QUASICOHERENT NOTES ON SHEAVES AND LOGIC

INGO BLECHSCHMIDT

Rough notes, use with care.
Comments are very much welcome at
ingo.blechschmidt@math.uni-augsburg.de.
Merge requests can be submitted on GitLab.

Abstract. Exactly which information does a proof of a statement tell us besides that the proved statement is true? What do we gain if we refrain from using the axiom "any statement is either true or false"?

In this course, we consider mathematical proofs as objects in their own right and study them from a higher point of view. To this end, we employ Gentzen's calculus of natural deduction to formalize informal arguments. This allows us to analyze on which logical principles given proofs are based on.

We study intuitionistic logic, where we don't use the law of excluded middle ("any statement is true or not true"), and discuss Gödel's incompleteness theorem, which to a zeroth approximation states that there are true statements which cannot be proved.

We then treat realizability theory, which connects logic with computability theory. It provides a context in which certain anti-classical statements hold: for instance that any function $\mathbb{R} \to \mathbb{R}$ is continuous. We utilize this to conduct *proof mining*: extract from given proofs additional information like upper bounds. This will be illustrated with applications in analysis and numerical analysis.

In the last part of the course, we explore the internal language of toposes, alternate mathematical universes in which not the usual laws of logic hold. We learn how we can profitably employ these toposes in algebra and geometry, and will also briefly touch upon the effective topos, which is in some sense a reification of realizability theory and provides a setting to study higher-order computability theory.

Contents

Acknowledgments

I'm grateful to all the local and remote participants of the course for their many questions and suggestions. In particular I'm grateful to asdfusername from the Matheplanet, Tobias Land, and Leopold Schlicht for correcting several errors in older versions of these notes. I'm grateful to Tim Baumann, who among other things contributed the full text of a section of these notes.

1. Basics

"The idea of the internal language of a category or higher category is not quite as scary as you're making it sound. It's just the language you'd speak if you lived there." at https://golem.ph.utexas.edu/category/2017/11/internal_languages_of_higher_c_1.html#c053066

Mention "∃!" as syntactic sugar

Define PRA using mapping recipes instead of primitive-recursive functions and explain why
Explain which metatheory is used
spectrum of finitism
xxx (translate from the pizza seminar notes)
Diaconescu (AxC implies LEM)

1.1. Gentzen's calculus of natural deduction.

signature
term
formula
sequent
theory
ex: Heyting Arithmetic
ex: proof that $1 + 1 = 2$ in HA

1.2. Local operators.

Definition 1.1. A *local operator* is a mapping $\varphi \mapsto \nabla\varphi$ from formulas to formulas such that for all formulas φ and ψ it holds that

(1) $\top \vdash \varphi \implies \nabla\varphi$
(2) $\top \vdash \nabla(\nabla\varphi) \implies \nabla\varphi$
(3) $\top \vdash \nabla(\varphi \wedge \psi) \iff (\nabla\varphi) \wedge (\nabla\psi)$

Say that $\nabla\varphi$ has to be given by a syntactic construction. It may not be an arbitrary mapping of formulas.

We could be more general and demand that the axioms are only provable modulo a background theory T.

The interpretation of the first axiom is that ∇ weakens a formula. The second axiom then says that weakening twice is the same as weakening once. (Note that $\nabla\varphi \implies \nabla(\nabla\varphi)$ is an instance of the first axiom, hence $\nabla(\nabla\varphi) \iff \nabla\varphi$ holds.)

Example 1.2. The following are all local operators:

$$\begin{array}{lll} \nabla\varphi :\equiv (\varphi \vee \alpha) & & \text{for a fixed formula } \alpha, \\ \nabla\varphi :\equiv (\beta \implies \varphi) & & \text{for a fixed formula } \beta, \\ \nabla\varphi :\equiv ((\varphi \implies \lambda) \implies \lambda) & & \text{for a fixed formula } \lambda. \end{array}$$

Example 1.3. For $\lambda \equiv \bot$ we get an important special case: $\nabla\varphi :\equiv \neg\neg\varphi$.

Later, when studying the internal language of toposes, we will see how to interpret local operators geometrically: Instead of requiring that φ holds everywhere, $\nabla\varphi$ says that φ holds on some smaller subspace. For example, $\neg\neg\varphi$ can be interpreted as: "φ holds on a dense open subspace". This justifies the use of the adjective "local".

Definition 1.4. Let ∇ be a local operator. The ∇-translation φ^∇ of a formula φ is defined recursively as follows (where all $\triangledown$ in gray should be ignored):

$$\begin{aligned}
(f = g)^\nabla &:\equiv \nabla(f = g) \\
\top^\nabla &:\equiv \triangledown\top \quad (\Leftrightarrow \top) \\
\bot^\nabla &:\equiv \nabla\bot \\
(\varphi \wedge \psi)^\nabla &:\equiv \triangledown(\varphi^\nabla \wedge \psi^\nabla) \\
(\varphi \vee \psi)^\nabla &:\equiv \nabla(\varphi^\nabla \vee \psi^\nabla) \\
(\varphi \Rightarrow \psi)^\nabla &:\equiv \triangledown(\varphi^\nabla \Rightarrow \psi^\nabla) \\
(\forall x : X.\ \varphi)^\nabla &:\equiv \triangledown(\forall x : X.\ \varphi^\nabla) \\
(\exists x : X.\ \varphi)^\nabla &:\equiv \nabla(\exists x : X.\ \varphi^\nabla)
\end{aligned}$$

Lemma 1.5. *Let Σ be a signature. Let ∇ be a local operator over Σ and let φ be a formula over Σ. Then the sequents*

(a) $\nabla(\varphi^\triangledown) \vdash_{\vec{x}} \varphi^\triangledown$ *and* (b) $\varphi^\nabla \dashv\vdash_{\vec{x}} \varphi^\triangledown$,

where $\varphi^\triangledown$ (note the gray color!) is defined like φ^∇ by the equations of Definition 1.4, but not ignoring the gray $\triangledown$'s, are derivable using only the standard rules of Gentzen's calculus of natural deduction.

Definition 1.6. A formula φ is called *geometric* if and only if it consists only of the following logical symbols and connectives:

$$= \quad \top \quad \bot \quad \wedge \quad \vee \quad \exists$$

A geometric formula may not contain $\forall$-quantification or "$\Rightarrow$" (and therefore also no negations, since $\neg\psi \equiv (\psi \Rightarrow \bot)$).

