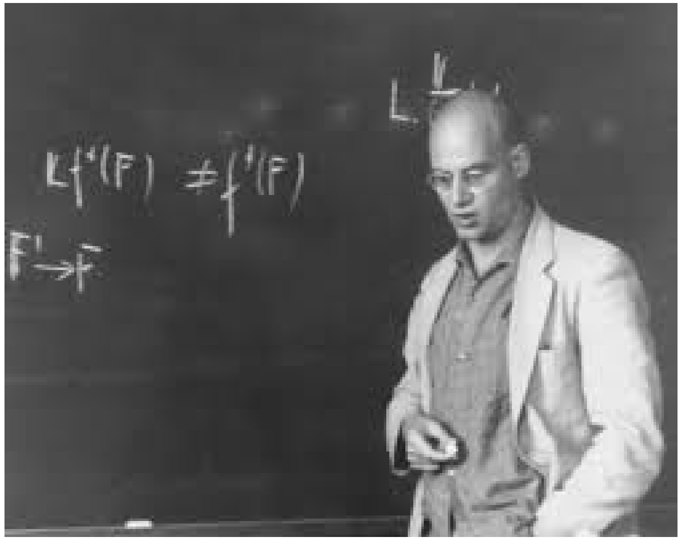
Plan

Lecture 1: Kripke-Joyal, some examples

Lecture 2: Newton-Puiseux, Zariski topos, Presheaf models of type theory

Lecture 3: Zariski topos, light condensed sets; towards higher topos

Sheaf models and constructive mathematics



Sheaf models and constructive mathematics

Sheaf models and constructive mathematics

Sheaf models

Rich history, which mixes logic and mathematics

1945-1950: Leray, Cartan, definition of sheaves over a topological space

1950 Eilenberg and Zilber "Semi-simplical complexes and singular homology"

1951 Church: complete Boolean algebra semantics of type theory

1956 Beth "Semantic construction of intuitionistic logic", *sheaf* model

1958 Kripke: letter to Prior, *presheaf* model

Sheaf models

1960 Grothendieck: sites, topos

1964 Cohen: forcing

1966 Scott, Solovay: forcing, Boolean valued model

1970 Kreisel and Troelstra: model of choice sequences

Sheaf models

Different intuitions

temporal (Beth, Kripke)

spatial (Eilenberg)

finite information (Cohen)

Kripke-Joyal semantics

Unification of logic and sheaf model via (Beth)-Kripke-Joyal semantics

Compositional explanation of what a mathematical statement means

"Epistemological" explanation

This compared with the "computational" interpretation of proofs as programs

Important to combine the epistemological and computational aspects

Semantics of intuitionistic logic

Brouwer $(\forall_n\ \alpha(n) = 0) \vee \exists_n\ \alpha(n) \neq 0$ not valid

Heyting 1931: formal rules of intuitionistic logic

Constructive mathematics: mathematics developped using intuitionistic logic

"Dynamical structure", evolving with time

Semantics of intuitionistic logic

Kripke model, indexed by time e.g. $1 \rightarrow 0$

Time dependent set: $A_0 \rightarrow A_1$

New elements can appear, and some new identifications can be discovered

We take $K_0 = \mathbb{Q}$ and $K_1 = \mathbb{Q}[i]$

Crucially, we can stay at time 0 for ever

Kripke insits on this point in his 1964 paper, and points out the difference with Beth models where we are forced to eventually move to a new stage

Semantics of intuitionistic logic

K defines a *discrete* field (decidable equality) of characteristic 0

We have $\forall_{x:K}\ x = 0 \vee U(x)$

where $U(x)$ means that x is a unit, i.e. $\exists_{y:K}\ xy = 1$

Theorem: *In this theory, we* cannot *prove that we have*

$(\forall_{x:K}\ x^2 + 1 \neq 0) \vee \exists_{x:K}\ x^2 + 1 = 0$

Semantics of intuitionistic logic

Indeed we don't have $\forall_{x:K}\ x^2+1\neq 0$ at time 0 since we may go to time 1, where we *do* have a root of $x^2+1=0$

And we don't have $\exists_{x:K} x^2+1=0$ since we may stay at time 0 forever

So the formula $(\forall_{x:K}\ x^2+1\neq 0)\vee\exists_{x:K}\ x^2+1=0$ is not valid in this Kripke model, and hence not provable

Interpretation: if K is given as a (discrete) field there is *no* algorithm to decide whether X^2+1 is irreducible or not

Semantics of intuitionistic logic

Note that there is *no* mention of recursive function theory/Turing machine

van der Waerden (1930) *Eine Bemerkung über die Unzerlegbarkeit von Polynomen* (before recursive functions theory was developped!)

