A general Nullstellensatz for generalized spaces

Logic Workshop in Munich
May 10th, 2019

Ingo Blechschmidt
Università di Verona

The mystery of nongeometric sequents

Let $\mathbb{T}$ be a geometric theory, for instance the theory of rings.

sorts, function symbols, relation symbols, geometric sequents as axioms

sorts: R
fun. symb.: $0, 1, -, +, \cdot$
axioms: $(\top \vdash_{x,y:R} xy = yx), \ldots$

$\mathbb{Z}$ $\mathbb{Z}[X, Y, Z]/(X^n + Y^n - Z^n)$ $\mathcal{O}_X$ $U_{\mathbb{T}}$

A *geometric sequent* is a syntactical expression of the form $(\varphi \vdash_{x_1 : X_1, \ldots, x_n : X_n} \psi)$, where $x_1 : X_1, \ldots, x_n : X_n$ is a list of variable declarations, the X_i ranging over the available sorts, and φ and ψ are *geometric formulas*. Often the variable context is abbreviated to $\vec{x} : \vec{X}$ or even just $\vec{x}$. Such a sequent is read as "in the context of variables $\vec{x}$, φ entails ψ".

Geometric formulas are built from atomic propositions (using equality or the relation symbols) using the connectives $\top$, $\bot$, $\wedge$, $\bigvee$ (set-indexed disjunction) and $\exists$. Geometric formulas may not contain $\neg$, $\Rightarrow$, $\forall$.

There is a notion of a *model* of a geometric theory in a given topos. For instance, a ring in the usual sense is a model of the theory of rings in the topos Set. The structure sheaf of a scheme X is a model in the topos $\mathrm{Sh}(X)$ of set-valued sheaves on X.

With *topos* we mean Grothendieck topos, and as metatheory we use a constructive but impredicative flavour of English (which could be formalized by what is supported by the internal language of elementary toposes with an NNO). However the Nullstellensatz presented later makes no use of the subobject classifier, hence the results can likely be generalized to hold in a predicative metatheory or to hold for arithmetic universes.

The mystery of nongeometric sequents

Let $\mathbb{T}$ be a geometric theory, for instance the theory of rings.

sorts, function symbols, relation symbols, geometric sequents as axioms

sorts: R
fun. symb.: $0, 1, -, +, \cdot$
axioms: $(\top \vdash_{x,y:R} xy = yx), \ldots$

$\mathbb{Z}$ $\mathbb{Z}[X,Y,Z]/(X^n + Y^n - Z^n)$ $\mathcal{O}_X$ $U_{\mathbb{T}}$

Theorem. There is a **generic model** $U_{\mathbb{T}}$. It is **conservative** in that for any geometric sequent σ the following notions coincide:

1. The sequent σ holds for $U_{\mathbb{T}}$.
2. The sequent σ holds for any (sheaf) model of $\mathbb{T}$.
3. The sequent σ is provable modulo $\mathbb{T}$.

Among all models in any topos, the *universal* or *generic* one is special. It enjoys the universal property that any model in any topos can be obtained from it by pullback along an essentially unique geometric morphism. It is intriguing from a logical point of view because it has exactly those properties which are shared by any model in any topos.

One could argue, with a certain amount of success, that the generic model of the theory of rings is what a mathematician implicitly refers to when she utters the phrase “Let R be a ring”. This point of view is fundamental to the slogan *continuity is geometricity*, as expounded for instance in Continuity and geometric logic by Steve Vickers.

The mystery of nongeometric sequents

Let $\mathbb{T}$ be a geometric theory, for instance the theory of rings.

sorts, function symbols, relation symbols, geometric sequents as axioms

sorts: R
fun. symb.: $0, 1, -, +, \cdot$
axioms: $(\top \vdash_{x,y:R} xy = yx), \ldots$

$\mathbb{Z}$ $\quad \mathbb{Z}[X,Y,Z]/(X^n + Y^n - Z^n)$ $\quad \mathcal{O}_X$ $\quad U_{\mathbb{T}}$

Theorem. There is a **generic model** $U_{\mathbb{T}}$. It is **conservative** in that for any geometric sequent σ the following notions coincide:

1. The sequent σ holds for $U_{\mathbb{T}}$.
2. The sequent σ holds for any (sheaf) model of $\mathbb{T}$.
3. The sequent σ is provable modulo $\mathbb{T}$.

Observation (Kock). The generic local ring is a field:

$$(x = 0 \Rightarrow \bot) \vdash_{x:R} (\exists y : R.\, xy = 1)$$

Among all models in any topos, the *universal* or *generic* one is special. It enjoys the universal property that any model in any topos can be obtained from it by pullback along an essentially unique geometric morphism. It is intriguing from a logical point of view because it has exactly those properties which are shared by any model in any topos.

One could argue, with a certain amount of success, that the generic model of the theory of rings is what a mathematician implicitly refers to when she utters the phrase "Let R be a ring". This point of view is fundamental to the slogan *continuity is geometricity*, as expounded for instance in Continuity and geometric logic by Steve Vickers.

Crucially, the conservativity statement only pertains to properties which can be put as geometric sequents. Generic models may have additional nongeometric properties. Because conservativity does not apply to them, they are not shared by all models in all toposes – but any consequences which can be put as geometric sequents are.

For instance, if we want to verify a geometric sequent for all local rings, we may freely use the displayed field axiom. Hence one reason why these nongeometric sequents are interesting is because they provide us with new reduction strategies ("without loss of generality").

On the generic model

The generic model is **not** the same as …

- the **initial model** (think $\mathbb{Z}$) or
- the **free model on one generator** (think $\mathbb{Z}[X]$).

Set-based models are **too inflexible**.

The generic model is a **sheaf model**.

In case the theory $\mathbb{T}$ is a Horn theory (for instance if it is an equational theory), the *term algebra* (the set of terms in the empty context modulo provable equality) is a model of $\mathbb{T}$. While such models do enjoy some nice categorical properties, they are in general *not* the generic model.

For instance, if $\mathbb{T}$ is the theory of rings, then the initial model is $\mathbb{Z}$. This model validates some geometric sequents which are not validated by all rings, for instance $(x^2 = 0 \vdash_{x:R} x = 0)$ or $(1 = 0 \vdash \bot)$.