Proposition 1.7. *Let ∇ be a local operator over a signature Σ. Let T be a theory over Σ.*

(a) *Suppose that $\varphi \vdash_{\vec{x}} \psi$ is derivable in T. Then $\varphi^\nabla \vdash_{\vec{x}} \psi^\nabla$ is derivable in T^∇, where the theory T^∇ has the same function and relation symbols as T, but every axiom $\alpha \vdash_{\vec{x}} \beta$ of T has been replaced by $\alpha^\nabla \vdash_{\vec{x}} \beta^\nabla$.*

(b) *Let φ be a geometric formula. Then $\varphi^\nabla \dashv\vdash_{\vec{x}} \nabla\varphi$ is derivable using only the standard rules of Gentzen's calculus.*

Proof. TODO □

Proposition 1.8. *If (1)–(3) of Definition 1.1 and additionally $\nabla\bot \vdash_{\vec{x}} \nabla\varphi$ are derivable in T using minimal logic for all formulas φ and ψ, then the following stronger statement holds:*

(a)' *If $\varphi \vdash_{\vec{x}} \psi$ is derivable in T using intuitionistic logic, then $\varphi^\nabla \vdash_{\vec{x}} \psi^\nabla$ is derivable in T^∇ using minimal logic.*

Proof. TODO □

Remark 1.9. The proposition applies to $\nabla \equiv \neg\neg$. For $\nabla\varphi \equiv \varphi \vee \alpha$ the result also holds, provided that one uses a variant of the ∇-translation where the $\bot$-case is defined by $\bot^\nabla :\equiv \alpha$ instead of $\nabla\bot \equiv \bot \vee \alpha$. This is necessary since $\alpha \vee \bot \dashv\vdash \alpha$ is derivable in intuitionistic logic but generally not in minimal logic.

Proposition 1.10. *For $\nabla = \neg\neg$ an even stronger statement holds:*

(a)" *If $\varphi \vdash_{\vec{x}} \psi$ is derivable in T using* classical *logic, then $\varphi^\nabla \vdash_{\vec{x}} \psi^\nabla$ is derivable in $T^{\neg\neg}$ using minimal logic.*

Theorem 1.11. *Let φ and ψ be geometric formulas. Assume that $\varphi \vdash_{\vec{x}} \psi$ is derivable in T using classical logic. Then $\varphi \vdash_{\vec{x}} \psi$ is derivable in $(T^{\neg\neg})^\nabla$ using intuitionistic logic (with $\nabla :\equiv \_ \vee \psi$).*

Proof. From the classical derivability of $\varphi \vdash_{\vec{x}} \psi$ in T it follows by Proposition 1.10 that $\varphi^{\neg\neg} \vdash_{\vec{x}} \psi^{\neg\neg}$ is derivable in $T^{\neg\neg}$ using intuitionistic logic. Since φ and ψ are geometric, we get $\neg\neg\varphi \vdash_{\vec{x}} \neg\neg\psi$ in $T^{\neg\neg}$ using part (b) of Proposition 1.7 for both φ and ψ. Hence $\varphi \vdash_{\vec{x}} \neg\neg\psi$ in $T^{\neg\neg}$.

Now we use what is called "Friedman's trick": By applying another (later cleverly chosen) local operator ∇ with Proposition 1.7(a) we get $\varphi^\nabla \vdash_{\vec{x}} (\neg\neg\psi)^\nabla$ in $(T^{\neg\neg})^\nabla$ using intuitionistic logic. Therefore $\varphi \vdash_{\vec{x}} (\neg\neg\psi)^\nabla$ by Proposition 1.7(b) and axiom (1) of Definition 1.1. But for $\nabla :\equiv \_ \vee \psi$

$$\begin{array}{lll} (\neg\neg\psi)^\nabla & \equiv & (\psi^\nabla \implies \bot^\nabla) \implies \bot^\nabla \\ & \dashv\vdash_{\vec{x}} & (\nabla\psi \implies \bot^\nabla) \implies \bot^\nabla \\ & \dashv\vdash_{\vec{x}} & (\psi \vee \psi \implies \psi) \implies \psi \\ & \dashv\vdash_{\vec{x}} & \psi \end{array}$$

in $T^{\neg\neg}$ using intuitionistic logic. □

Corollary 1.12. *Let φ and ψ be geometric formulas in* HA. *Then $\varphi \vdash_{\vec{x}} \psi$ modulo* PA, *classically, if and only if $\varphi \vdash_{\vec{x}} \psi$ modulo* HA, *intuitionistically.*

Proof. Assume that the sequent $\varphi \vdash_{\vec{x}} \psi$ is derivable using the standard rules of Gentzen's calculus, the axioms of Peano arithmetic, and the law of excluded middle. Then we get from Theorem 1.11 that $\varphi \vdash_{\vec{x}} \psi$ is derivable modulo $(\mathrm{HA}^{\neg\neg})^\nabla$. One can show that every axiom of $(\mathrm{HA}^{\neg\neg})^\nabla$ is derivable in HA. do this for the induction axiom Therefore $\varphi \vdash_{\vec{x}} \psi$ modulo HA. □

Proposition 1.13. *Let φ be a formula such that $\alpha^\nabla \vdash_{\vec{x}} \nabla\alpha$ is derivable for every antecedent α of an implication $\alpha \Rightarrow \beta$ that is contained in φ. Then $\nabla\varphi \vdash_{\vec{x}} \varphi^\nabla$ is derivable.*

Proof. TODO □

2. Gentzen's consistency proof of Peano arithmetic

The goal of this section is to explain the following four theorems. Formulas will always refer to formulas over the signature of Heyting (or Peano) arithmetic $(N, 0, s, +, \cdot)$.

Theorem 2.1. *Sufficiently infinitary systems show that Heyting arithmetic is consistent.*

Theorem 2.2. $\mathrm{PRA} + \text{QF-TI}(\varepsilon_0)$ *shows that Heyting arithmetic is consistent.*

Theorem 2.3. *For any ordinal number $\alpha < \varepsilon_0$, Heyting arithmetic shows* $\mathrm{TI}(\alpha)$.

Theorem 2.4. $\mathrm{PRA} + \text{QF-TI}(\varepsilon_0)$ *shows that Heyting arithmetic doesn't show* $\text{QF-TI}(\varepsilon_0)$.

We haven't yet discussed how we can express statements like the consistency of Heyting arithmetic in a weak system like PRA in which we don't even have quantifiers at our disposal. We'll later have to review our proofs of Theorem 2.2 and Theorem 2.4 to see that they can indeed be formalized. The meaning of QF-TI and TI will be explained below.

