Sheaf Models and Constructive Mathematics

Thierry Coquand

Seminario del Dipartimento di Informatica, Università di Verona, 12/04/2021

This talk

Discussion about *algorithms* and *proofs* in algebra

Algebraic closure of a field in constructive mathematics

Effective construction

An instance of the notion of *site* introduced by Grothendieck

The notions of *site* and of *topos* are important for *constructive* mathematics

Algebraic closure

F field

Study if an equation system has a solution in F

First try to see if the system has a solution in an algebraic closure of F

This is always possible

Then try to "descend" the solution to F

In general very difficult

E.g. if a solution in a Galois extension is invariant under automorphisms or group representation where all values of its character function are in F

Constructive algebra

Algebraic closure in constructive mathematics??

The problem is more basic than use of Zorn's Lemma

We cannot decide if a given polynomial in $F[X]$ is irreducible or not

Factorization Problem

Eine Bemerkung über die Unzerlegbarkeit von Polynomial

van der Waerden 1930

Ein Körper K soll explizite-bekannt *heißen wenn seine Elemente Symbole aus einem bekannten abzählbaren Vorrat von unterscheidbaren symbolen sind, deren Addition, Multiplikation, Subtraktion und Division sich in endlichvielen Schritten ausführen lassen.*

A field is called *explicitely known* if its elements are symbols from a known countable set of symbols, over which the arithmetic operations can be carried out by a finite number of steps

Factorization Problem

Behauptung. *Solange man keine allgemeine Methode hat, jedes Problem von der Art "Gibt es ein n mit der Eigenschaft $E(n)$?" zu lösen, solange kann es auch keine allgemeine Methode der Faktorzerlegung von Polynomen $f(x)$ mit Keffizienten aus einem explizite-bekannten Körper geben.*

If we can solve the irreducibility problem, we can decide a question $\exists n\ E(n)$ with $E(n)$ decidable

Factorization Problem

$F = \mathbb{Q}(\theta_1, \theta_2, \dots)$

$p_1,\ p_2,\ \dots$ enumeration of prime numbers

$\theta_n^2 = p_n$ if n does not satisfy $E(n)$

$\theta_n^2 = -1$ is n satisfies $E(n)$

Is $X^2 + 1$ irreducible in $F[X]$?

diese Eigenschaft $E(n)$ is für jedes n nach der Kronerckerschen Methode (siehe G. Hermann, a.a.O.) entscheidbar.

Factorization Problem

Note that this was formulated *before* the notion of *recursive* function was introduced!

Problem of polynomial factorization for coefficients in a *computable* field

Elements can be represented in a computer and we have algorithms for the arithmetic operations

Here we represent abstractly the question in intuitionistic logic

Use topos theory to show that a given class of problem does not have an *algorithmic* solution!

Constructive algebra

Algebra developped using *intuitionistic* logic

(Discrete) field: $\forall x\ (x = 0 \vee \exists y\ xy = 1)$

Also $1 \neq 0$ and this implies $\forall x\ (x = 0 \vee x \neq 0)$

Kripke counter-model

Times t_0 and t_1

A set is now given by a function $X_0 \rightarrow X_1$

X_0 what we know of the set at times t_0

X_1 what this set becomes at times t_1, with some elements identified and new elements coming in

We *may* stay at time t_0 forever

"Dynamic" structure

Constructive algebra

Kripke counter-model

At time t_0 we take $F = \mathbb{Q}$

At time t_1 we take $F = \mathbb{Q}[i]$

This defines a field $\forall x\ (x = 0 \vee \exists y\ xy = 1)$

We don't have $\forall x\ (x^2 + 1 \neq 0) \vee \exists x\ (x^2 + 1 = 0)$ at time t_0

$\exists x\ (x^2 + 1 = 0)$ at time t_0: we don't have any root

$\forall x\ (x^2 + 1 = 0)$ at time t_0: maybe we go to time t_1 and find a root

Constructive algebra

How to make sense of the (separable) algebraic closure of F?