In general, the generic model cannot be realized as a set-based model (with a set for each sort, a map for each function symbol and so on). Sets are too constant for this purpose; the flexibility of sheaves ("variable sets") is required: The generic model lives in the topos of set-valued sheaves over $\mathcal{C}_{\mathbb{T}}$.

On the generic model

The generic model is **not** the same as …

- the **initial model** (think $\mathbb{Z}$) or
- the **free model on one generator** (think $\mathbb{Z}[X]$).

Set-based models are **too inflexible**.

The generic model is a **sheaf model**.

The special case that the generic model of a theory $\mathbb{T}$ can be realized as a set-based model occurs iff $\mathbb{T}$ is Morita-equivalent to the empty theory, that is, iff $\mathbb{T}$ has exactly one model in any topos.

The special case that there exists at least some conservative set-based $\mathbb{T}$-model occurs iff $\mathbb{T}$ has a conservative geometric expansion to a theory which is Morita-equivalent to the empty theory.

A primer on sheaf semantics

Write "$\mathrm{Set}[\mathbb{T}] \models \varphi$" for $\{.\,\top\} \models \varphi$. We define

$$\{\vec{x}.\,\alpha\} \models \varphi \quad (\text{“}\varphi \text{ holds on stage } \{\vec{x}.\,\alpha\}\text{”})$$

for Horn formulas α (in contexts $\vec{x}$) and first-order formulas φ.

$$\begin{array}{ll}
\{\vec{x}.\,\alpha\} \models \top & \text{iff true} \\
\{\vec{x}.\,\alpha\} \models \bot & \text{iff } \cancel{\text{false}}\ \alpha \vdash_{\vec{x}} \bot \\
\{\vec{x}.\,\alpha\} \models s = t : F & \text{iff } s = t \in F(\{\vec{x}.\,\alpha\}) \\
\{\vec{x}.\,\alpha\} \models \varphi \wedge \psi & \text{iff } \{\vec{x}.\,\alpha\} \models \varphi \text{ and } \{\vec{x}.\,\alpha\} \models \psi \\
\{\vec{x}.\,\alpha\} \models \varphi \vee \psi & \text{iff } \cancel{\{\vec{x}.\,\alpha\} \models \varphi \text{ or } \{\vec{x}.\,\alpha\} \models \psi} \\
& \quad \text{there exists a covering } (\{\vec{y}_i.\,\beta_i\} \xrightarrow{p_i} \{\vec{x}.\,\alpha\})_i \\
& \qquad \text{such that for all } i\text{: } \{\vec{y}_i.\,\beta_i\} \models p_i^*\varphi \text{ or } \{\vec{y}_i.\,\beta_i\} \models p_i^*\psi \\
\{\vec{x}.\,\alpha\} \models \varphi \Rightarrow \psi & \text{iff for all } \{\vec{y}.\,\beta\} \xrightarrow{p} \{\vec{x}.\,\alpha\}\text{: } \{\vec{y}.\,\beta\} \models p^*\varphi \text{ implies } \{\vec{y}.\,\beta\} \models p^*\psi \\
\{\vec{x}.\,\alpha\} \models \forall s : F.\,\varphi & \text{iff for all } \{\vec{y}.\,\beta\} \xrightarrow{p} \{\vec{x}.\,\alpha\} \text{ and } s_0 \in F(\{\vec{y}.\,\beta\})\text{: } \{\vec{y}.\,\beta\} \models (p^*\varphi)[s_0/s] \\
\{\vec{x}.\,\alpha\} \models \exists s : F.\,\varphi & \text{iff } \cancel{\text{there exists } s_0 \in F(\{\vec{x}.\,\alpha\}) \text{ such that } \{\vec{x}.\,\alpha\} \models \varphi[s_0/s]} \\
& \quad \text{there exists a covering } (\{\vec{y}_i.\,\beta_i\} \xrightarrow{p_i} \{\vec{x}.\,\alpha\})_i \text{ such that for all } i\text{:} \\
& \qquad \text{there exists } s_0 \in F(\{\vec{y}_i.\,\beta_i\}) \text{ such that } \{\vec{y}_i.\,\beta_i\} \models (p_i^*\varphi)[s_0/s]
\end{array}$$

The internal language of a (Grothendieck or elementary) topos $\mathcal{E}$ is a device which allows us to speak and reason about the objects and morphisms of $\mathcal{E}$ in a naive element-based language close to the usual formal mathematical language. Using this language, objects of $\mathcal{E}$ look like plain old sets [or types]; morphisms look like plain old maps between those sets; epimorphisms look like surjections; group objects look like groups; and so on.

In particular, we can use the internal language to define what it means for a given $\mathbb{T}$-structure in $\mathcal{E}$ to be a model – namely iff it looks like a model from the internal point of view.

The internal language can be implemented by the *Kripke–Joyal semantics*, a translation procedure which converts formulas of the internal language into external statements about the objects and morphisms of $\mathcal{E}$. The slide displays some of the translation rules in the case that $\mathcal{E}$ is a Grothendieck topos.

We can actually do mathematics internally because the Kripke–Joyal semantics is sound with respect to intuitionistic logic: If $\mathcal{E} \models \varphi$ and if φ intuitionistically entails a further formula ψ, then $\mathcal{E} \models \psi$.

An instructive special case is provided by the topos Set, because $\mathrm{Set} \models \varphi$ iff φ holds in the usual mathematical sense.

A primer on sheaf semantics

Write "$\mathrm{Set}[\mathbb{T}] \models \varphi$" for $\{.\,\top\} \models \varphi$. We define

$$\{\vec{x}.\,\alpha\} \models \varphi \quad (\text{“}\varphi \text{ holds on stage } \{\vec{x}.\,\alpha\}\text{”})$$

for Horn formulas α (in contexts $\vec{x}$) and first-order formulas φ.

