Sheaf Models and Constructive Mathematics

Thierry Coquand

HOTTEST seminar, 2021/01/28

This talk

First part: (separable) algebraic closure of a field

Topos model where we have an algebraic closure

Effective model

Second part: this is a model of higher order logic (Simple Type Theory)

How to refine this model to a model of Dependent Type Theory

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 representations where all characters are in F

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 $\forall x\ (x = 0 \vee x \neq 0)$

Algebraic closure?? 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

Constructive algebra

Kripke counter-model on $0 \leqslant 1$

At time 0 we take $F = \mathbb{Q}$

At time 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 0

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 is 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 ACF

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

Why? The 1975 note presents an elegant algebraic formulation of quantifier elimination

Tarski and Chevalley Theorem (projection of constructible sets)

Actually another way to prove the consistency is to establish some kind of 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

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

$R \Vdash \forall x \psi$ if for all $f : R \to S$ 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 $f : R \to S$

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

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

$R \Vdash a = b$ iff $a - b$ 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*

Remark: the argument suggested by André Joyal is more complex but it gives more information (quantifier elimination); this illustrates the fact that we can prove consistency without proving quantifier elimination (Herbrand 1930 about the theory of real closed fields)

Forcing

This is a nice result since the proof of consistency is very simple

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

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: $F[x]$ where $x^2 = 3$ and then $F[x, y]$ 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: $P = X^2 - 4X + 3$

$R = F[b]$ 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 $(X - 3)(X - 1) = X^2 - 4X + 3$

$R = F[X]/(X - 3) \times F[X]/(X - 1) = R/(a) \times R[1/a]$

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

Site

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

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

Algebraic closure

In the topos model over this site, we can consider

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

(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

$\bigvee_{a_1,\ldots,a_n} \quad x^n + a_1 x^{n-1} + \cdots + a_n = 0$

where the disjunction is over all lists $a_1, \ldots, a_n$ in F

Algebraic closure

This model is *effective*

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

E.g. Abhyankar proof of Newton-Puiseux Theorem

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 have to be in an algebraic extension of F

We first prove that theorem assuming an algebraic closure of F

We find the triangular algebra $F[a, b]$ with $a^2 = 13/36$ and $b^2 = 3$

Algebraic closure

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

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

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 $R[a, b]$

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

More general structures

We would like e.g. to consider the (groupoid) of all L-vectors spaces

This is not possible in the topos of sheaves since *we don't have universes*

Other example: we have the sheaf $G_m(A) = Hom(F[X, 1/X], A)$

Abelian group, one would like to form the groupoid of G_m-torsors

Theorem: *Any given G_m-torsor is trivial*

More general structures

Can we extend the model to a model of univalent dependent type theory *where we have an algebraic closure of a given field*

In such a model we should be able to state and prove

$$\Pi_{x:L} \left\| \Sigma_{y:L}\ y^2 =_L x \right\|$$

Combining forcing and realizability

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

How to go from presheaves to sheaves

Base category $\mathcal{C}$

$\Omega(X)$ set of sieves on X

Grothendieck topology: subpresheaf $\mathrm{Cov}(X)$ of $\Omega(X)$

Each $a : \Omega$ defines an idempotent monad $\eta_a^F : F \mapsto F^{T(a)}$

$F^{T(a)}$ type of "partial elements" of F of extent a

F is a sheaf if, and only if, each η_a^F is an isomorphism

Note that $F \mapsto F^{T(a)}$ defines an *idempotent* monad

Model of dependent type theory

Category of "shapes" $\mathcal{B}$ with an interval object I and a *cofibration classifier* Φ

A type is interpreted as a presheaf on $\mathcal{B}$ with an extra "filling" *structure*

Dependent type $\Gamma \vdash A$

Dependent presheaf with a fibration *structure*

Usual Kan filling condition is a *property*

We can then model *univalence* and *Higher Inductive Types*

Th. C. *A survey of constructive presheaf models of univalence*

Presheaf models

Since this approach is effective and essentially algebraic there is *no problem* to relativise it to an arbitrary presheaf model