Solution: the algebraic closure of F may not exist in our "universe" but it always exists in a topos extension of this universe

Furthermore this topos is effective

Constructive algebra and topos theory

This was suggested in two short papers of André Joyal

Les théorèmes de Chevalley-Tarski et remarque sur l'algèbre constructive 1975

La Logique des Topos 1982 (with André Boileau)

Hilbert: introduction and elimination of ideal elements

Consistency of the first-order theory AC_F of algebraically closed field over F

Constructive algebra and topos theory

Consider the *classifying topos* of the theory AC_F

This gives a "primitive recursive proof of consistency of the theory" (1982)

Why? Sketch of an elegant algebraic formulation of quantifier elimination

Constructive algebra and topos theory

Tarski and Chevalley Theorem (projection of constructible sets)

See Mohamed Barakat 2019

An algorithmic approach to Chevalley's Theorem on images of rational morphisms between affine varieties

Another way to prove the consistency is to establish a *cut-elimination* result

Forcing

We consider the forcing relation $R \Vdash \psi$

R is a (f.p.) F-algebra and ψ a first-order formula with parameters in R

$R \Vdash \psi \rightarrow \varphi$ if for all $f : R \rightarrow S$ we have $S \Vdash \psi f$ implies $S \Vdash \varphi f$

$R \Vdash \forall x \psi$ if for all $f : R \rightarrow S$ and a in S we have $S \Vdash \psi f(a/x)$

$R \Vdash \psi \wedge \varphi$ if $R \Vdash \psi$ and $R \Vdash \varphi$

Beth (1956) and Kripke (1964) semantics

Forcing

For ψ of the form $a = b$ or $\exists x \psi_1$ or $\psi_0 \vee \psi_1$

$R \Vdash \psi$ if $R/(a) \Vdash \psi$ and $R[1/a] \Vdash \psi$

$R \Vdash \psi$ if $R[X]/(P) \Vdash \psi$ with P monic (separable)

and we also have

$R \Vdash \exists x \psi$ if we have a in R such that $R \Vdash \psi(a/x)$.

$R \Vdash \psi \vee \varphi$ if we have $R \Vdash \psi$ or $R \Vdash \varphi$

$R \Vdash a = b$ if $a = b$ in R

Forcing

Then we have $R \Vdash \psi$ implies $S \Vdash \psi f$ for $f : R \rightarrow S$

Proposition: *We have $R \Vdash \psi$ if ψ provable in the theory AC_F*

$R \Vdash \exists x \ (x^2 + 1 = 0)$ since $R[u] \Vdash u^2 + 1 = 0$ with $R[u] = R[X]/(X^2 + 1)$

$R \Vdash a = 0 \vee \exists x \ (ax = 1)$ since $R/(a) \Vdash a = 0$ and $R[1/a] \Vdash \exists x \ (ax = 1)$

A proof of $R \Vdash \psi$ for ψ *coherent* is a finite tree

For getting consistency it is enough to show that we don't have $F \Vdash 0 = 1$

Forcing

By a direct proof tree induction

$R \Vdash u = 0$ iff u is nilpotent in R

This follows from: if u nilpotent in $R[1/a]$ and $R/(a)$ then u is nilpotent in R and if u nilpotent in $R[X]/(P)$ then u nilpotent in R

Corollary: *The theory of algebraically closed field over F is consistent*

The name "forcing" comes from Cohen (1964) and the notation $\Vdash$ from Scott

Scott pointed out the connection with intuitionistic logic

Consistency

The argument suggested by André Joyal is more complex but it gives more information

This is an elegant algebraic formulation of *quantifier elimination*

Consistency

Associate to each ring R a Boolean algebra $B(R)$

$B(R)$ is a point-free/algebraic descrition of the spectrum of R with the *constructible* topology

$D : R \rightarrow B(R)$ universal map such that

$$D(0) = 0 \qquad D(1) = 1 \qquad D(ab) = D(a) \wedge D(b) \qquad D(a + b) \leqslant D(a) \vee D(b)$$

Consistency

Any map $R \to S$ gives a map $B(R) \to B(S)$

Theorem: *The map* $B(\iota) : B(R) \to B(R[X])$ *has a left adjoint*

Chevalley's theorem: the projection of a constructible set is constructible

This corresponds to quantifier elimination $\exists : B(R[X]) \to B(R)$

We have $\exists(\psi(X)) \leqslant \varphi$ iff $\psi(X) \leqslant B(\iota)(\varphi)$

The argument is not developped in Joyal's papers, but there are now notes from Luis Español González, which describes the argument: e.g. reduces the general case of the Theorem to the case where R is a field

Consistency

This illustrates the fact that we can prove consistency without proving quantifier elimination

This was explicitely noticed by Herbrand's PhD thesis 1930

Il nous parait probable qu'elle permettrait également d'arriver à la non-contradiction de la théorie des corps réels et "réellement fermés"; mais les méthodes du Chapitre suivant nous y conduiraient plus aisément.