$\{\vec{x}.\,\alpha\} \models \top$ iff true

$\{\vec{x}.\,\alpha\} \models \bot$ iff ~~false~~ $\alpha \vdash_{\vec{x}} \bot$

$\{\vec{x}.\,\alpha\} \models s = t : F$ iff $s = t \in F(\{\vec{x}.\,\alpha\})$

$\{\vec{x}.\,\alpha\} \models \varphi \wedge \psi$ iff $\{\vec{x}.\,\alpha\} \models \varphi$ and $\{\vec{x}.\,\alpha\} \models \psi$

$\{\vec{x}.\,\alpha\} \models \varphi \vee \psi$ iff $\cancel{\{\vec{x}.\,\alpha\} \models \varphi \text{ or } \{\vec{x}.\,\alpha\} \models \psi}$

there exists a covering $(\{\vec{y}_i.\,\beta_i\} \xrightarrow{p_i} \{\vec{x}.\,\alpha\})_i$

such that for all i: $\{\vec{y}_i.\,\beta_i\} \models p_i^*\varphi$ or $\{\vec{y}_i.\,\beta_i\} \models p_i^*\psi$

$\{\vec{x}.\,\alpha\} \models \varphi \Rightarrow \psi$ iff for all $\{\vec{y}.\,\beta\} \xrightarrow{p} \{\vec{x}.\,\alpha\}$: $\{\vec{y}.\,\beta\} \models p^*\varphi$ implies $\{\vec{y}.\,\beta\} \models p^*\psi$

$\{\vec{x}.\,\alpha\} \models \forall s : F.\,\varphi$ iff for all $\{\vec{y}.\,\beta\} \xrightarrow{p} \{\vec{x}.\,\alpha\}$ and $s_0 \in F(\{\vec{y}.\,\beta\})$: $\{\vec{y}.\,\beta\} \models (p^*\varphi)[s_0/s]$

$\{\vec{x}.\,\alpha\} \models \exists s : F.\,\varphi$ iff $\cancel{\text{there exists } s_0 \in F(\{\vec{x}.\,\alpha\}) \text{ such that } \{\vec{x}.\,\alpha\} \models \varphi[s_0/s]}$

there exists a covering $(\{\vec{y}_i.\,\beta_i\} \xrightarrow{p_i} \{\vec{x}.\,\alpha\})_i$ such that for all i:

there exists $s_0 \in F(\{\vec{y}_i.\,\beta_i\})$ such that $\{\vec{y}_i.\,\beta_i\} \models (p_i^*\varphi)[s_0/s]$

The Kripke–Joyal semantics can be extended to interpret unbounded quantification ("for all sets" as opposed to "for all elements of the particular set X") and dependent types. The former are for instance required to express universal properties ("for all groups", "for all rings"), and the latter are all over the place, even if their use might not be particularly highlighted.

With these extensions, we can import all of everyday constructive impredicative mathematics into the internal world of a topos.

Some illustrations of working with the internal language can be found in these sets of slides:

- Slides for Jürgen Jost's group seminar at the MPI Leipzig
- Slides for *Toposes in Como* (recording available)

A longer exposition, with pointers to the literature, can be found in Section 2 of these notes.

A selection of nongeometric properties

The **generic object** validates:

1. $\forall x, y : U_{\mathbb{T}}.\ \neg\neg(x = y)$.
2. $\forall x_1, \ldots, x_n : U_{\mathbb{T}}.\ \neg\forall y : U_{\mathbb{T}}.\ \bigvee_{i=1}^{n} y = x_i$.
3. $(U_{\mathbb{T}})^{U_{\mathbb{T}}} \cong 1 \amalg U_{\mathbb{T}}$.

The **generic ring** validates:

1. $\forall x : U_{\mathbb{T}}.\ \neg\neg(x = 0)$.
2. $\forall x : U_{\mathbb{T}}.\ (x = 0 \Rightarrow 1 = 0) \Rightarrow (\exists y : U_{\mathbb{T}}.\ xy = 1)$.

The **generic local ring** validates:

1. $\neg\forall x : U_{\mathbb{T}}.\ \neg\neg(x = 0)$.
2. $\forall a_0, \ldots, a_{n-1} : U_{\mathbb{T}}.\ \neg\neg\exists x : U_{\mathbb{T}}.\ x^n + a_{n-1}x^{n-1} + \cdots + a_0 x^0 = 0$.
3. Let $\Delta = \{\varepsilon : U_{\mathbb{T}} \mid \varepsilon^2 = 0\}$. For any map $f : \Delta \to U_{\mathbb{T}}$, there are unique elements $a, b : U_{\mathbb{T}}$ s. th. $f(\varepsilon) = a + b\varepsilon$ for all $\varepsilon : \Delta$.

The generic object, the generic model of the theory which has exactly one sort and no function symbols, relations symbols or axioms, appears to be slightly indecisive: On the one hand, up to a double negation, it is a subsingleton; on the other hand, it is infinite. This observation is due to Carsten Butz and Peter Johnstone (Classifying toposes for first-order theories).

The generic ring, the generic model of the theory of rings, is similarly indecisive. It is infinite in the following sense:

$$\forall x_1, \ldots, x_n : U_{\mathbb{T}}.\ \left(\forall y : U_{\mathbb{T}}.\ \bigvee_{i=1}^{n} (y = x_i)\right) \Rightarrow 1 = 0.$$

The theory of local rings is the quotient theory of the theory of rings obtained by adding the axioms

$$(1 = 0 \vdash \bot) \text{ and } ((\exists z.\ (x + y)z = 1) \vdash_{x,y} (\exists z.\ xz = 1) \vee (\exists z.\ yz = 1)).$$

(Assuming the axiom of choice, a ring is local in this sense iff it local in the usual sense (has exactly one maximal ideal).)

The first displayed property of the generic local ring illustrates that nongeometric sequents need not be inherited by quotient theories.

A selection of nongeometric properties

The **generic object** validates:

1. $\forall x, y : U_{\mathbb{T}}.\ \neg\neg(x = y)$.
2. $\forall x_1, \ldots, x_n : U_{\mathbb{T}}.\ \neg\forall y : U_{\mathbb{T}}.\ \bigvee_{i=1}^{n} y = x_i$.
3. $(U_{\mathbb{T}})^{U_{\mathbb{T}}} \cong 1 \amalg U_{\mathbb{T}}$.