Proof of Theorem 2.1. In a sufficiently infinitary system, we can define by recursion on the structure of a formula of Heyting arithmetic what it means for a formula to be *true*:

$$\begin{aligned} \top &\quad\text{is true if and only if}\quad 1 = 1, \\ \bot &\quad\text{is true if and only if}\quad 1 = 0, \\ \varphi \wedge \psi &\quad\text{is true if and only if}\quad \varphi \text{ is true and } \psi \text{ is true}, \\ \forall x : N.\ \varphi &\quad\text{is true if and only if}\quad \varphi[\underline{n}/x] \text{ is true for all } n \in \mathbb{N}, \end{aligned}$$

and so on. (We'll see that such a definition is not possible in a system like PA, though we can define, for each numeral n, a predicate True_n such that $\mathrm{True}_n(\ulcorner\varphi\urcorner)$ expresses that φ is true for all formulas φ of length less than n.)

We can then prove by induction on the structure of a derivation that for any provable sequent $\varphi \vdash_{\vec{x}} \psi$, truth of φ implies truth of ψ (for all values of the free variables).

Hence, if Heyting arithmetic proves $\top \vdash \bot$, then $1 = 1$ implies $1 = 0$. Therefore the assumption that Heyting arithmetic is inconsistent leads to a contradiction, that is, Heyting arithmetic is consistent. □

Include interlude on ordinal numbers. Also spell out the finitary definition of ordinal numbers up to ε_0 using Cantor normal form.

Definition 2.5. Let $(\prec)$ be a relation symbol for a relation on $N \times N$. By $\mathrm{TI}(\prec)$ ("$(\prec)$-induction") we mean the formula

$$\big(\forall n : N.\ (\forall m : N.\ m \prec n \Rightarrow P(m)) \Rightarrow P(n)\big) \Longrightarrow \big(\forall n : N.\ P(n)\big)$$

in the language of arithmetic enriched by a predicate symbol P. We say that a formal system S over the signature of arithmetic satisfies $\mathrm{TI}(\prec)$ if $\mathrm{TI}(\prec)$ is derivable in the system S extended by this predicate symbol P but without any axioms governing P.

If α is an ordinal number for which we have settled on some canonical representation by a formula of arithmetic in two free variables, written $x \prec y$, then we mean by $\mathrm{TI}(\alpha)$ the formula $\mathrm{TI}(\prec)$.[1] As is often the case in mathematical logic, the same intuitive concept (an order type) can be formalized in different ways (by different formulas representing the order type). Depending on the strength of the studied system, these different ways might turn out to not be equivalent. Consider, for instance, the following contrived example (from [?]):

Example 2.6. WIP, doesn't look right Set $x \prec y$ if and only if $x < y$ and there is no PA-proof of $\bot$ of length less than x. In a sufficiently infinistic metatheory, this order represents the same order type as the usual order does, the first infinite ordinal ω. However, it's unreasonable to expect that PA verifies $\mathrm{TI}(\prec)$.

[1] Formally, this is the result of substituting in $\mathrm{TI}(R)$ for R the formula $(\prec)$.

Theorem 2.3 shows that Heyting arithmetic verifies transfinite induction up to any ordinal less than ε_0. Regarding the logical setup, the following two propositions are therefore redundant. They're included here because their proofs are instructive.

Proposition 2.7. *Heyting arithmetic verifies* $\mathrm{TI}(\omega)$.

Proof. The total order representing ω is, by convention, the usual order. In the language enriched by a predicate symbol P, we are to show that $P(n)$ holds for all numbers given that

$$\forall n : N.\ (\forall m : N.\ m < n \Rightarrow P(m)) \Longrightarrow P(n). \tag{$\star$}$$

To this end, we use ordinary induction to verify that

$$\forall n : N.\ \forall m : N.\ m < n \Rightarrow P(m).$$

The base case $n = 0$ is trivial, since given $m < 0$ we may deduce $\bot$ and therefore $P(m)$. To verify the induction step $n \to s(n)$, let $m < s(n)$ be given. Then $m < n$ or $m = n$. In the first case, the claim $P(m)$ follows by the induction hypothesis. In the second case, the claim follows by combining assumption ($\star$) and the induction hypothesis. □

Proposition 2.8. *Heyting arithmetic verifies* $\mathrm{TI}(\omega \cdot 2)$.

Proof. To represent the ordinal $\omega \cdot 2$ in Heyting arithmetic, we define an order $\prec$ by

$$\begin{aligned} m \prec n :\equiv\ & (\mathrm{Even}(m) \wedge \mathrm{Odd}(n)) \vee \\ & (m < n \wedge ((\mathrm{Even}(n) \wedge \mathrm{Even}(m)) \vee (\mathrm{Odd}(n) \wedge \mathrm{Odd}(m)))). \end{aligned}$$

where we us the abbreviations $\mathrm{Even}(t) :\equiv (\exists k : N.\ 2k = t)$ and $\mathrm{Odd}(t) :\equiv (\exists k : N.\ 2k + 1 = t)$. We show, in the language extended by a predicate symbol P, that $P(n)$ holds for all n under the assumption

$$\forall n : N.\ (\forall m : N.\ m \prec n \Rightarrow P(m)) \Longrightarrow P(n). \tag{$\star\star$}$$

We start by showing $P(2a)$ for all numbers a, utilizing transfinite induction up to ω. So let a be arbitrary such that $P(2b)$ holds for all $b < a$, we are to show that $P(2a)$. We want to verify $P(2a)$ using ($\star\star$). Let therefore m be arbitrary such that $m \prec 2a$. We are to show that $P(2m)$. Since $m \prec 2a$, there exists a number b such that $m = 2b$ and $b < a$. Thus $P(2b)$ by the outer inductive hypothesis.

Next we show $P(2a + 1)$ for all numbers a, again using transfinite induction up to ω. Let a be arbitrary such that $P(2b + 1)$ holds for all $b < a$. We have to show that $P(2a + 1)$. To show that the antecedent of ($\star\star$) holds for $n = 2a + 1$ and let m be arbitrary with $m \prec 2a + 1$. Then there exists a number b such that either $m = 2b$ or $m = 2b + 1$. In the first case, we get $P(2b)$ from the statement proven by our first induction. In the second case we also have $b < a$, therefore the induction hypothesis gives us $P(2b + 1)$.