It was about the theory of real closed fields (independently of Tarski)

Forcing

This consistency proof has a very simple structure

But we have more

We build a model of *higher-order logic* i.e. simple type theory with a type of propositions, in which we have an algebraic closure

Note that we build a model of simple type theory and not set theory

We need only to consider a special kind of F-algebra: the triangular F-algebras

Sheaf models

Definition: *A F-algebra is triangular if it can be obtained from F by a sequence of (formal) monic separable extensions*

P separable: we have $AP + BP' = 1$ "all roots are simple roots"

Example: $\mathbb{Q}[x]$ where $x^2 = 3$ and then $\mathbb{Q}[x, y]$ where $y^3 + xy + 1 = 0$

Theorem: *If R is triangular then $R = R/(a) \times R[1/a]$ for all a in R*

Furthermore $R/(a)$ and $R[1/a]$ are products of triangular algebras

Site

Example: $P = X^2 - 4X + 3$

$R = \mathbb{Q}[b]$ where $b^2 - 4b + 3 = 0$

Inverse of $a = b - 4$? Compute gcd of $X - 4$ and $X^2 - 4X + 3$

We have $(b - 4)b = -3$ so inverse is $-b/3$ and $R[1/a] = R$

Inverse of $a = b - 3$? Compute gcd of $X - 3$ and $X^2 - 4X + 3$

Discover $(X - 3)(X - 1) = X^2 - 4X + 3$

$R = \mathbb{Q}[X]/(X - 3) \times \mathbb{Q}[X]/(X - 1) = R/(a) \times R[1/a]$

We have $R[1/a] = F$ and $R/(a) = F$

Forcing done constructively

Recursive realizability emphasizes the active aspect of constructive mathematics. However, Kleene's notion has the weakness that it disreagards that aspect of constructive mathematics which concern epistemological change. Precisely that aspect of constructive mathematics which Kleene's notion neglects is emphasized by Kripke's semantics for intuitionistic logic. However, Kripke's notion makes it appear that the constructive mathematician is a passive observer of a structure which gradually reveals itself. What is lacking is the emphasis on the mathematician as active which Kleene's notion provides.

Relativised realizability in intuitionistic arithmetic at all finite types

N. Goodman, JSL 1978

Forcing done constructively

In this example

We *discover* a factorization of $P = X^2 - 4X + 3$ by asking what is the inverse of $a - 3$

Interaction between *computation* and *knowledge*

Dynamical algebra

Only need to compute gcd of polynomials

This is computable, while to decide irreducibility is not possible in general

Introduced by Dominique Duval (1985), following a suggestion of Daniel Lazard, for computer algebra

cf. Teo Mora's book

Solving Polynomial Equation Systems: the Kronecker-Duval Philosophy

Site

We define a site

Objects: triangular F-algebra

Maps: maps of F-algebra

Coverings:

$R = R_1 \times \cdots \times R_m$

$R \to R[X]/(P)$ with P separable monic polynomial

Site

What is a *sheaf* over this site?

We should have $L(R)$ set for each triangular algebra R

We should have $L(R) \rightarrow L(S)$ for $R \rightarrow S$

(1) $L(R) = L(R_1) \times \cdots \times L(R_m)$ if $R = R_1 \times \cdots \times R_m$

(2) if we have $u(a)$ in $L(R[a])$ and $u(a) = u(b)$ in $L(R[a, b])$ then we have $u(a) = u$ for some unique u in $L(R)$

Here $R[a] = R[X]/(P)$ and $R[a, b] = R[X, Y]/(P(X), P(Y))$

Algebraic closure

In the topos model over this site, we can consider the presheaf

$L(R) = Hom(F[X], R)$

(Note that $F[X]$ is not in the base category, not being triangular.)