The **generic ring** validates:

1. $\forall x : U_{\mathbb{T}}.\ \neg\neg(x = 0)$.
2. $\forall x : U_{\mathbb{T}}.\ (x = 0 \Rightarrow 1 = 0) \Rightarrow (\exists y : U_{\mathbb{T}}.\ xy = 1)$.

The **generic local ring** validates:

1. $\neg\forall x : U_{\mathbb{T}}.\ \neg\neg(x = 0)$.
2. $\forall a_0, \ldots, a_{n-1} : U_{\mathbb{T}}.\ \neg\neg\exists x : U_{\mathbb{T}}.\ x^n + a_{n-1}x^{n-1} + \cdots + a_0 x^0 = 0$.
3. Let $\Delta = \{\varepsilon : U_{\mathbb{T}} \mid \varepsilon^2 = 0\}$. For any map $f : \Delta \to U_{\mathbb{T}}$, there are unique elements $a, b : U_{\mathbb{T}}$ s. th. $f(\varepsilon) = a + b\varepsilon$ for all $\varepsilon : \Delta$.

All of the displayed properties give rise to reduction techniques: If we want to verify a geometric sequent for all rings, it suffices to verify it for the generic ring; but the generic ring has additional nongeometric properties not shared by every ring, such as the two displayed ones. (This was for instance used by Anders Kock and by Gonzalo Reyes.)

However, we face some challenges when pursuing these reduction techniques, including the following:

1. It is not easy to determine interesting and useful properties of the generic model.
2. The set of validated nongeometric sequents changes slightly unpredictably when passing to quotient theories. For instance, when proving that a geometric sequent holds for all rings, we may assume that any element is *not not* zero. But we may not assume this simplification if we want to verify a geometric sequent for all local rings (and if we want to exploit the given locality in the proof).
3. There is only so much we want to state and prove in full generality for all rings, all local rings, all modules, and so on. We are often much more interested in properties of particular mathematical objects.

A selection of nongeometric properties

The **generic object** validates:

1. $\forall x, y : U_{\mathbb{T}}.\ \neg\neg(x = y)$.
2. $\forall x_1, \ldots, x_n : U_{\mathbb{T}}.\ \neg\forall y : U_{\mathbb{T}}.\ \bigvee_{i=1}^{n} y = x_i$.
3. $(U_{\mathbb{T}})^{U_{\mathbb{T}}} \cong 1 \amalg U_{\mathbb{T}}$.

The **generic ring** validates:

1. $\forall x : U_{\mathbb{T}}.\ \neg\neg(x = 0)$.
2. $\forall x : U_{\mathbb{T}}.\ (x = 0 \Rightarrow 1 = 0) \Rightarrow (\exists y : U_{\mathbb{T}}.\ xy = 1)$.

The **generic local ring** validates:

1. $\neg\forall x : U_{\mathbb{T}}.\ \neg\neg(x = 0)$.
2. $\forall a_0, \ldots, a_{n-1} : U_{\mathbb{T}}.\ \neg\neg\exists x : U_{\mathbb{T}}.\ x^n + a_{n-1}x^{n-1} + \cdots + a_0 x^0 = 0$.
3. Let $\Delta = \{\varepsilon : U_{\mathbb{T}} \mid \varepsilon^2 = 0\}$. For any map $f : \Delta \to U_{\mathbb{T}}$, there are unique elements $a, b : U_{\mathbb{T}}$ s. th. $f(\varepsilon) = a + b\varepsilon$ for all $\varepsilon : \Delta$.

The firstly-mentioned problem on the previous page is alleviated by the Nullstellensatz presented in this talk, which gives a systematic and universal source of nongeometric sequents validated by the generic model. However, manual work is still required to reduce this set of sequents to a smaller, manageable one consisting of memorable properties while hopefully still preserving universality.

To counter the third problem, it's prudent to consider geometric theories which depend on a given mathematical object of interest. For instance, given a ring A, we can consider the theory of prime ideals of A, of complemented prime ideals, of filters, and so on. The classifying toposes of these theories are of independent interest – in fact they are sheaf toposes over certain important spaces in algebraic geometry – and nongeometric sequents validated by their generic models bundle nontrivial information about A. More details are on the following slide.

Affine schemes

Let A be a ring. Is there a **free local ring** $A \to A'$ over A?

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr] & & \underset{\text{local}}{R} \\
& \underset{\text{local}}{A'} \arrow[ur, dashed, "\text{local}"'] &
\end{tikzcd}$$

For a fixed ring R, the localisation $A' := A[S^{-1}]$ with $S := f^{-1}[R^\times]$ would do the job. (S is a *filter*.)

Hence we need the **generic filter**.

A ring is *local* iff every invertible sum contains an invertible summand, that is if $1 \neq 0$ and if $x + y$ invertible implies x invertible or y invertible. Assuming the axiom of choice, this elementary definition is equivalent to the textbook definition of a local ring (a ring with exactly one maximal ideal). A ring homomorphism is *local* iff it reflects invertibility.

The notion of a *filter* in a ring A is a direct axiomatisation of what classically would be the complement of a prime ideal. The filter axioms are: $1 \in F$, $(xy \in F) \Leftrightarrow ((x \in F) \wedge (y \in F))$, $\neg(0 \in F)$, $(x + y \in F) \Rightarrow ((x \in F) \vee (y \in F))$.

A *free local ring* over A is a homomorphism into a local ring A' such that any homomorphism into a local ring R factors uniquely over A' via a local homomorphism.

For any particular local ring $A \xrightarrow{f} R$, the localisation $A[S^{-1}]$ with $S = f^{-1}[R^\times]$ is a local ring which fits into the displayed diagram. However, in general there is no single choice of S which would work for any local ring R. Indeed, classically one can show that a free local ring over A exists if and only if A contains exactly one prime ideal, in which case A itself is the free local ring.

Affine schemes

Let A be a ring. Is there a **free local ring** $A \to A'$ over A?

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr] & & \underset{\text{local}}{R} \\ & \underset{\text{local}}{A'} \arrow[ur, dashed, "\text{local}"'] & \end{tikzcd}$$

For a fixed ring R, the localisation $A' := A[S^{-1}]$ with $S := f^{-1}[R^\times]$ would do the job. (S is a *filter*.)