Finally, since we can write an arbitrary number n as $n = 2a$ or as $n = 2a + 1$, we get $P(n)$ from the statement proven by the first or second induction. □

Proof of Theorem 2.3. We define a family of orders $(\prec_r)$ by recursion on r:

$$\begin{aligned} x \prec_0 y &:\equiv x < y \\ x \prec_{r+1} y &:\equiv y \neq 0 \wedge \big(x = 0 \vee \exists i : N.\ (i \leq y \wedge \nu(x,i) < \nu(y,i) \wedge \\ &\qquad \forall j : N.\ j \leq \max\{x,y\} \wedge i \prec_r j \Rightarrow \nu(x,j) = \nu(y,j))\big) \end{aligned}$$

The number $\nu(x,i)$ is the largest power m such that p_i^m is a factor of x, where p_i is the i-th prime number ($p_0 = 2, p_1 = 3, \ldots$), or zero in case $x = 0$. (In algebra, it's customary to set $\nu(0,i) := \infty$. But we want to stay exclusively in the realm of natural numbers.) The order $(\prec_{r+1})$ is precisely the lexicographic order where primes with $(\prec_r)$-larger index are given priority. Sorted according to $(\prec_1)$, the natural numbers line looks like follows:

$$\begin{array}{lllll} 0 & & & & \\ 1 & 2^1 & 2^2 & 2^3 & \cdots \\ 3^1 & 3^1 2^1 & 3^1 2^2 & 3^1 2^3 & \cdots \\ 3^2 & 3^2 2^1 & 3^2 2^2 & 3^2 2^3 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \\ 5^1 & 5^1 2^1 & 5^1 2^2 & 5^1 2^3 & \cdots \\ 5^1 3^1 & 5^1 3^1 2^1 & 5^1 3^1 2^2 & 5^1 3^1 2^3 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \\ 5^2 & 5^2 2^1 & 5^2 2^2 & 5^2 2^3 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

The order $(\prec_r)$ represents the order type $\omega^{\omega^{\cdots^{\omega}}}$ (with $(r+1)$ occurences of ω), and we select $(\prec_r)$ to canonically represent this order type.

In order to show the claim it suffices to verify that Heyting arithmetic verifies $\mathrm{TI}(\prec_r)$ for all numerals r. We do this by ordinary induction on r (externally). The base case $r = 0$ is done by Proposition 2.7. For the induction step $r \to s(r)$, one verifies that there is way to reduce the statement $\mathrm{TI}(\prec_{r+1})$ for a predicate symbol P to the statement $\mathrm{TI}(\prec_r)$ for a related predicate $B_r[P]$ defined in terms of P, similar to the proof that ordinary induction implies $\mathrm{TI}(\omega)$. The details are left to a guided exercise. □

We'll later learn how to represent families of relations defined by primitive recursion in Heyting arithmetic. We'll therefore obtain a formula A in three variables $x, y, r : N$ such that for each numeral m, the formula $A[\underline{m}/r]$ is provably equivalent to $(\prec_m)$. However, it's important to understand that the proof of Theorem 2.3 can't be adapted to show that Heyting arithmetic verifies

"for any $r : N$ and any predicate P, $(\prec_r)$-induction holds for P".

Indeed, since the language of Heyting arithmetic doesn't allow to quantify over predicates, this statement can't be directly formalized in Heyting arithmetic. The following statement can (in the language of Heyting arithmetic extended by a predicate symbol P):

$$\forall r.\ \Big(\big(\forall n : N.\ (\forall m : N.\ m \prec_r n \Rightarrow P(m)) \Rightarrow P(n)\big) \Longrightarrow \big(\forall n : N.\ P(n)\big)\Big)$$

This statement expresses that for the fixed predicate given by the predicate symbol, the principle of $(\prec_r)$-induction holds for any $r : N$. But still, the proof of Theorem 2.3 can't be adapted to yield a proof of this statement (in Heyting arithmetic with the extended language). If this statement had a proof, then Heyting arithmetic would verify $\mathrm{TI}(\varepsilon_0)$. explain how

We could extend Heyting arithmetic with the necessary language and axioms to formalize speaking about predicates. The argument given in the proof of Theorem 2.3 can be formalized in this system; it is (an intuitionistic variant of) a system called Z_2 and is vastly stronger than Heyting arithmetic. check nomenclature, it is Z_2?

Gentzen proved Theorem 2.4 without using Gödel's second incompleteness theorem. If we allow ourselves to use this powerful result, a proof of Theorem 2.4 is easy:

Proof of Theorem 2.4. Assume that Heyting arithmetic shows $\mathrm{TI}(\varepsilon_0)$. Then the consistency proof, valid even in $\mathrm{PRA} + \mathrm{TI}(\varepsilon_0)$, can be interpreted in Heyting arithmetic to yield a proof of consistency of HA in HA. By Gödel's second incompleteness theorem, this implies that HA is inconsistent. But by Theorem 2.2 this is a contradiction. □

Proof of Theorem 2.2 (sketch). We set up a two-player game between a *falsifier* and a *verifier*. The state of the game is a sequent $\Gamma \vdash \varphi$, where we employ a variant of natural deduction in which we don't explicitly write down the context at the turnstile, in which formulas may only contain the symbols $=, \wedge, \forall, \neg$, and in which to the left of a turnstile a finite list of assumptions may appear.

The falsifier tries to demonstrate that the current sequent doesn't represent a valid conclusion. For this, they have various moves available, for instance they may substitute arbitrary numerals for free variables ("Well, does it hold for these choices of the parameters?") and they may reduce a sequent of the form $\Gamma \vdash \varphi \wedge \psi$ to either of the sequents $\Gamma \vdash \varphi$ and $\Gamma \vdash \psi$ ("Well, does this conjunct hold?").

The goal of the verifier is to identify the sequent as valid. They too have various moves available, for instance reducing a sequent of the form $((\forall x : N.\ \varphi), \Gamma) \vdash \underline{n} = \underline{m}$ in which $n \neq m$ to $((\forall x : N.\ \varphi), \varphi[\underline{k}/x], \Gamma) \vdash \underline{n} = \underline{m}$ where k is an arbitrary numeral ("Well, the consequent doesn't hold, but one of the assumptions is invalid!").

A sequent is *irreducible* if and only if no reduction steps of any player can be applied to it. A sequent $\Gamma \vdash \underline{n} = \underline{m}$ is in *endform* if and only if $n = m$ or if Γ contains a false equality.

