamical proof contains either a contradiction or the atomic formula under investigation

The Method of Tree

That this method of proof is complete is exactly the completeness of *hyperresolution*.

It follows from cut-elimination/normalization (and negative translation) that this method of proof is complete w.r.t. first-order reasoning even using classical logic

This can also be read as a conservativity result

The Method of Tree

Here for instance we can explore the consequences of $a_1 = 0, \ldots, a_k = 0$ in the theory of non trivial integral domain over a ring R

A branch may *collapse* if $\perp$ is derivable (for instance $a = 0, a - 1 = 0$ then $1 = 0$ and $\perp$ directly derivable)

Definition: An atom $a = 0$ is a consequence iff there exists a finite tree where this atom $a = 0$, or a contradiction $\perp$, appears at all leaves and $\perp$ is a consequence iff there exists a finite tree where $\perp$ appears at all leaves

Example: we can derive $\perp$ from $1 - a = 0, b^2 a = 0, 1 - b = 0$

The Method of Tree

Each proof tree of $a = 0$ from $a_1 = 0, \ldots, a_k = 0$ can be decorated by algebraic identities (Nullstellensatz identities)

Example: we can derive $\perp$ from $1 - a = 0, b^2 a = 0, 1 - b = 0$

Tree induction proceeds from the leaves to the root 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* $a_1 = 0, \ldots, a_k = 0$ *are inconsistent iff* $1 \in <a_1, \ldots, a_k>$

We can read an algebraic identity $1 = u_1 a_1 + \cdots + u_k a_k$ from any tree derivation of $a_1 = 0 \wedge \cdots \wedge a_k = 0 \rightarrow \perp$

Theorem: $a_1 = 0, \ldots, a_k = 0 \vdash b_1 = 0 \vee \cdots \vee b_m = 0$ *iff the monoid generated by* $b_1, \ldots, b_m$ *meets the ideal generated by* $a_1, \ldots, a_k$

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

The Method of Tree

Consistency of the infinity axiom

Valuation ring

combinatorics (König's Theorem on graphs)

Consistency of the theory of splitting field and of algebraically closed fields

Consistency of the infinity axiom

A basic example is given by the theory of axioms

$$f(x) \neq a, \qquad f(x) = f(y) \to x = y, \qquad x = x, \qquad x = y \to f(x) = f(y)$$

This theory is a Post system (no branching)

This theory has no finite model, so its consistency cannot be clear

Consistency of the infinity axiom

The direct consequences of this theory are

$f^n(a) = f^n(a)$

$f^n(a) \neq f^m(a)$ if $n \neq m$.

In particular $\bot$ is not derivable.

Consistency of the infinity axiom

This is essentially the reasoning hinted by Hilbert in

"On the foundations of logic and arithmetic", 1904

"The considerations just sketched constitute the first case in which a direct proof of consistency has been succesfully carried out for axioms, whereas the method of a suitable specialization, or of the construction of examples, which is otherwise customary for such proofs-in geometry in particular- necessarily fails here."

Though simple it involves non feasible methods (cut-elimination)

An application

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

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

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

Theorem: *The implication*

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

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

An application

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 result in the theory of ideals (and was actually proved before by Kronecker)

In Bourbaki, Algèbre Commutative, Vol. 7, this appears in the exercises, as an application of the theory of valuations (non constructive proof)

An application

How to read this argument constructively??

We reason in the field $\mathbb{Q}(a_1, \ldots, a_n, b_1, \ldots, b_m)$ and we show that

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

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

$$p_1 = 3c_1, \quad p_2 = -3c_1^2 - 2c_0 c_2, \quad p_3 = c_1^3 + 4c_0 c_1 c_2$$
$$p_4 = -c_0^2 c_1 c_3 - 2c_0 c_1^2 c_2 - c_0^2 c_2^2 + 4c_0^3 c_4$$
$$p_5 = c_0^2 c_1^2 c_3 + c_0^2 c_1 c_2^2 - 4c_0^3 c_1 c_4$$
$$p_6 = -c_0^3 c_1 c_2 c_3 + c_0^4 c_3^2 + c_0^3 c_1^2 c_4$$

Finite combinatorics

The method of tree has been also investigated in finite combinatorics

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

Elegant proof of König's theorem: a graph cannot be two-coloured iff it contains a cycle of odd length

Here the points will be the two-colours on a graph

Finite combinatorics

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

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

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

Proposition: *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

First-order formulation

Given a ring R can we find a field K with a map $f : R \to K$?