Hence we need the **generic filter**.

The free local ring over A is $A^\sim := \underline{A}[F^{-1}]$, where F is the generic filter, living in $\mathrm{Spec}(A)$, the classifying topos of filters of A.

If we want a free local ring to exist for any ring A, we have to broaden our notion of existence and embrace rings which live in toposes other than Set. There is a notion of a homomorphism between rings living in arbitrary toposes, and using this notion one can verify:

The free local ring over A can be built in the classifying topos of filters of A, as the localisation (in that topos) of A at the generic filter. (More precisely, as the localisation of the mirror image of A in that topos, that is the constant sheaf $\underline{A}$.)

The classifying topos of filters of A coincides with the topos of sheaves over what's called the *spectrum of* A in algebraic geometry, and under this equivalence the free local ring coincides with the structure sheaf of spectrum. In fact the classifying topos serves as a good constructive substitute for the classical spectrum construction, enjoying the expected universal property even if the axiom of choice is not available, which is why it is simply denoted "$\mathrm{Spec}(A)$" on the slide.

(The classifying topos of prime ideals of A is also interesting; it coincides with the topos of sheaves over the spectrum of A equipped with the constructible topology.)

Affine schemes

Let A be a ring. Is there a **free local ring** $A \to A'$ over A?

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr] & & \underset{\text{local}}{R} \\
& \underset{\text{local}}{A'} \arrow[ur, dashed, "\text{local}"'] &
\end{tikzcd}$$

For a fixed ring R, the localisation $A' := A[S^{-1}]$ with $S := f^{-1}[R^\times]$ would do the job. (S is a *filter*.)

Hence we need the **generic filter**.

The free local ring over A is $A^\sim := \underline{A}[F^{-1}]$, where F is the generic filter, living in $\mathrm{Spec}(A)$, the classifying topos of filters of A.

If A is reduced ($x^n = 0 \Rightarrow x = 0$):

$A^\sim$ is a **field**: $\forall x : A^\sim.\ (\neg(\exists y : A^\sim.\ xy = 1) \Rightarrow x = 0)$.
$A^\sim$ has **¬¬-stable equality**: $\forall x, y : A^\sim.\ \neg\neg(x = y) \Rightarrow x = y$.
$A^\sim$ is **anonymously Noetherian**.

Assuming the Boolean prime ideal theorem, the geometric sequents validated by $A^\sim$ are easy to describe: They are precisely those which are validated by all the stalks $A_{\mathfrak{p}}$ of A.

But $A^\sim$ enjoys further unique properties which are not shared by the stalks of A, other localisations of A, quotients of A or indeed any reasonable construction. Three of these are displayed on the slide. (A ring is *anonymously Noetherian* iff each of its ideals is *not not* finitely generated. Textbook proofs of Hilbert's basis theorem are constructively acceptable for this Noetherian condition.)

The object $A^\sim$ strikes a fine balance: On the one hand, it is still close to A, so that information learned about $A^\sim$ teaches us about A; on the other hand, it enjoys unique properties rendering it simpler than A.

This balance allows for a simple and conceptually satisfying proof of *Grothendieck's generic freeness lemma*, an important theorem in algebraic geometry. Details can be found in this set of slides.

A systematic source of nongeometricity?

Empirical fact. In **synthetic algebraic geometry**, every known property of $\underline{\mathbb{A}}^1$ followed from its **synthetic quasicoherence**:

> *For any finitely presented $\underline{\mathbb{A}}^1$-algebra A, the canonical map*
>
> $$A \longrightarrow (\underline{\mathbb{A}}^1)^{\mathrm{Hom}_{\underline{\mathbb{A}}^1}(A,\underline{\mathbb{A}}^1)}, \quad s \longmapsto (x \mapsto x(s))$$
>
> *is an isomorphism of $\underline{\mathbb{A}}^1$-algebras.*

1. Does a general metatheorem explain this observation?
2. Is there a systematic source in any classifying topos?
3. Is there even an exhaustive source?

$$\begin{tikzcd} \mathbb{T} \text{ proves } \alpha \arrow[r, Rightarrow, bend right] & \alpha \text{ holds for } U_{\mathbb{T}} \arrow[l, bend right, "\times"'] \arrow[r, Rightarrow, bend right] & \alpha \text{ is } \mathbb{T}\text{-redundant} \arrow[l, bend right, "\times"'] \end{tikzcd}$$

Mimicking the synthetic approach to differential geometry, synthetic algebraic geometry is a framework for algebraic geometry in which schemes can be modelled by plain old sets, morphisms of schemes by plain old maps between those sets, group schemes by plain old groups, and so on. Unlike its close cousin, it is far less developed; some first steps are outlined in Sections 19 and 20 of these notes.

Synthetic algebraic geometry is carried out internally to the *big Zariski topos* of a given base scheme; in the special case that the base scheme is the terminal scheme $\mathrm{Spec}(\mathbb{Z})$, this topos is just the classifying topos of local rings. The relevant generic model living in the big Zariski topos is denoted "$\underline{\mathbb{A}}^1$" because it coincides with the functor of points of the affine line.

A systematic source of nongeometricity?

> A. Kock has pointed out [5 (ii)] that the generic local ring satisfies the nongeometric sentence
>
> $$\forall x_1 \ldots \forall x_n . (\neg(\bigwedge_i (x_i = 0)) \to \bigvee_i (\exists y.\, x_i y = 1))$$
>
> which in classical logic defines a field! The problem of characterising all the nongeometric properties of a generic model appears to be difficult. If the generic model of a geometric theory T satisfies a sentence α then any geometric consequence of $T+(\alpha)$ has to be a consequence of T. We might call α T-redundant. Does the generic T-model satisfy all T-redundant sentences?

Gavin Wraith. *Some recent developments in topos theory.*
In: Proc. of the ICM (Helsinki, 1978).

1. Does a general metatheorem explain this observation?
2. Is there a systematic source in any classifying topos?
3. Is there even an exhaustive source?

$$\mathbb{T}\text{ proves }\alpha \;\Longrightarrow\; \alpha\text{ holds for }U_{\mathbb{T}} \;\Longrightarrow\; \alpha\text{ is }\mathbb{T}\text{-redundant}$$

Mimicking the synthetic approach to differential geometry, synthetic algebraic geometry is a framework for algebraic geometry in which schemes can be modelled by plain old sets, morphisms of schemes by plain old maps between those sets, group schemes by plain old groups, and so on. Unlike its close cousin, it is far less developed; some first steps are outlined in Sections 19 and 20 of these notes.

