Constructive Logic

Thierry Coquand

August 2008

This course

To present constructive mathematics using logic

Introduction to recent work in constructive algebra (H. Lombardi, P. Schuster, I. Yengui, . . .)

Connection with computer algebra? New algorithms? New ways of implementing algorithms?

Hilbert's Program, some history

The word *algebra* comes from the title of a book *Hibab al-jabr wal-muqubala* (around 825)

The word *algorithm* comes from the name of the author of this book *Al-Khwarizmi*

Until 1800 most works in algebra are mostly computations (like in computer algebra)

Example: elimination theory (Bezout, Poisson), Lagrange

Some history

The situation changes with Gauss, Abel, Galois

concept of *irreducible* polynomial: Gauss (cyclotomic polynomial), fundamental notion for Abel and Galois

Construction of the splitting field of a polynomial

Rational functions of given quantities (which will become *domain of rationality* for Kronecker, and later our notion of field, introduced by Dedekind)

Some history

The proofs still have a direct algorithmic interpretation

Galois insists on the *ideal* character of these computations

"*If now, you give me an equation that you have in any way you like and you want to know whether it is or not solvable by radicals, I have nothing to do but to indicate to you the way to reply to the question, but whithout to obliging either myself or anyone else to do so. In other word, the calculations are impracticable.*"

Same for Kronecker. The connection with computations is however essential

Some history

The connection between reasoning and algorithms became then less and less clear, typically through the different versions that Dedekind will give to his theory of ideals

Reference: Harold Edwards *The genesis of ideal theory*, Arch. Hist. Ex. Sci. 23 (1980)

Hilbert: all ideals of $K[X_1, \ldots, X_n]$ are of finite type

Noetherian: all ideals are of finite type

This proposition has *no* computational content, and it is logically complex (technically it cannot be expressed in first-order logic)

Some history

Examples: Dedekind domains

There are now described as: Noetherian integrally closed domain where any nonzero prime ideal is maximal

But a lot of important and computational properties of Dedekind domains are best captured without the Noetherian hypothesis (Prüfer domain)

For instance the fact that the intersection of two finitely generated ideals is finitely generated in a Dedekind domain corresponds to a nice algorithm (fundamental for Dedekind) which disappears if we use the notion of Noetherian ring

Mathematics and algorithms

We have lost the direct connection between reasoning and computing

It may be that, from a proof of an existence statement in mathematics, it is *not possible* to extract from it a computation of the witness the existence of which is claimed by this statement

Where does this non effectiveness come from?

Excluded-Middle

The law of Excluded-Middle, which implies in particular

$$\forall x.\psi(x) \vee \exists x.\neg\psi(x)$$

is the cause of the non effectiveness of mathematical arguments

This has been noticed explicitely first by Brouwer (and probably Hilbert was already aware of this point)

Not at all obvious when Brouwer made this remark since at the time people thought about the Axiom of Choice as the source of non effectivity

A simple example

Proposition: *If K is a field and P is a non constant polynomial in $K[X]$ there exists Q in $K[X]$ such that Q is irreducible and Q divides P*

The classical proof claims the existence of such a polynomial Q but it cannot give an algorithm for finding Q

Indeed, it can be shown that there is *no* such algorithm even if K is given as effectively as possible (this means that there is a test of equality, and a computable function which gives the inverse of any non zero element)

Axiom of Choice

The axiom of choice can be stated as the fact that any surjective map has a section

This is not valid constructively

$\{0,1\}^{\mathbb{N}} \to [0,1]$

$(b_n) \longmapsto \Sigma b_n/2^n$

This is a surjective map, but it has *no* continuous section

Axiom of Choice

It can be shown that

AC $\longrightarrow$ EM

where AC is the Axiom of Choice and EM is the law of Excluded-Middle

Brouwer-Heyting-Kolmogorov Interpretation

On the other hand, it was noticed by Kolmogorov that if we don't use the law of Excluded-Middle, then all logical connectives have a natural algorithmic interpretation

$A \vee B$: we can find either a proof of A or a proof of B

$A \wedge B$: we can find either a proof of A and a proof of B

$A \rightarrow B$: we can transform any proof of A to a proof of B

$\exists x.P(x)$: we can produce an object a with a proof of $P(a)$

$\forall x.P(x)$: for any a we can produce a proof of $P(a)$

Brouwer-Heyting-Kolmogorov Interpretation

A proof of $\neg A$ is an argument showing that we cannot prove A

On this interpretation we cannot claim $A \vee \neg A$: for any A we cannot either find a proof of A or show that we cannot prove A