Theorem: L *is actually a* sheaf *and is the (separable) algebraic closure of* F

$L(R) = L(R_1) \times \cdots \times L(R_m)$

Algebraic closure

We have the pull-back diagram $P(a) = P(b) = 0$ and P monic

$$\begin{array}{ccc} R & \longrightarrow & R[b] \\ \downarrow & & \downarrow \\ R[a] & \longrightarrow & R[a,b] \end{array}$$

Note that $R[a]$ is a free R-module of basis $1,\ a, \ldots,\ a^{n-1}$

If $Q(a) = Q(b)$ with $d(Q) < d(P)$ then Q is a constant

Algebraic closure

The classifying topos of AC_F satisfies the axioms

$1 \neq 0 \qquad \forall x \;\; x = 0 \vee \exists y \; (xy = 1)$

$\forall x_1 \ldots \forall x_n \exists x \quad x^n + x_1 x^{n-1} + \cdots + x_n = 0$

The site we presented defines a topos over which we have L algebraic closure of F, which also satisfies the geometric (non coherent) axiom

$\forall x \bigvee_P \;\; P(x) = 0$

where the disjunction is over all monic separable polynomials P in $F[X]$

Algebraic closure

This model is *effective*

We can use it to do actual computations (Th. C. and B. Mannaa)

Algebraic closure

E.g. Abhyankar proof of Newton-Puiseux Theorem

Algebraic Geometry for Scientists and Engineers

course notes taken by Sudhir Ghorpade

For instance, given an equation $y^4 - 3y^2 + xy + x^2 = 0$ find y as a formal serie in x (in general $x^{1/n}$)?

The coefficients of this power serie have to be in an algebraic extension of $\mathbb{Q}$

Algebraic closure

We first prove that theorem assuming an algebraic closure of $\mathbb{Q}$

We need to consider *structures* we can build from L, in this examples $L((X))$

Theorem: $\cup_n L((X^{1/n}))$ *is separably closed*

Since this interpretation is *effective*, we find a triangular algebra $\mathbb{Q}[a,b]$ with $a^2 = 13/36$ and $b^2 = 3$

Algebraic closure

Note that $L[[X]] = L^{\mathbb{N}}$

We get a logical explanation of the following fact

In the Puiseux series expansion of y in terms of x, which might be infinite, we only need to consider a *finite* algebraic extension of $\mathbb{Q}$

Weak existence

We have $\forall_{x:L}\exists_{y:L}\ y^2 = x$ in this topos with $car(F) \neq 2$

Proposition: *There is no function* $f : L \to L$ *such that* $f(x)^2 = x$

$\Pi_{x:L}\{y : L \mid y^2 = x\}$ is empty

If $u \neq 0$ in R and $a^2 = u = b^2$ we don't have $a = b$ in $R[a, b]$

$$\begin{array}{ccc} R & \longrightarrow & R[b] \\ \downarrow & & \downarrow \\ R[a] & \longrightarrow & R[a,b] \end{array}$$

Weak existence

Existence means *local* existence, and it might be that we have witnesses that are not compatible, so that we cannot "patch" them together

What is going on?

J.L. Bell, *From Absolute to Local Mathematics*, 1988

Parallel with physics

Let S be a "space" (can be given by a Grothendieck site)

Canonical map $f : S \to 1$ and $f^* : Sh(1) \to Sh(S)$

$Sh(1)$ is the usual frame of sets and f^* is sheafification operation

The algebraic closure of F may not exist in $Sh(1)$ but may exist in $Sh(S)$

What is going on?

Bell: This is like change of *reference frames* in physics

Example (D. Scott): what is a real number in $Sh([0,1])$? It is a continuous function from $[0,1]$ to $\mathbb{R}$ seen from $Sh(1)$

In $Sh(1)$ such a real number is "varying"

But it is "constant" in $Sh([0,1])$!

What is going on?

Invariant physical law

Classical logic may not hold in $Sh(X)$ even if it holds in $Sh(1)$

E.g. $t_1 \rightarrow t_0$

If p does not hold at t_0 but becomes known at t_1 we don't have $p \vee \neg p$ at t_0

What is going on?

In $Sh(1)$ we have the field F

It may not be algebraically closed

In $Sh(S)$ the field F becomes (separably) algebraically closed!

F becomes $F^* = L$ where $L(R) = R \otimes_F F = R$

What is going on?

If A is a central simple algebra on F

A may not be trivial, e.g. quaternion algebra over $\mathbb{Q}$

But A becomes *trivial* in $Sh(S)$

This does not "descend"

What is going on?

A proof of Skolem-Noether Theorem by descent

Let u be an automorphism of A. We can transfer u to $Sh(S)$.