Synthetic algebraic geometry is carried out internally to the *big Zariski topos* of a given base scheme; in the special case that the base scheme is the terminal scheme $\mathrm{Spec}(\mathbb{Z})$, this topos is just the classifying topos of local rings. The relevant generic model living in the big Zariski topos is denoted "$\underline{\mathbb{A}}^1$" because it coincides with the functor of points of the affine line.

Marc Bezem, Ulrik Buchholtz and Thierry Coquand answered in their 2017 paper Syntactic forcing models for coherent logic Gavin Wraith's question in the negative. (As Thierry remarked during the talk, this is even if one takes care to phrase the question in a way to exclude the trivial counterexamples given by instances of the law of excluded middle in the language of $\mathbb{T}$.) If the answer had been positive, this would have given a neat, if somewhat hard to use in practice, characterisation of the formulas validated by the generic model.

A systematic source of nongeometricity?

Empirical fact. In **synthetic algebraic geometry**, every known property of $\underline{\mathbb{A}}^1$ followed from its **synthetic quasicoherence**:

For any finitely presented $\underline{\mathbb{A}}^1$-algebra A, the canonical map

$$A \longrightarrow (\underline{\mathbb{A}}^1)^{\mathrm{Hom}_{\underline{\mathbb{A}}^1}(A,\underline{\mathbb{A}}^1)}, \quad s \longmapsto (x \mapsto x(s))$$

is an isomorphism of $\underline{\mathbb{A}}^1$-algebras.

1. Does a general metatheorem explain this observation?
2. Is there a systematic source in any classifying topos?
3. Is there even an exhaustive source?

$$\begin{tikzcd} \mathbb{T}\text{ proves }\alpha \arrow[r, Rightarrow, bend right] & \alpha\text{ holds for }U_{\mathbb{T}} \arrow[l, bend right, "\times"'] \arrow[r, Rightarrow, bend right] & \alpha\text{ is }\mathbb{T}\text{-redundant} \arrow[l, bend right, "\times"'] \end{tikzcd}$$

The topos-theoretic *Nullstellensatz*, to be presented on the next slides, answers the displayed three questions in the affirmative.

Briefly, the Nullstellensatz is a certain statement in the language of a given geometric theory $\mathbb{T}$ which is

- validated by the generic $\mathbb{T}$-model,
- typically not validated by other $\mathbb{T}$-models, and
- such that any statement validated by the generic $\mathbb{T}$-model can be deduced, in intuitionistic logic, from the axioms of $\mathbb{T}$ and the Nullstellensatz.

We believe that this characterisation is as explicit as it can get, but would be delighted to be surprised by a future improvement. We stumbled on it by playing with the synthetic quasicoherence statement, not least thanks to encouragement by Alexander Oldenziel. However the route from that statement to the Nullstellensatz is not quite direct; it turns out that synthetic quasicoherence is a corollary of a specialisation of a higher-order version of the Nullstellensatz to Horn theories.

A topos-theoretic Nullstellensatz

Theorem. Internally to $\mathrm{Set}[\mathbb{T}]$:

> *For any geometric* sequent σ over the signature of $\underline{\mathbb{T}}/U_{\mathbb{T}}$, if σ holds for $U_{\mathbb{T}}$, then $\underline{\mathbb{T}}/U_{\mathbb{T}}$ proves σ.*

By $\underline{\mathbb{T}}$ we mean the geometric theory internal to $\mathrm{Set}[\mathbb{T}]$ obtained by pulling back the set of sorts of $\mathbb{T}$, the set of function symbols and so on along the unique geometric morphism $\mathrm{Set}[\mathbb{T}] \to \mathrm{Set}$. For instance, if $\mathbb{T}$ is the theory of rings, then from the internal point of view of $\mathrm{Set}[\mathbb{T}]$, the theory $\underline{\mathbb{T}}$ will again be the theory of rings.

The theory $\underline{\mathbb{T}}/U_{\mathbb{T}}$ will be defined on the next slide. It is a certain geometric theory internal to $\mathrm{Set}[\mathbb{T}]$.

The asterisks in *geometric* sequent* and *provability** indicate that any infinities used to index disjunctions have to be come from the base topos. This restriction is an important subtlety, though not vital to this talk. If $\mathbb{T}$ is a coherent theory, then for coherent sequents there is no difference between provability in coherent logic, provability in geometric logic and provability*.

A topos-theoretic Nullstellensatz

Theorem. Internally to $\mathrm{Set}[\mathbb{T}]$:

> *For any geometric* sequent σ over the signature of $\underline{\mathbb{T}}/U_{\mathbb{T}}$, if σ holds for $U_{\mathbb{T}}$, then $\underline{\mathbb{T}}/U_{\mathbb{T}}$ proves σ.*

The algebraic Nullstellensatz. Let A be a ring. Let $f, g \in A[X]$ be polynomials. Then, subject to some conditions:

$$\underbrace{\big(\forall x \in A.\, (f(x) = 0 \Rightarrow g(x) = 0)\big)}_{\text{algebraic truth}} \Longrightarrow \underbrace{\big(\exists h \in A[X].\, g = hf\big)}_{\text{algebraic certificate}}$$

By $\underline{\mathbb{T}}$ we mean the geometric theory internal to $\mathrm{Set}[\mathbb{T}]$ obtained by pulling back the set of sorts of $\mathbb{T}$, the set of function symbols and so on along the unique geometric morphism $\mathrm{Set}[\mathbb{T}] \to \mathrm{Set}$. For instance, if $\mathbb{T}$ is the theory of rings, then from the internal point of view of $\mathrm{Set}[\mathbb{T}]$, the theory $\underline{\mathbb{T}}$ will again be the theory of rings.

The theory $\underline{\mathbb{T}}/U_{\mathbb{T}}$ will be defined on the next slide. It is a certain geometric theory internal to $\mathrm{Set}[\mathbb{T}]$.