Other example: we cannot claim $\forall n.f(n) = 0 \vee \exists n.f(n) \neq 0$

This would mean that we can decide "uniformely" if a numerical function is always 0 or not

Simple example

Discrete fields are axiomatised by the two conditions

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

$0 \neq 1$

Intuitively we have a structure with an equality (a priori, we don't know that we can decide this equality) and we can decide if an element is 0 or we can find an inverse of this element

We can then show $a \neq 0 \leftrightarrow \exists x.ax = 1$ *purely by logical consideration*

Simple example

Indeed we know $a = 0 \vee \exists x.ax = 1$, if furthermore $a \neq 0$ then we must have $\exists x.ax = 1$

Conversely if $ax = 1$ then $a = 0$ would imply $0 = 1$ and we have $0 \neq 1$ hence we have $a \neq 0$

Hence we deduce $a = 0 \vee a \neq 0$, and hence $a = b \vee a \neq b$

Hence by pure logic, we have shown that we can decide the equality

Simple example

This reasoning can be seen as an general algorithm, which transforms the algorithm which decides if an element is 0 or compute the inverse to an algorithm which decides equality

Notice furthermore that the correctness of this algorithm is exhibited at the same time

A *proof* in intuitionistic logic can be seen as an *algorithm* which comes together with its correctness proof

Intuitionistic Logic and algorithm

Bishop saw each proofs in his book as *instructions* for humans to carry out some computations

Constructive mathematics should provide an elegant way of developing algorithms together with their proofs of correctness

A general formulation of set theory and logic based on the Brouwer-Heyting-Kolmogorov interpretation is expressed in *Martin-Löf Type Theory*

Main Slogan

Algorithmic mathematics appears to be equivalent to mathematics that uses only intuitionistic logic

This is an experimental remark, from the experience of people working in constructive mathematics (Bridges, Richman, Lombardi)

"The desire for algorithmic interpretation forces the use of intuitionistic logic, and that restriction of the logic results in arguments that are entirely algorithmic in character"

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 in $R^{n \times n}$ then P is similar to one canonical idempotent matrix $I_{k,n},\ k \leqslant n$*

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

Constructive algebra

Proposition: *There is no irreducibility test for $k[X]$ even if k is discrete*

We reduce the problem to a decision $\forall n.\alpha_n = 0 \vee \exists n.\alpha_n = 1$

Is $X^2 + 1$ irreducible over $k[X]$ where k is the field generated by the elements $\alpha_n i,\ n \in \mathbb{N}$??

This field k is well-defined: its elements are polynomials $f(\alpha_0 i, \ldots, \alpha_n i)$ and it is *discrete*

$X^2 + 1$ is irreducible over $k[X]$ iff $\forall n.\alpha_n = 0$

Constructive algebra

For some special discrete fields k there is such a test

Kronecker gives some test in the case $k = \mathbb{Q}(X_1, \ldots, X_n)$ or for algebraic extensions of such field. See H. Edwards' *Essays in Constructive Mathematics*

In Kronecker's approach/Edwards' book, such an irreducibility test plays a fundamental role

Constructive algebra

In practice this lack of irreducibility test is not a problem since $k[X]$ is always a *Bezout* domain

That is, given p, q we can compute g such that $<g> = <p, q>$

This is a first-order (coherent) condition

$$\forall p\ q. \exists g\ u\ v\ a\ b.\ \ p = gu \wedge q = gv \wedge g = ap + bq$$

We get g by the Euclidian division algorithm (notice that even when we can compute irreducible factors, the computation of g is much less expensive)

Logical complexity

We have seen that the effectiveness of mathematical arguments is connected to purely logical considerations

We have introduced the distinction: intuitionistic/classical logic

There are further purely logical considerations relevant for Hilbert's program

Logical complexity

We have the following classification of logic, the three first levels are constructive

1 equational logic: theory of rings

2 (first-order) coherent logic: theory of local rings, discrete fields

3 (first-order) intuitionistic logic: to be regular

4 (first-order) classical logic

5 higher-order logic: to be Noetherian

Logical complexity

To be Noetherian: all ideals are finitely generated

This involves a quantification over all *subsets* of the ring

First-order: we quantify only over the elements of the ring

Logical complexity

There is *no* completeness theorem for higher-order logic (Gödel)