Gentzen showed, using transfinite induction up to ε_0, that any provable sequent can be reduced to endform. The consistency of Heyting arithmetic follows from this result as follows. Assume that Heyting arithmetic proves $\bot$. Then the sequent $\vdash \underline{1} = \underline{0}$ of the modified calculus is provable as well (where the list of assumptions on the left of the turnstile is empty). It is therefore reducible to endform; but on the other hand, it is irreducible, as is immediate from the complete list of allowed reduction rules (not given here). Therefore $1 = 0$ or the empty list contains a false equality. This is a contradiction. □

Let's call reasoning within $\mathrm{PRA} + \text{QF-TI}(\varepsilon_0)$ *sesquifinitary* find a better notion or decide that it's best, similar to how reasoning within PRA is dubbed *finitary* and reasoning within PA (and particularly much stronger systems) is dubbed *infinitary*. (For some people, induction up to ε_0 for quantifier-free formulas is finitistically acceptable, but we don't want to take a stand on this.)

The proof of Theorem 2.2 doesn't only give a sesquifinitary justification of the proof techniques Peano arithmetic gives us clarify, but also elucidates the sesquifinitary *meaning* of sequents of Heyting arithmetic: Recall that formulas containing nested quantifiers don't have a (sesqui-)finitary meaning a priori; but in view of the consistency result, they can't be entirely devoid of content – for instance we can stop looking for a finitary disproof of a statement if we know that it has a proof in Peano arithmetic.

For Gentzen, the sesquifinitary meaning of a sequent is the strategy to reduce it to endform.
details

think about acceptability of Peano arithmetic (in contrast to Heyting arithmetic). look up established translation of Gödel's "für sich".

properly put into the bibliography: 1. http://www.helsinki.fi/~vonplato/articles.html/vonPlato2009GenOri.pdf 2. all four of Gentzen's proofs

link Rathjen's survey article on ordinal analysis, https://www1.maths.leeds.ac.uk/~rathjen/ICMend.pdf

explain significance of ε_0

3. Arithmetization of syntax

The goal of this section is to explain how Heyting arithmetic and related systems can talk about formulas and provability in formal systems, particularly themselves. This ability, together with a fixed-point theorem, comprises the core of Gödel's incompleteness theorems.

We implicitly used the fact that statements and results about syntax can be arithmetized already in Section 2. For instance, Theorems 2.2 and 2.4 stated that (some variant of) PRA showed some facts about HA, but at that point we neither gave a fully formal proof nor did we explain how to formulate the claims as formulas of PRA. This section rectifies this ommission.

It may come at some surprise that it's not even possible to directly formulate the statements "$2^x = y$" or "$x! = y$" in raw Heyting arithmetic. For *numerals* x, the expressions 2^x and $x!$ can be rewritten as $2 \cdot \ldots \cdot 2$ and $x \cdot (x-1) \cdot \ldots \cdot 1$, showing that they can be expressed in the language of arithmetic. However, for *variables* they can't be rewritten in this way; the term language of Heyting arithmetic doesn't admit expressions such as

$$\underbrace{2 \cdot \ldots \cdot 2}_{x \text{ factors}}.$$

This section shows that such expressions can be made sense of in Heyting arithmetic, and in fact in much weaker systems, though it's not obvious how.

Remark 3.1. There is a related fine point often glossed over in introductory courses. For instance, in textbooks on linear algebra one will find the definition "a vector space V is finitely generated if and only if

$$\exists n : \mathbb{N}.\ \exists x_1 : V.\ \ldots \exists x_n : V.\ \forall x : V.\ \exists a_1, \ldots, a_n : \mathbb{R}.\ x = \textstyle\sum_i a_i x_i."$$

Such a definition cannot be directly expressed in first-order logic: The number of existential quantifiers depends on n, which is not a placeholder for a numeral but an internal variable.

3.1. **Representing functions.** explain classes of functions: prim.-rec., provably total, rec., arbitrary

Somewhat counterintuitively, we'll see in Theorem 3.8 that in any reasonable formal system only computable functions have a chance of being representable, let alone of being provably total. At first sight, this seems to be at odd with the fact that, for instance, in the context of ZFC non-computable functions are routinely defined and studied.

Definition 3.2. Let S be a formal system whose language comprises that of arithmetic.

(1) A function $f : \mathbb{N}^r \to \mathbb{N}$ is *representable in* S if and only if there is a formula φ with free variables $x_1, \dots, x_r, y$ such that S derives, for each $\vec{a} \in \mathbb{N}^r$, the sequents
   (a) $\varphi[\underline{\vec{a}}/\vec{x}] \wedge \varphi[\underline{\vec{a}}/\vec{x}, y'/y] \vdash_{y,y'} y = y'$
   (b) $\top \vdash \varphi[\underline{\vec{a}}/\vec{x}, \underline{f(\vec{a})}/y]$.

(2) A function $f : \mathbb{N}^r \to \mathbb{N}$ is *provably total in* S (also called "provably recursive") if and only if there is a formula φ with free variables $x_1, \dots, x_r, y$ such that S derives
   (a) the single sequent $\top \vdash \forall \vec{x} : \vec{N}.\ \exists! y : N.\ \varphi$ ("φ is a provably functional relation") and
   (b) for each $\vec{a} \in \mathbb{N}^r$, the sequent $\top \vdash \varphi[\underline{\vec{a}}/\vec{x}, \underline{f(\vec{a})}/y]$.

If a function f can be represented by a formula φ, we can formalize the statement "$f(\vec{x}) = y$" as "φ". The conditions (b) of each of the definitions guarantee that this translation is faithful with respect to numerals as arguments. Condition (a) in the definition of representability ensures that f appears to be single-valued from the point of view of S (at least for numerals as arguments), while condition (a) in the definition of provable totality ensures that f appears to be a well-defined total function.

Provably total functions are trivially also representable. The converse is totally wrong. There are many examples of functions which a sufficiently strong metatheory believes to be total (defined on all inputs) but which a particular formal system can't prove to be total. For instance, the function which maps a hydra (coded in a suitable fashion as a natural number) to the number of steps Hercules needs in order to kill the hydra (when following some specified strategy) isn't provably total in Peano arithmetic, for otherwise Peano arithmetic could show that every Hydra–Hercules battle ends. include short excurse on the hydra game. At least reference Andrej's blog post http://math.andrej.com/2008/02/02/the-hydra-game/.