We replace $\mathcal{B}$ by $\mathcal{C} \times \mathcal{B}$

$\mathsf{I}(X, J) = \mathsf{I}_{\mathcal{B}}(J)$

Different options are possible for Φ

Descent data

For going to presheaves to sheaves we have the condition that

$$\eta_a : F \to F^{T(a)}$$

is an isomorphism

Descent data for a sieve S on X:

we have u_f in $F(Y)$ for $f : Y \to X$ in the sieve S and $u_f g = u_{fg}$

Descent data operation

Over a type theoretic model, $F(X)$ is now a space

It is natural to change the notion of descent data to the following

-we have a path $u(f,g)$ between $u_f g$ and u_{fg}

-we have a triangle $u(f,g,h)$ connecting $u_f gh$ and $u_{fg}h$ and u_{fgh}

-and so on

For groupoids the condition with triangles is the cocycle condition used to glue algebraic structures

This defines an operation $D_a F(X)$ and we have a map $\eta_{D_a} : F \to D_a F$

Descent data operation

Constructive Sheaf Models of Type Theory
Th. C., Fabian Ruch and Christian Sattler

Operation D which is pointed $\eta_A : A \to DA$

Theorem: *If D is a descent data operation then $D(\eta_A)$ and η_{DA} are path equal and are equivalences*

This generalizes idempotent monads

For instance η_A is an equivalence if it has a left inverse

Axiomatisation: *lex operation* which generalizes the exponential operation

A *descent data* operation is a lex operation which is a modality

Descent data operation

If the base category $\mathcal{C}$ is small

Theorem: *D_a defines a left exact modality preserving universe size and such that each universe of modal D_a-types is itself modal*

Left exact modality are systematically studied in

Modalities in homotopy type theory
Egbert Rijke, Michael Shulman, Bas Spitters

See Remark A. 29

Descent data operation

For each universe $\mathcal{U}$ we have $D_a : \mathcal{U} \to \mathcal{U}$

We have that $\Sigma_{F:\mathcal{U}}\mathsf{isMod}_a(F)$ is itself D_a-modal

Definition: *F is a (proof relevant) sheaf if it is D_a-modal for all a*

Theorem: *If* Cov *is a Grothendieck topology on $\mathcal{B}$ then each universe of sheaves is itself a sheaf*

$\Sigma_{F:\mathcal{U}}\Pi_{a:\mathsf{Cov}}\mathsf{isMod}_a(F)$ is itself D_a-modal for all $a : \mathsf{Cov}$

Sheaf Model

We get a *new* model of type theory where a type is interpreted by a type *together with* a proof that this type if D_a-modal for all a

This is a model of *univalence* and *Higher Inductive Types*

"Internal model" methods, from PM Pédrot, K. Quirin, N. Tabareau, ...

Lawvere-Tierney Sheafification in Homotopy Type Theory, K. Quirin PhD

Failure is Not an Option: An Exceptional Type Theory

Sheaf Model

E.g. for nat, we consider the type with constructors

$0 : N$

$S : N \to N$

$\mathsf{patch} : \Pi_{a:\mathsf{Cov}}\ D_a N \to N$

$\mathsf{linv} : \Pi_{a:\mathsf{Cov}} \Pi_{n:N}\ \mathsf{patch}_a\ (\eta_a\ n) =_N n$

Sheaf Model

For $T = \|A\|$

inc : $A \to T$

squash : $\Pi_{t_0\ t_1:T}\ t_0 =_T t_1$

patch : $\Pi_{a:\mathsf{Cov}}\ D_a T \to T$

linv : $\Pi_{a:\mathsf{Cov}} \Pi_{t:T}\ \mathsf{patch}_a\ (\eta_a\ t) =_T t$

Sheaf Model

In the special case where the topology is trivial $\mathsf{Cov} = 1$

We only have one descent operation D

It is not the case that all presheaves are D-modal in general

This operation D is reminiscent of the cobar operation used by Mike Shulman

All $(\infty, 1)$*-topos have a strict univalent universe*

however it is a *left exact modality*

Sheaf Model

Lemma: *If* $\Gamma \vdash A$ *and* $\Gamma \vdash S : \mathsf{Cov}$ *and* A *is* D_S*-modal and each* $A\rho f$ *is contractible for* f *in* $S\rho$ *then* $A\rho$ *is inhabited*