For first-order logic, as shown by Skolem and Gödel there is a completeness theorem (however the proof is not constructive)

Logical complexity

Most notions in algebra can be captured by first-order logic

For instance the notion of *ring* is purely equational, the notion of local ring, and of discrete fields can be expressed in coherent logic

This classification is relevant for constructive logic because of the following (classical) result which can be seen as a possible heuristic principle in constructive mathematics

If a result expressed in coherent *logic is semantically valid then it can be proved in coherent logic*

Logical complexity

The usual Completeness Theorem for first-order logic is also an interesting principle

If a result expressed in first-order *logic is semantically valid then it can be proved in first-order logic*

This is a remarkable result, which can be seen as a partial realisation of Hilbert's Program

We can replace *semantics* by *syntax*

Example: Jacobson radical

Classically one defines $J \subseteq R$ as the intersection of all maximal ideals of R

One can prove $x \in J \leftrightarrow \forall z.inv(1 - xz)$ where $inv(u) \equiv \exists y.uy = 1$

It follows that we have

$$\forall z.inv(1 - uz) \wedge \forall z.inv(1 - vz) \quad \rightarrow \quad \forall z.inv(1 - (u + v)z)$$

This is a *first-order tautology* and hence it can be proved in first-order logic

Furthermore the proof cannot be "too complicated"

Equational logic: example

Using existence a maximal ideal, it is simple to see that we cannot have $g : R^n \to R^m$ and $f : R^m \to R^n$ with $gf = 1$ if $n < m$

In term of matrix we cannot have Q in $R^{m\times n}$ and P in $R^{n\times m}$ such that $QP = I_m$

This is a purely equational statement. Hence it has a purely equation proof. For instance for $n = 1,\ m = 2$ we get that the following system has only a solution if the ring is trivial

$$ax = 1 \qquad ay = 0 \qquad bx = 0 \qquad by = 1$$

Coherent logic

A formula is positive iff it uses only $\bot, \wedge, \vee$ and $\exists$

A formula is coherent iff it is an implication between two positive formula

Example: axioms for local rings, for discrete fields and for algebraically closed fields

Main result: If a coherent formula is a semantical consequence of a coherent theory then there is an intuitionistic first-order derivation (and hence an algorithm)

Example

Lemma: *If R is a local ring and P is an idempotent matrix in $R^{n\times n}$ then P is similar to one canonical idempotent matrix $I_{k,n},\ k \leqslant n$*

This is a positive statement which holds in the theory of local rings

Hence, if it is true, we should expect to have a direct intuitionistic proof (we shall give one later)

Important constructive notions

Logically simple notions

Bezout Domain instead of Principal Ideal Domain

Gcd Domain instead of Unique Factorization Domain

Prüfer Domain instead of Dedekind Domain

Important constructive notions

Noetherian is a logically complex notion, and we shall avoid it as much as possible

coherent is often used instead of Noetherian

This is logically less complex (it involves quantification over integers). Remarkably, to be a Bezout domain or a Prüfer domain imply to be coherent

Important constructive notions

In algebra, most important notions can be formulated in *first-order* logic, for which Hilbert's notion of logical simplicity of proofs can be applied

Most notions are even formulated in *coherent* first-order logic

In analysis, one needs a stronger notion, namely ω-logic (the proofs are well-founded countably branching tree, not necessarily finite), which also satisfies a completeness theorem

Summary

The source of non effectivity in mathematical arguments is the law of Excluded-Middle

Intuitionistic logic is logic without using the law of excluded-middle. Any argument in intuitionistic logic has a direct computational interpretation (via the Brouwer-Heyting-Kolmogorov interpretation)

Completeness holds for first-order logic, and holds constructively for coherent logic. There is no completeness for higher-order logic.