This is an automorphism of A^*, and A^* is a matrix algebra

It is an inner automaorphism, assuming the result known for matrix algebra

This means that the linear system $xu(e_1) = e_1x, \ \ldots, \ xu(e_m) = e_mx$ has a non zero solution in F^*

Since it has a non zero solution in F^* it has one non zero solution in F

Hence u can be represented by an inner automorphism in A as well

Explaining the sheaf condition

If a linear system in F has a non zero solution in $Sh(S)$ then it has a non zero solution in F

Example of descent

$G_m(R) = (A \otimes_F R)^{\times}$

$T(R)$ set of a in $G_m(R)$ such that $u = Int(a)$

T is an example of G_m-torsor

Any G_m-torsor is trivial

Explaining the sheaf condition

Any triangular algebra is regular $\forall x \exists ! y\ (x^2 y = x \wedge y^2 x = y)$

In $R[a,b]$ we can find idempotent e with $(1-e) = (a-b)$

$P_1(a,X) = \frac{P(X)-P(a)}{X-a}$

P separable

$R[a,b]/(e)$ can be described as $P(a) = 0$ and $P_1(a,b) = 0$

We have $R[a,b] = R \times R[a,b]/(e)$

$M(R[a,b]) = M(R) \times M(R[a,b]/(e))$

Explaining the sheaf condition

The sheaf condition can hence be reformulated as follows

(1) $M(R) = M(R_1) \times \ldots M(R_m)$ if $R = R_1 \times \cdots \times R_m$

(2) If $u(a) = u(b)$ in $M(R[a,b]/(e))$ we have $u(a) = u$ for some uniquely determined u in $M(R)$

Connection with Galois descent

Explaining the sheaf condition

$R[x_1,\dots,x_n]$ universal decomposition algebra of a monic separable polynomial over R

$$P = X^n - a_1X^{n-1} + \cdots + (-1)^n a_n$$

$$\sigma_1(x_1,\dots,x_n) = a_1 \qquad \dots \qquad \sigma_n(x_1,\dots,x_n) = a_n$$

The sheaf condition can be reformulated as: if $u(x_1)$ in $F(R[x_1])$ is such that $u(x_1) = \cdots = u(x_n)$ in $F(R[x_1,\dots,x_n])$ then $u(x_1)$ in $F(R)$

For Galois $u(x_1) = \frac{u(x_1)+\cdots+u(x_n)}{n}$

It implies that if $v(x_1,\dots,x_n)$ is invariant by permutation then it is in $F(R)$

Topos as generalised set theory

C. McLarty *The Uses and Abuses of the History of Topos Theory*, 1990

The notion of topos was introduced by Grothendieck

Lawvere-Tierney: notion of elementary topos 1970

Cartesian Closed Category with a subobject classifier

Model of *higher order logic* and not set theory

Dana Scott *A Proof of the Independence of the Continuum Hypothesis*, 1967

Topos as generalised set theory

His confidence in the project was strengthened by Dana Scott's work on Boolean valued models, which he heard about at a meeting that same spring at Oberwolfach. Even here it was not the set theoretic aspect of the work that caught Lawvere's attention but the logical aspect. He has said the independence proofs in ZF were less important to him than a paper in which Scott proved the continuum hypothesis independent of a kind of third order theory of the real numbers, because, Scott says: 'once one accepts the idea of Boolean values there is really no need to make the effort of constructing a model for full transfinite set theory' (Scott [1967], p. 109).

To Lawvere this seemed not only simpler than the version for ZF but more to the point.

Topos as generalised set theory

How to generalize the interpretation

Type theory/set theory

Gödel/Tarski formulation of simple type theory: only types $0,\ 1,\ 2, \dots$, with $n+1$ type of subsets of type n and 0 type of individuals

Set theory: start with 0 empty set and iterate power set transfinitely

Most technical difficulties of forcing are connected to this transfinite iteration

Topos as generalised set theory

This is one direction how to extend this model to more than simple type theory

But there is *another* direction

It is to add a *universe*, as in dependent type theory

The collection of sheaves is not a sheaf it is a *stack*

This is another direction: ∞-topos theory

Constructive algebra

Poincaré 1901

Sur les propriétés arithmétiques des courbes algébriques

François Châtelet *Géométrie Galoisienne* 1946

Algebraic versus Arithmetical