If a system doesn't manage to verify a representable function f to be total, then this intuitively means that the system isn't strong enough to find a single coherent *reason* – a proof – of the individual facts that $f(0)$, $f(1)$, and so on are defined; the proofs of the individual facts get more and more complex.

Example 3.3. Let $\mathsf{lcm} : \mathbb{N} \to \mathbb{N}$ be the function which maps a number n to the least common multiple of the numbers $1, \dots, n$. Then lcm is provably total in HA. A formula witnessing this claim is

$$(\forall i : N.\ 1 \leq i \wedge i \leq x \Rightarrow i \mid y) \wedge \Big(\forall z : N.\ \big((\forall i : N.\ 1 \leq i \wedge i \leq x \Rightarrow i \mid z) \Rightarrow y \mid z\big)\Big),$$

where "$a \mid b$" is a syntactic sugar for "$\exists u : N.\ b = ua$".

Given a provably functional relation φ, we can extend the language of S by a function symbol whose graph will be given by φ without making the system stronger. We'll now make this claim precise.

Definition 3.4. An extension S' of a formal system S is *conservative over* S if and only if every sequent in the language of S which is provable in S' is also provable in S.

Example 3.5. Peano arithmetic is not conservative over Heyting arithmetic, even though they are *equiconsistent*, that is, the consistency of one system implies the consistency of the other and vice versa.

Proposition 3.6. *Let S be a formal system in minimal logic, intuitionistic logic, or classical logic.*

(1) *Let α be a formula with a free variable $x : X$ such that S proves $\top \vdash \exists! x : X.\ \alpha$. The system S enriched by a new constant symbol $\iota x.\ \alpha$ and the axiom $\top \vdash \alpha[(\iota x.\ \alpha)/x]$ is conservative over S.*

(2) *Let φ be a formula with free variables $x_1 : X_1, \dots, x_r : X_r, y : Y$ such that S proves $\top \vdash \forall \vec{x} : \vec{X}.\ \exists! y : Y.\ \varphi$. The system S enriched by a new function symbol f_φ and the axiom $\top \vdash \forall \vec{x} : \vec{X}.\ \varphi[f_\varphi(\vec{x})/y]$ is conservative over S.*

Proof. The idea is to specify a translation $\psi \mapsto \psi^T$ of formulas in the extended system to formulas of S such that provability of $\psi \vdash_{\vec{z}} \chi$ in the extended system implies provability of $\psi^T \vdash_{\vec{z}} \chi^T$ in S.

It's easiest to explain what such a translation can look like by giving examples:

$$(\forall y : Y.\ R(g(\iota x.\ \alpha, y), z))^T :\equiv (\exists x : X.\ (\alpha \wedge (\forall y : Y.\ R(g(x, y), z))))$$
$$(\forall x : X.\ g(f_\varphi(2x)) = h(x))^T :\equiv (\forall x : X.\ \exists y : Y.\ (\varphi[(2x)/x] \wedge (g(y) = h(x))))$$

Instead of using the idiom "$\exists.\ \varphi \wedge \cdots$", one could equivalently use "$\forall.\ \varphi \Rightarrow \cdots$". Also it doesn't matter at which position these quantifiers are put in, as long as occuring variables are already bound.

Verifying that proofs in the extended system give rise to proofs in the original system (of the translated sequents) is an instructive exercise. □

For the central representability result, it won't cause additional difficulties to consider IQ, *intuitionistic Robinson arithmetic*. This system is the same as Heyting arithmetic, but with the induction axiom schema removed and only the weak axiom

$$\top \vdash \forall n : N.\ n = 0 \vee (\exists m : N.\ n = s(m))$$

newly put in. (This axiom is trivially provable in Heyting arithmetic, by an induction proof with the curious property that the proof of the induction step doesn't use the induction hypothesis.) Intuitionistic Robinson arithmetic is noteworthy because it is given by a finite list of axioms, without any axiom schemas. However, it's extremely weak; it can't even prove $\forall n : N.\ 0 + n = n$.[2] It can only verify specific instances of this universal statement, for instance like this:

$$0 + \underline{2} = 0 + s(s(0)) = s(0 + s(0)) = s(s(0)) = \underline{2}.$$

[2] One can build within a set theory such as ZF a model of IQ comprising the ordinary natural numbers and two further "rogue" elements a and b. In this model $0 + a = b$. link https://math.stackexchange.com/a/1066378/61604

The statements of the following theorems require some explanations.

Theorem 3.7. *Every computable function is representable in* IQ.

Theorem 3.8. *If a function is representable in a consistent recursively axiomatizable formal system (such as, presumably,* HA, PA, *or* ZFC*), then it is computable.*

explain resolution of counterintuitiveness

Theorem 3.9. *Primitive-recursive functions are provably total in* HA *(and in much weaker systems). Furthermore, the relevant recursion rules are provable in* HA.

Definition 3.10. (1) A partial function $\mathbb{N}^r \rightharpoonup \mathbb{N}$ is *computable* (or "recursive") if and only if it's the induced partial function of a mapping recipe. A partial function $\mathbb{N}^r \rightharpoonup \mathbb{N}$ is *primitive-recursive* if and only if it's the induced (a priori partial, but actually total) function of a mapping recipe built using only 0, succ, proj_i, comp, and rec.

(2) A *mapping recipe* (a kind of syntactical object) is inductively made up of the ingredients.