Forcing for coherent theories

We consider only logical theories which extends the equational theory of rings

We define a forcing relation $R \Vdash \psi$ where R is a ring and ψ is a formula with parameters in R, by induction on ψ

If ψ is a formula with parameters in R and $f : R \to S$ is a ring morphism, we write $f(\psi)$ the formula where we replace the parameter a by $f(a)$

Forcing for coherent theories

$R \Vdash t_1 = t_2$ iff $t_1 = t_2$ in R

$R \Vdash \psi_1 \wedge \psi_2$ iff $R \Vdash \psi_1$ and $R \Vdash \psi_2$

$R \Vdash \psi_1 \to \psi_2$ iff for any $f : R \to S$ if we have $S \Vdash f(\psi_1)$ then we have $S \Vdash f(\psi_2)$

$R \Vdash \forall x.\psi(x)$ iff for any $f : R \to S$ and any a in S we have $S \Vdash f(\psi)(a)$

Forcing for coherent theories

The other clauses are relative to a notion of basic covering of a ring R that are a finite sequence of morphisms $f_1 : R \to S_1, \ \ldots, \ f_n : R \to S_n$

$R \Vdash \psi_1 \vee \psi_2$ iff we have a finite covering $f_1 : R \to S_1, \ \ldots, \ f_n : R \to S_n$ with $S_i \Vdash f_i(\psi_1)$ or $S_i \Vdash f_i(\psi_2)$ for all i

$R \Vdash \exists x.\psi(x)$ iff we have a finite covering $f_1 : R \to S_1, \ \ldots, \ f_n : R \to S_n$ and a finite number of elements u_i in S_i such that with $S_i \Vdash f_i(\psi)(u_i)$

Forcing for coherent theories

For the theory of local rings, the coverings are given by $R \to R[1/a_i]$ where $a_1, \ldots, a_n$ is a finite sequence of elements of R such that $1 = <a_1, \ldots, a_n>$

For the theory of discrete fields the covering are generated by the basic covering given by $R \to R/<a>$ and $R \to R[1/a]$. We *force* a to be zero or to be invertible

For the theory of algebraically closed fields, we add the basic covering $R \to R[x]/<p>$ where p is a unitary polynomial. We *force* the polynomial p to have a root.

Example

For the theory of local ring, if a is an element of R

$$R \Vdash inv(a) \vee inv(1-a)$$

since we have the covering $R \to R[1/a],\ R \to R[1/1-a]$ and

$$R[1/a] \Vdash inv(a) \qquad R[1/1-a] \Vdash inv(1-a)$$

Main Lemmas

Lemma: *If* $R \Vdash \psi$ *and* $f : R \to S$ *then* $S \Vdash f(\psi)$

Lemma: *If we have a covering* $f_i : R \to R_i$ *and* $R_i \Vdash f_i(\psi)$ *for all* i *then* $R \Vdash \psi$

Main result

Theorem: *If we have* $\psi_1, \ldots, \psi_n \vdash \psi$ *in* intuitionistic *logic and* $R \Vdash \psi_1, \ldots, R \Vdash \psi_n$ *then* $R \Vdash \psi$

This is a powerful result for showing that a formula is *not* derivable intuitionistically

Application 1

Proposition: *The formula* $\forall x.J(x) \vee inv(x)$ *is* not *derivable intuitionistically in the theory of local rings*

One possible reading of this proposition is that we cannot decide $J(x)$ or $inv(x)$ in general in a local ring

This formula is derivable classically since we have

$$\forall y.inv(1 - xy) \vee inv(xy)$$

and $inv(xy) \leftrightarrow inv(x) \wedge inv(y)$

Application 1

For showing the Proposition we show that we don't have $\mathbb{Z} \Vdash inv(2) \vee J(2)$

We show first that $R \Vdash J(a)$ iff a is *nilpotent* in R and $R \Vdash inv(a)$ iff a is invertible in R

We deduce that $R \Vdash inv(a) \vee J(a)$ holds iff a is invertible in R if R is an *integral* domain

Application 2

Proposition: *If T is the theory of algebraically closed fields k with a map $f : R \to k$ we have $T \vdash f(a) = 0$ iff a is nilpotent in R*

This is known as the "theorem of zeros" in Bourbaki, commutative algebra, Chapter 5

Application 2

Corollary: *With the same hypothesis, we have* $T \vdash f(p_1) = 0 \wedge \ldots f(p_n) = 0 \rightarrow f(p) = 0$ *iff* a *belongs to the radical of the ideal generated by* $p_1, \ldots, p_n$

Corollary: *The theory of algebraically closed fields over a given non trivial ring is consistent*

Furthermore this proof is intuitionistic (and does not rely on the actual construction of the algebraic closure; this is in the spirit of Hilbert's program)