The asterisks in *geometric* sequent* and *provability** indicate that any infinities used to index disjunctions have to be come from the base topos. This restriction is an important subtlety, though not vital to this talk. If $\mathbb{T}$ is a coherent theory, then for coherent sequents there is no difference between provability in coherent logic, provability in geometric logic and provability*.

The algebraic Nullstellensatz states that, in some cases, algebraic truths are witnessed by explicit *algebraic certificates* – syntactical objects giving a priori reasons for why a given truth is to be expected.

In the topos-theoretic Nullstellensatz, algebraic truths are replaced by arbitrary truths of the generic model, subject only to the condition that they can be expressed as a geometric sequent, and algebraic certificates are replaced by *logical certificates*: proofs.

A topos-theoretic Nullstellensatz

Theorem. Internally to $\mathrm{Set}[\mathbb{T}]$:

> *For any geometric* sequent σ over the signature of $\underline{\mathbb{T}}/U_{\mathbb{T}}$, if σ holds for $U_{\mathbb{T}}$, then $\underline{\mathbb{T}}/U_{\mathbb{T}}$ proves σ.*

The algebraic Nullstellensatz. Let A be a ring. Let $f, g \in A[X]$ be polynomials. Then, subject to some conditions:

$$\underbrace{\big(\forall x \in A.\, (f(x) = 0 \Rightarrow g(x) = 0)\big)}_{\text{algebraic truth}} \Longrightarrow \underbrace{\big(\exists h \in A[X].\, g = hf\big)}_{\text{algebraic certificate}}$$

A naive version. "Internally to $\mathrm{Set}[\mathbb{T}]$, for any geometric sequent σ over the signature of $\underline{\mathbb{T}}$, if σ holds for $U_{\mathbb{T}}$, then $\underline{\mathbb{T}}$ proves σ." **False,** for instance with the theory of rings we have

$$\begin{array}{ll} & \mathrm{Set}[\mathbb{T}] \models \neg(\ulcorner \underline{\mathbb{T}} \text{ proves } (\top \vdash 1 + 1 = 0)\urcorner) \\ \text{but} & \mathrm{Set}[\mathbb{T}] \not\models \neg(1 + 1 = 0). \end{array}$$

While, as stated on slide 1/20, the generic model $U_{\mathbb{T}}$ is a conservative $\mathbb{T}$-model, the classifying topos $\mathrm{Set}[\mathbb{T}]$ does not believe this fact. That is, the statement "$U_{\mathbb{T}}$ is a conservative $\underline{\mathbb{T}}$-model" is not true internally to $\mathrm{Set}[\mathbb{T}]$. What is true is the modified statement "$U_{\mathbb{T}}$ is a conservative* $\underline{\mathbb{T}}/U_{\mathbb{T}}$-model".

A varying internal theory

Theorem. Internally to $\mathrm{Set}[\mathbb{T}]$:

For any geometric* sequent σ over the signature of $\mathbb{T}/U_{\mathbb{T}}$, if σ holds for $U_{\mathbb{T}}$, then $\mathbb{T}/U_{\mathbb{T}}$ proves σ.

Definition. The theory $\mathbb{T}/U_{\mathbb{T}}$ is the internal geometric theory of **$U_{\mathbb{T}}$-algebras**, the theory which arises from $\mathbb{T}$ by adding:

1. for each element $x : U_{\mathbb{T}}$ a constant symbol e_x,
2. for each function symbol f and n-tuple $(x_1, \ldots, x_n) \in (U_{\mathbb{T}})^n$ the axiom $(\top \vdash f(e_{x_1}, \ldots, e_{x_n}) = e_{f(x_1,\ldots,x_n)})$,
3. for each relation symbol R and n-tuple $(x_1, \ldots, x_n) \in (U_{\mathbb{T}})^n$ such that $R(x_1, \ldots, x_n)$ the axiom $(\top \vdash R(e_{x_1}, \ldots, e_{x_n}))$.

Just as locales internal to a topos $\mathcal{E}$ can be externalized to yield localic geometric morphisms into $\mathcal{E}$, internal Grothendieck toposes can be externalized to yield bounded geometric morphisms. Since the composition of bounded geometric morphisms is bounded, the externalisation of a Grothendieck topos internally to a Grothendieck topos is itself a Grothendieck topos, hence the classifying topos of some geometric theory.

Constructing internally to $\mathrm{Set}[\mathbb{T}]$, where $\mathbb{T}/U_{\mathbb{T}}$ is just an ordinary geometric theory, the classifying topos of that theory, and then externalising the resulting Grothendieck topos results in the classifying topos of $\mathbb{T}$-homomorphisms. There are two canonical geometric morphisms from this topos to $\mathrm{Set}[\mathbb{T}]$, the morphism computing the domain and the morphism computing the codomain, and the morphism obtained by the externalisation procedure is the former.

Revisiting the test cases

Theorem. Internally to $\mathrm{Set}[\mathbb{T}]$:

> *For any geometric* sequent σ over the signature of $\underline{\mathbb{T}}/U_{\mathbb{T}}$, if σ holds for $U_{\mathbb{T}}$, then $\underline{\mathbb{T}}/U_{\mathbb{T}}$ proves σ.*

In the object classifier. Let $x, y : U_{\mathbb{T}}$. Assume that $\neg(x = y)$. By the Nullstellensatz $\underline{\mathbb{T}}/U_{\mathbb{T}}$ proves $(e_x = e_y \vdash \bot)$. But this is false in the $\underline{\mathbb{T}}/U_{\mathbb{T}}$-model $U_{\mathbb{T}}/(x \sim y)$.

In the ring classifier. Let $f, g : U_{\mathbb{T}}[X]$ such that any zero of f is a zero of g. By the Nullstellensatz $\underline{\mathbb{T}}/U_{\mathbb{T}}$ proves this fact. Hence it holds in the $\underline{\mathbb{T}}/U_{\mathbb{T}}$-model $U_{\mathbb{T}}[X]/(f)$. In this model f has the zero $[X]$. Hence also $g([X]) = 0$ in $U_{\mathbb{T}}[X]/(f)$, that is $g = hf$ for some $h : U_{\mathbb{T}}[X]$.