Definition of field *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*

For some given field, e.g. if K is a given algebraic extension of $\mathbb{Q}$ of $\mathbb{F}_p$, we can decide irreducibility (Kronecker)

Semantics of intuitionistic logic

This is one first use of sheaf models/topos: to show that something is not constructively provable

Here are two more complex examples:

-in a local ring define $J(x) = \forall_y U(1 - xy)$ then we don't have $U(x) \vee J(x)$

-in simplicial sets, if $Y \to X$ is a Kan fibration and $x_0 \to x_1$ in X then we cannot build an equivalence $Y(x_0) \to Y(x_1)$ (Th. C. and M. Bezem 2013)

The second point showed that Voevodsky's semantics of dependent type theory with univalence where a type is interpreted as a Kan simplicial set cannot be done in an intuitionistic framework

Semantics of intuitionistic logic

The second example illustrates the fact that we want more than a semantics of first-order logic

We want to be able to interpret *function spaces*

What logic should we interpret? (This will be the topic of the next 2 lectures)

Topos $\leftrightarrow$ simple type theory

Higher Topos $\leftrightarrow$ dependent type theory $+$ univalence

Semantics of intuitionistic logic

This is a *negative* use of (pre)sheaf models (independence result)

Positive use of sheaf models: we can *force* the existence of “ideal” objects

Example: force the existence of a prime ideal

Constructively, cannot show the existence of a prime ideal for a given ring R

Prime ideals

A. Joyal's definition of the spectrum of R

Distributive lattice freely generated by *symbols* $D(a)$ and relations

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

This defines the Zariski spectrum $Z(R)$ as a *distributive lattice*

We think of $Z(R)$ as a topological space

$a \mapsto D(a)$ is a prime filter, where the truth values are open sets of $Z(R)$

Prime ideals

While it is not possible in general to build a prime ideal/filter of R we have an interpretation of $Z(R)$ as the distributive lattice of finitely generated *radical* ideals of R. This shows the *consistency* of $Z(R)$ seen as a theory.

In general the lattice of ideals of R is not distributive

$$\langle X+Y\rangle \cap \langle X,Y\rangle \neq (\langle X+Y\rangle \cap \langle X\rangle) + (\langle X+Y\rangle \cap \langle Y\rangle)$$

However the lattice of radical ideals is distributive

$$\sqrt{\langle a\rangle} \wedge \sqrt{\langle b,c\rangle} = \sqrt{\langle ab,ac\rangle}$$

Theorem: *We have* $1 = D(a_1) \vee \cdots \vee D(a_n)$ *if, and only if,* $1 = \langle a_1, \ldots, a_n\rangle$. *More generally* $D(a) \leqslant D(b_1, \ldots, b_n)$ *iff* a *is in the* radical *of the ideal* $(b_1, \ldots, b_n)$

Zariski and constructible spectrum

The *constructible spectrum* $B(R)$ is simply the free Boolean algebra over the Zariski spectrum $Z(R)$

(Compare with the definition in wikipedia!)

So we add new formal symbols $V(a)$ with the conditions $V(a) \wedge D(a) = 0$ and $V(a) \vee D(a) = 1$

Theorem: *We have* $\wedge_i D(a_i) \wedge \wedge_k V(c_k) \leqslant \vee_j D(b_j) \vee \vee_l V(e_l)$ *iff* $\wedge_i D(a_i) \wedge \wedge_l D(e_l) \leqslant \vee_j D(b_j) \vee \vee_k D(c_k)$

This was Gentzen's insight when he invented sequent calculus!