L is a sheaf

Application $\Pi_{x:L} \left\| \Sigma_{y:L}\ y^2 =_L x \right\|$ is valid in the sheaf model

Sheaf Model

$u \neq 0$ in R and $a^2 = u = b^2$

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

$\mathsf{inc}(a, \mathsf{refl}_u)$ and $\mathsf{inc}(b, \mathsf{refl}_u)$ path related in $\left\| \Sigma_{y:L}\ y^2 =_L u \right\| (R[a,b])$

This forms a descent data

Sheaf Model

We get a model of Dependent Type Theory with univalence and higher inductive types with an algebraic closure of F

We have a type L which is a F-algebra and satisfies

$$\left\|\Sigma_{x:L} x^n + a_1 x^{n-1} + \cdots + a_n =_L 0\right\|$$

$$\Pi_{x:L}\ (x =_L 0\ +\ \Sigma_{y:L} xy =_L 1)$$

$$\neg(0 =_L 1)$$

Furthermore this model is effective

Future work: Long exact sequence

We have the short exact sequence of Abelian groups if $car(F) \neq 2$

$$1 \longrightarrow \mu_2 \longrightarrow G_m \xrightarrow{()^2} G_m \longrightarrow 1$$

We deduce the fibration sequence $\mathsf{B}\mu_2 \to \mathsf{B}G_m \to \mathsf{B}G_m$ hence the long fibration sequence (I learnt this from Ulrik Buchholtz)

$$\mu_2 \to G_m \to G_m \to \mathsf{B}\mu_2 \to \mathsf{B}G_m \to \mathsf{B}G_m$$

Long exact sequence

Applying global section

$$\mu_2(F) \to G_m(F) \to G_m(F) \to \mathsf{B}\mu_2(F) \to \mathsf{B}G_m(F)$$

and then we apply π_0 and get an exact sequence

$$\pi_0(G_m(F)) \to \pi_0(G_m(F)) \to \pi_0(\mathsf{B}\mu_2(F)) \to \pi_0(\mathsf{B}G_m(F))$$

Hence $\pi_0(\mathsf{B}\mu_2(F)) = F^\times/F^{\times 2}$, which is $\mathsf{H}^1(G(F_{sep}/F), \mu_2)$, since $\mathsf{B}G_m(F)$ is trivial

We can do the same for $\mathsf{B}^2\mu_2 \to \mathsf{B}^2G_m \to \mathsf{B}^2G_m$

Merkurjev's Theorem provides a simple description of $\mathsf{H}^2(G(F_{sep}/F), \mu_2)$

Future work: Nominal notations

In some models (cartesian or Dedekind cubical sets) we can think of stages I as finite sets of spatial "dimensions" $i_1, \ldots, i_n$

We get a "nominal" extension of type theory where elements may depend on dimensions $u(i_1, \ldots, i_n)$

For the algebraic closure model, the elements now also depend on algebraic quantity, e.g. $u(i, j, k, a, b)$ with $a^2 = 2,\ b^3 = b + a$

The maps in $\mathcal{C} \times \mathcal{B}$ can be thought of as substitutions

Future work: simplify the model

Connection with Galois descent

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

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 $F(R[x_1, \ldots, x_n])$ then $u(x_1)$ in $F(R)$

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

Sheaf Model

Can one simplify the descent data condition?

For instance a descent data for $R \to R[a]$, with a of degree 3

filled triangle connecting $u(a),\ u(b),\ u(c)$

natural strengthening of $u(a) = u(b) = u(c)$

Future work: Zariski topology

We can extend the base category, taking all finitely presented F-algebra

We take Zariski topology instead, so that $F[X]$ represents a sheaf

It is not a field anymore but a local ring which is separably closed (and contains the separable closure of F)

At any point we have a finite number of dimension variables and algebraic variables, with some conditions on these variables

$F[X]$ represents a "line"

We then have two notion of intervals and we can force $F[X]$ to be contractible