One can formulate it as the problem of consistency of the following system: theory of rings with positive diagram of R and the axioms

$0 \neq 1$

$x = 0 \vee \exists y.xy = 1$

The *models* of this theory are exactly the fields K with a map $R \to K$

Method of tree

Tree induction gives the following result

Proposition: *We have* $a_1 = 0, \ldots, a_k = 0 \vdash a = 0$ *iff* a *is in the radical of the ideal generated by* $a_1, \ldots, a_k$

We get the same result if, instead of the theory of fields, we take the theory of integral domains

$xy = 0 \to x = 0 \vee y = 0$

Method of tree

We have the following algebraic interpretation: each node of the tree defines a *finite presentation* of a ring

The previous proposition can be reduced to

Lemma: *If R is a ring and $a \in R$ and $b \in R$ is nilpotent in $R/< a >$ and nilpotent in $R[x]/<ax - 1>$ then a is nilpotent in R*

$R[x]/<ax - 1>$ is also written $R[1/a]$

Method of tree

If we have two polynomials $P, Q \in k[X]$ over *a field* k we can show

$$\exists P_1, Q_1, A, B, G. \quad P = GP_1 \wedge Q = GQ_1 \wedge AP_1 + BQ_1 = 1$$

If we have two polynomials $P, Q \in R[X]$ over a ring we can build a binary tree such that

the children of a node S are $S/<u>$ and $S[1/u]$ for some $u \in S$

at each leaf S we have P_1, Q_1, A, B, G satisfying $P = GP_1 \wedge Q = GQ_1 \wedge AP_1 + BQ_1 = 1$ in $S[X]$

Application: separable polynomials and reduced rings

Classically any ring R which is *reduced* can be embedded in a product of fields

Let $P \in R[X]$ be a monic polynomial which is *separable*: there exists $A, B \in R[X]$ such that $AP + BP'$ is an invertible constant

Theorem: *The quotient ring $R[X]/<P>$ is reduced*

Concretely it means that if $Q \in R[X]$ and P divides Q^2 then P divides Q

Application: separable polynomials and reduced rings

The Theorem can be shown directly if R is a field

We take $gcd(P, Q) = G$ so that $P = GP_1,\ Q = GQ_1$ and we have A, B such that $AP_1 + BQ_1 = 1$

Then P_1 divides GQ_1^2 and hence P_1 divides G. So P_1^2 divides P and $P_1 = 1$ since P is separable

So P divides Q

Application: separable polynomials and reduced rings

In general, we can divide $Q = PC + D$ since P is monic

In the theory of field T extending the diagram of R we can show that each coefficient a of D is 0

But we know that $\vdash_T a = 0$ implies $a = 0$ *in* R since R is reduced

Hence $D = 0$ and P divides Q

(This gives yet another proof that if P is separable then its universal decomposition algebra is reduced)

Application: 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 consistency of the theory of fields extended with special symbols x_1, x_2, x_3 and axioms

$$x_1 + x_2 + x_3 = a$$

$$x_1x_2 + x_2x_3 + x_3x_1 = b$$

$$x_1x_2x_3 = c$$

Construction of the splitting field

We can show that this theory is *not contradictory*

We show

$$\begin{aligned} I &= <x_1+x_2+x_3-a, x_1x_2+x_2x_3+x_3x_1-b, x_1x_2x_3-c> \\ &= <x_1^3-ax_1+bx_1-c, x_2+(x_1-a)x+x_1^2-ax_1+b, x_3+x_1+x_2-a> \end{aligned}$$

Hence $1 \notin I$ and $K[x_1,x_2,x_3]/I$ 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)

Hence the theory of fields containing the roots of a polynomial x^3-ax^2+bx-c is consistent

Construction of the algebraic closure

We can add the axiom schema to our atomic system

$$\exists x.x^n + u_1 x^{n-1} + \cdots + u_0 = 0$$

The *models* of this theory are exactly the algebraically closed fields K with a map $R \to K$

Construction of the algebraic closure

Lemma: *If $a \in R$ is nilpotent in $R[x]/<x^n + u_1 x^{n-1} + \cdots + u_0>$ then it is nilpotent in R*

Theorem: $a_1 = 0, \ldots, a_k = 0 \vdash a = 0$ *in the theory of algebraically closed fields extending the positive diagram of R iff a is in the radical of the ideal generated by $a_1, \ldots, a_k$*

In particular this theory is *inconsistent* iff $1 = 0$ in R

This gives a simple proof of the consistency of the theory of algebraically closed fields (without relying on quantifier eliminations)

Factorisation of primes

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

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

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

Interpretation of cut-elimination

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

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)

References

Abramsky "Domain theory in logical form"

G. Sambin (papers on formal topology)

P. Johnstone *Stone Spaces*

Mathreview of Bridges *Constructive Functional Analysis* by Kreinovich

References

Richman (papers on constructive mathematics)

MRR Mines-Richman-Ruitenburg

Coste-Lombardi-Roy

Edwards (papers on Kronecker and *Essays on Constructive Mathematics*)