- $0 : N \rightsquigarrow N$, interpreted as the zero function.
- $\mathsf{succ} : N \rightsquigarrow N$, interpreted as the successor function.
- $\mathsf{proj}_i : N^r \rightsquigarrow N$, interpreted as the i-th projection.
- $(+) : N^2 \rightsquigarrow N$, interpreted as addition.
- $(\cdot) : N^2 \rightsquigarrow N$, interpreted as multiplication.
- $\delta : N^2 \rightsquigarrow N$, interpreted as $(x, y) \mapsto \begin{cases} 1, & \text{if } x = y, \\ 0, & \text{otherwise.} \end{cases}$
- $\mathsf{comp}(f, g_1, \ldots, g_r) : N^s \rightsquigarrow N$ for mapping recipes $f : N^r \rightsquigarrow N$, $g_i : N^s \rightsquigarrow N$, $i = 1, \ldots, r$, interpreted as the composition $(x_1, \ldots, x_s) \mapsto f(g_1(x_1, \ldots, x_s), \ldots, g_r(x_1, \ldots, x_s))$.
- $\mu(f) : N^r \rightsquigarrow N$ for a mapping recipe $f : N^{r+1} \rightsquigarrow N$, interpreted as the partial function ("unbounded minimization")
$$(x_1, \ldots, x_r) \longmapsto \min\{n \in \mathbb{N} \,|\, f(x_1, \ldots, x_r, n) = 0\}.$$
- $\mu_<(g, f) : N^r \rightsquigarrow N$ for mapping recipes $g : N^r \rightsquigarrow N$, $f : N^{r+1} \rightsquigarrow N$, interpreted as the total function ("bounded minimization")
$$\vec{x} \longmapsto \min(\{n < g(\vec{x}) \,|\, f(\vec{x}, n) = 0\} \cup \{g(\vec{x})\}).$$
- $\mathsf{rec}(f, g) : N^{r+1} \rightsquigarrow N$ for mapping recipes $f : N^r \rightsquigarrow N$, $g : N^{r+2} \rightsquigarrow N$ ("primitive recursion"), interpreted as the function $h : \mathbb{N}^{r+1} \to \mathbb{N}$ with
$$h(\vec{x}, n) = \begin{cases} f(\vec{x}), & \text{if } n = 0, \\ g(\vec{x}, m, h(\vec{x}, m)), & \text{if } n = s(m) \text{ for a number } m. \end{cases}$$

Remark 3.11. In a previous version of these notes, the composition recipe was given as follows: "$\mathsf{comp}(f, g_1, \ldots, g_r) : N^{s_1+\cdots+s_r} \rightsquigarrow N$ for mapping recipes $f : N^r \rightsquigarrow N$, $g_i : N^{s_i} \rightsquigarrow N$, $i = 1, \ldots, r$, interpreted as the composition $(x_{11}, \ldots, x_{1s_1}, \ldots, x_{r1}, \ldots, x_{rs_r}) \mapsto f(g_1(x_{11}, \ldots, x_{1s_1}), \ldots, g_r(x_{r1}, .$ Without an additional recipe which allows for duplication of variables, the resulting system of recipes isn't sufficiently expressive.

Functions given by mapping recipes can be mechanically computed, granted enough time and computational space. The converse statement, the claim that any total function which is physically computable in the real world is given by a mapping recipe, is known as the *Church–Turing thesis*. Most people believe in this thesis, but as a statement about the real world it isn't, of course, amenable to a rigorous proof. Certainly any program running on conventional computers of our time can be realized as (hugely complex) mapping recipes.

Remark 3.12. Bounded minimization can be expressed using primitive recursion. Also the recipes $(+)$, $(\cdot)$, and δ can be expressed using primitive recursion. We included these because we'll need to talk about them for a bootstrapping process.

Proof of Theorem 3.7. We have to give for each mapping recipe h that induces a partial function $\mathbb{N}^r \to \mathbb{N}$ a formula φ_h in IQ (with free variables $x_1 : N, \dots, x_r : N, y : N$) that represents this function. (In the following we will conflate mapping recipes with the functions that they induce.) We do this by induction on the structure of h:

- $0 : N \rightsquigarrow N$ is represented by $\varphi_h :\equiv (y = 0)$.
- $\mathsf{succ} : N \rightsquigarrow N$ is represented by $\varphi_h :\equiv (y = s(x_1))$.
- $\mathsf{proj}_i : N^r \rightsquigarrow N$ is represented by $\varphi_h :\equiv (y = x_i)$.
- $(+) : N^2 \rightsquigarrow N$ is represented by $\varphi_h :\equiv (y = x_1 + x_2)$.
- $(\cdot) : N^2 \rightsquigarrow N$ is represented by $\varphi_h :\equiv (y = x_1 \cdot x_2)$.
- $\delta : N^2 \rightsquigarrow N$ is represented by $\varphi_h :\equiv ((y = 1 \wedge x_1 = x_2) \vee (y = 0 \wedge \neg\,(x_1 = x_2)))$.
- If $h \equiv \mathsf{comp}(f, g_1, \dots, g_r) : N^s \rightsquigarrow N$ for mapping recipes $f : N^r \rightsquigarrow N$, $g_i : N^s \rightsquigarrow N$, $i = 1, \dots, r$, we may assume by induction that there are formulas φ_f and φ_{g_i}, $i = 1, \dots, r$, that represent f or g_i respectively. Then h is represented by
$$\varphi_h :\equiv (\exists \vec{z} : \vec{N}.\ \varphi_f[\vec{z}/\vec{x}] \wedge \varphi_{g_1}[z_1/y] \wedge \dots \wedge \varphi_{g_r}[z_r/y]).$$
- If $h \equiv \mu(f) : N^r \rightsquigarrow N$ for a mapping recipe $f : N^{r+1} \rightsquigarrow N$, which is represented by φ_f, then h is represented by
$$\varphi_h :\equiv (\varphi_f[0/y, y/x_{r+1}] \wedge \forall \tilde{y} : N.\ (\varphi_f[0/y, \tilde{y}/x_{r+1}] \implies y \leq \tilde{y}))\,.$$
- If $h \equiv \mu_<(g, f) : N^r \rightsquigarrow N$ for mapping recipes $g : N^r \rightsquigarrow N$ and $f : N^{r+1} \rightsquigarrow N$, then h is represented by
$$\begin{aligned}\varphi_h :\equiv\ & ((\varphi_f[0/y, y/x_{r+1}] \vee \varphi_g) \\ & \wedge \forall \tilde{y} : N.\ ((\varphi_f[0/y, \tilde{y}/x_{r+1}] \vee \varphi_g[\tilde{y}/y]) \implies y \leq \tilde{y}))\,.\end{aligned}$$
- For $h \equiv \mathsf{rec}(f, g) : N^{r+1} \rightsquigarrow N$ with mapping recipes $f : N^r \rightsquigarrow N$, $g : N^{r+2} \rightsquigarrow N$ we would like to define something like
$$\begin{aligned}\varphi_h :\equiv\ & \exists v_0 : N, \dots, v_{x_{r+1}} : N.\ \varphi_f[v_0/y] \\ & \wedge (\forall i : N.\ i < x_{r+1} \implies \varphi_g[i/x_{r+1}, v_i/x_{r+2}, v_{i+1}/y]) \\ & \wedge (y = v_{x_{r+1}}).\end{aligned}$$
The only problem is that this definition does not make any sense at all: The variable x_{r+1} is internal to IQ and we are not allowed to use its value externally to define (the structure

of) a formula. The idea of this definition may however be rescued. To do this, we will develop a technique for encoding multiple natural numbers by a single number. This will allow us to replace "$\exists v_0 : N, \ldots, v_{x_{r+1}} : N.$" in the formula above by $\exists$-quantification over a single variable. We interrupt this proof here and will continue it once we have the required technique at our disposal.