Entailment Relations

This use of Gentzen's insight to describe distributive lattices goes back to Lorenzen

Algebraische und logistische Untersuchungen über freie Verbände, 1951

It was rediscovered in

Entailment Relations and Distributive Lattices, 1998, Th. C. and J. Cederquist

and it is presented in details in

Commutative Algebra: Constructive Methods, H. Lombardi and C. Quitté

Use of prime ideals

It can be shown that, even if one ring is given effectively, it is not possible in general to define effectively a prime ideal on this ring

Lawvere (ICM 1970) conjectured the existence of a prime filter for any non trivial ring in an arbitrary topos (= constructively)

Thought it would work constructively with prime filters instead of prime ideals

However, Joyal built a topos where a ring does not have any prime filter (the object of prime filters is empty)

Logical interpretation

"Lattice-valued" model: the predicate $a \longmapsto V(a)$ is a predicate on the ring R with values in the constructible spectrum/lattice

This predicate defines a (decidable) prime ideal on the ring

This is a "generic" decidable prime ideal

This prime ideal exists, but *in a sheaf model* over the constructible spectrum

Constructible spectrum

We have $V(a) = 1$ iff $D(a) = 0$ iff a is nilpotent

This corresponds to the (classical) result that an element is nilpotent iff it belongs to all nilpotent ideals

We have $V(ab) = V(a) \vee V(b)$ since $D(ab) = D(a) \wedge D(b)$

Application: Prime ideals

Define a polynomial to be *primitive* if the ideal generated by its coefficients is trivial

Proposition: *The product of two primitive polynomials is primitive*

For instance, if $a_0u_0 + a_1u_1 = b_0v_0 + b_1v_1 + b_2v_2 = 1$ then

$a_0b_0w_0 + (a_0b_1 + a_1b_0)w_1 + (a_0b_2 + a_1b_1)w_2 + a_1b_2w_3 = 1$

for some w_0, w_1, w_2, w_3

This is a concrete statement, proved using an ideal element

Concrete instance of Hilbert's program

Prime ideals

If α prime ideal then $(R/\alpha)[X]$ is an integral domain

$\Sigma a_i X^i$ is primitive if, and only if, $\Sigma a_i X^i \neq 0$ mod. α for *all* prime ideal α

There is no prime ideal that contains all a_i

It is clear that if A is an integral domain, then so is $A[X]$

Prime ideals

A prime ideal of R may not exist constructively

But it *always* exists in the sheaf model over $B(R)$!

By working in a sheaf model, we *force* the existence of a prime ideal

If $\Sigma c_k X^k = (\Sigma a_i X^i)(\Sigma b_j X^j)$ we have (“Gauss-Joyal” identity)

$\vee_k D(c_k) = (\vee_i D(a_i)) \wedge (\vee_j D(b_j))$

which is equivalent to $\wedge_k V(c_k) = (\wedge_i V(a_i)) \vee (\wedge_j V(b_j))$

Logical interpretation

One can build (effectively) a generic prime filter, but in a sheaf model (introduction), and we can then eliminate the use of this prime filter

This is a possible interpretation of Hilbert's method of *introduction* and *elimination* of ideal elements

This is closely connected to *forcing*: we force the existence of a prime ideal by moving to a sheaf model

In algebraic geometry, there is the notion of *descent*, going back to Galois, where we ask if we can "descend" the existence of the ideal object in the topos of sets

Use of sheaf models/topos theory

This is an example of the use of sheaf models

We can understand constructively a classical argument if this argument uses an object like prime ideal in a generic way

Note that such an object is justified by the use of the Axiom of Choice, and the technique of negative translation *does not* apply there

For other examples of this method, see the book of Lombardi and Quitté *Commutative Algebra: Constructive Methods*

Exercise

If R is connected (i.e. $e^2 = e$ implies $e = 0$ or $e = 1$) then any unit of $R[X, 1/X]$ can be written uniquely on the form

$X^m \Sigma_p u_p X^p$

where m integer and u_0 unit and u_p nilpotent for $p \neq 0$

Cf. Ingo Blechschmidt *Generalized spaces for constructive algebra* for other examples