This slide gives two examples how to use the Nullstellensatz to deduce properties of the generic model. A couple of remarks are in order.

The Nullstellensatz is trivial for sequents σ of the form $(\top \vdash \psi)$. The Nullstellensatz is only interesting in case that σ has a nontrivial antecedent or is set in a nonempty context.

Since the converse direction in the Nullstellensatz also holds (because $U_{\mathbb{T}}$ is a $\underline{\mathbb{T}}/U_{\mathbb{T}}$-model), the statements $\ulcorner\sigma$ holds for $U_{\mathbb{T}}\urcorner$ and $\ulcorner\underline{\mathbb{T}}/U_{\mathbb{T}}$ proves* $\sigma\urcorner$ are equivalent. This equivalence is intriguing from a logical point of view, since the former statement is a geometric implication while the latter can be put as a geometric formula. (Up to a subtle issue indicated on the next slide.)

To apply the Nullstellensatz, no description of a site defining $\mathrm{Set}[\mathbb{T}]$ is required.

Often when using the Nullstellensatz, we go from an (assumed) truth of $U_{\mathbb{T}}$ via provability* to another model M of $\underline{\mathbb{T}}/U_{\mathbb{T}}$. That is, we use provability* as a (one-way) *bridge*:

$$\begin{tikzcd}
 & \underline{\mathbb{T}}/U_{\mathbb{T}} \text{ proves}^\star\ \sigma \arrow[dr, Rightarrow, bend left] & \\
\sigma \text{ holds for } U_{\mathbb{T}} \arrow[ur, Leftarrow, bend left] & & \sigma \text{ holds for } M
\end{tikzcd}$$

Exhaustion and extensions

Theorem 1. A first-order formula holds for $U_{\mathbb{T}}$ iff it is intuitionistically provable from the axioms of $\mathbb{T}$ and the scheme

$$\ulcorner \sigma \text{ holds} \urcorner \implies \ulcorner \mathbb{T}/U_{\mathbb{T}} \text{ proves } \sigma \urcorner. \qquad \text{(Nullstellensatz)}$$

Theorem 2. Let $\mathbb{T}'$ be a quotient theory of $\mathbb{T}$. Assume that $U_{\mathbb{T}}$ is a sheaf for the topology cutting out $\mathrm{Set}[\mathbb{T}']$. Then internally to $\mathrm{Set}[\mathbb{T}']$:

> *A geometric** *sequent σ with Horn consequent holds for $U_{\mathbb{T}'}$ iff $\mathbb{T}/U_{\mathbb{T}}$ proves σ.*

Theorem 3. A higher-order formula holds for $U_{\mathbb{T}}$ iff it is provable in intuitionistic higher-order logic from the axioms of $\mathbb{T}$ and the higher-order Nullstellensatz scheme.

Theorem 1 states that the source provided by the Nullstellensatz is exhaustive. The notion of provability** is a strengthening of the notion of provability*, which in turn is a strengthening of the ordinary notion of provability in geometric logic. We are using it here because while the notion of provability* can be expressed in the internal language of a topos, it cannot be expressed in intuitionistic logic.

Theorem 2 provides a useful variant of the Nullstellensatz. Its assumptions are for instance satisfied if $\mathbb{T}$ is the theory of rings and $\mathbb{T}'$ is the theory of local rings. When applicable, it can be used to avoid doubly-internal toposes. It also explains, for instance, why in the formulation of synthetic quasicoherence no local rings appear even though the relevant topos is the classifying topos of local rings.

Theorems 3 and 4 generalize the Nullstellensatz to the higher-order setting. The map ev maps (the equivalence class of) a $\mathbb{T}/U_{\mathbb{T}}$-provably* geometric* formula θ in one free variable to the subset $\{x : U_{\mathbb{T}} \mid \theta(x)\}$.

Written details on all of this are slowly emerging.

Exhaustion and extensions

Theorem 1. A first-order formula holds for $U_{\mathbb{T}}$ iff it is intuitionistically provable from the axioms of $\mathbb{T}$ and the scheme

$$\ulcorner \sigma \text{ holds} \urcorner \implies \ulcorner \mathbb{T}/U_{\mathbb{T}} \text{ proves } \sigma \urcorner. \qquad \text{(Nullstellensatz)}$$

Theorem 2. Let $\mathbb{T}'$ be a quotient theory of $\mathbb{T}$. Assume that $U_{\mathbb{T}}$ is a sheaf for the topology cutting out $\mathrm{Set}[\mathbb{T}']$. Then internally to $\mathrm{Set}[\mathbb{T}']$:

> *A geometric** *sequent σ with Horn consequent holds for $U_{\mathbb{T}'}$ iff $\mathbb{T}/U_{\mathbb{T}}$ proves σ.*

Theorem 3. A higher-order formula holds for $U_{\mathbb{T}}$ iff it is provable in intuitionistic higher-order logic from the axioms of $\mathbb{T}$ and the higher-order Nullstellensatz scheme.

The Nullstellensatz is related to several precursors. A corollary of the Nullstellensatz is that, over the first-order theory validated by $U_{\mathbb{T}}$, any first-order formula is in fact logically equivalent to a geometric formula. This corollary has already been observed by Carsten Butz and Peter Johnstone in their paper Classifying toposes for first-order theories (Lemma 4.2 there). At that point, a characterisation of the first-order formulas in the general case, of the form as in Theorem 1, was still missing.

Theorem 3 is a relativisation of Olivia Caramello's completeness theorem, Theorem 2.4(ii) in her paper Universal models and definability. The passage from the external to the internal phrasing requires going from $\mathbb{T}$ to $\mathbb{T}/U_{\mathbb{T}}$.

Plans for the future include:

- Developing an Agda library for dealing with the internal language of toposes and related kinds of categories, employing Agda's metaprogramming facilities; with such a library at hand, formalising the Nullstellensatz in Agda.
- Exploring Nullstellensatz-style results for arithmetic universes.
- Applying the Nullstellensatz in constructive algebra and algebraic geometry, along the lines of generic freeness and synthetic algebraic geometry. Most of the toposes in geometric use are actually uncharted territory from a logical point of view.