fill in proof of computability
fill in proof of provable totality

3.2. **Engineering in arithmetic.**

Lemma 3.13. *There is a mapping recipe $J : \mathbb{N}^2 \rightsquigarrow \mathbb{N}$, called* pairing function*, such that there are mapping recipes $K, L : \mathbb{N} \rightsquigarrow \mathbb{N}$ with the following properties:*

(1) *The recipes J, K, and L are defined using only the basic recipes, composition, and bounded minimization, but not unbounded minimization or primitive recursion.*
(2) *Using only induction for quantifier-free formulas, one can prove the identities $K(J(x,y)) = x$, $L(J(x,y)) = y$, $J(K(z), L(z)) = z$ for all $x, y, z \in \mathbb{N}$ and the inequalities $J(x,y) \geq x$, $J(x,y) \geq y$ for $x, y \in \mathbb{N}$.*

Proof. One possibility is setting

$$J(x,y) := (x+y)(x+y+1)/2 + x.$$

fill in rest of the proof □

Theorem 3.14 ("The beta function lemma")**.** *There is a mapping recipe $\beta : \mathbb{N}^2 \rightsquigarrow \mathbb{N}$, called* beta function*, such that:*

(1) *The recipe β is defined using only the basic recipes, composition, and bounded minimization.*
(2) *For any number n and any numbers $a_0, \ldots, a_n$, there is a number d such that*

$$\beta(d,i) = a_i \text{ for all } i \leq n, \quad \text{and} \quad d > a_i \text{ for all } i \leq n.$$

(We don't claim that this statement is expressible or provable in some specific formal system. It's a statement taking place in the metatheory.)
(3) *The following statement is provable in Heyting arithmetic:*

$$\forall \ell.\ \forall d.\ \forall a.\ \exists d'.\ \big((\forall i.\ i < \ell \Rightarrow \beta(d',i) = \beta(d,i)) \wedge (\beta(d',\ell) = a) \wedge (d' > a)\big)$$

The applications of β in this statement are to be translated as in Proposition 3.6.

Proof. We define β by

$$\beta(d,i) := \beta^*(K(d), L(d), i),$$
$$\beta^*(c,m,i) := \mathsf{rem}(c, (i+1)m + 1),$$

where rem denotes the (recipe for the) remainder function. The hard part is to verify claims (2) and (3). The second claim follows from an iterated application of the third claim (or rather its proof, reinterpreted in the metatheory). But it's instructive to verify claim (2) directly.

For this, let numbers $a_0, \dots, a_n$ be given and set

$$k := \max\{n, a_0 + 1, \dots, a_n + 1\},$$
$$m := \operatorname{lcm}\{1, \dots, k\}.$$

The numbers $(i+1)m+1$ are pairwise coprime for $i = 0, \dots, n$: Let p be a common prime divisor of $(i+1)m+1$ and of $(j+1)m+1$. Then p divides $(j-i)m$, so $p \mid j-i$ or $p \mid m$. In the second case it follows that p divides 1, a contradiction; in the first case follows that $p \leq |j-i| \leq n \leq k$, so $p \mid m$, therefore we can reduce to the second case.[3]

By the Chinese remainder theorem, there exists a number c such that $c \equiv a_i$ modulo $(i+1)m+1$ for all $i \leq n$. We set $d := J(c, m)$. Then $\beta(d, i) = a_i$ and $a_i < k \leq m \leq d$ for all $i \leq n$.

Let's verify claim (3). We work informally, trusting the reader to convince themselves that the proof could be carried out in Heyting arithmetic. Let ℓ, d, a be given. Set $k := d + \ell + a + 1$ and $m := \mathsf{lcm}(k)$. We are allowed to use the lcm function since Heyting arithmetic proves that it's total, Example 3.3.[4] It suffices to prove the the following lemma; the claim then follows by using the lemma for $n := \ell$ and setting $d := J(c, m)$ as before.

$$\forall n.\ n \leq \ell \Longrightarrow \exists c.\ \forall i.\ i \leq n \Rightarrow \mathsf{rem}(c, (i+1)m+1) = \begin{cases} \beta(d, i), & \text{if } i < \ell, \\ a, & \text{otherwise.} \end{cases}$$

We verify this using ordinary induction on n. The base case $n = 0$ is trivial, we may set $c := a$.

For the induction step $n \to s(n)$, assume that $s(n) \leq \ell$. By induction hypothesis, there exists a number c' such that $\mathsf{rem}(c', (i+1)m+1) = \beta(d, i)$ for all $i \leq n$. There exists a number r such that $(i+1)m+1 \mid r$ for all $i \leq n$ and such that r is smallest with this property (with respect to divisibility).[5] One can verify that any prime factor of r is a prime factor of one of the numbers $(i+1)m+1$, $i = 0, \dots, n$.

The numbers r and $(n+2)m+1$ are coprime: If p is a common prime factor, then $p \mid (i+1)m+1$ for some $i \leq n$. We can therefore reason as we did in the proof of claim (2). We can therefore apply the Chinese remainder theorem to obtain a number c such that

$$\mathsf{rem}(c, r) = c' \quad \text{and} \quad \mathsf{rem}(c, (n+2)m+1) = a.$$

In particular, for $i \leq n$ it follows that $\mathsf{rem}(c, (i+1)m+1) = \beta(d, i)$ since $(i+1)m+1 \mid r$. □

[3] By *proof mining*, one can extract from this proof an explicit certificate for coprimality: Writing $m = (i-j)m'$,

$$1 = (1 - (i+1)(i-j)m' + (i+1)^2 m') \cdot ((i+1)im + 1) - (i+1)^2 m' \cdot ((j+1)m + 1).$$

[4] In the literature, often $k!$ instead of $\mathsf{lcm}(k)$ is used. At this point, we know how to represent the factorial function – using the beta function, which is representable in IQ and in HA even provably total. However, at this stage, there doesn't seem to be an easy proof of the fact that the factorial function represented in this way is provably total. (It is, if we assume the conclusion of the theorem we're proving, since this shows that any primitive-recursive function is provably total in HA.) The lcm function is better suited because we can represent it and prove it to be total without recourse to the beta function.

[5] This follows by using ordinary induction on j to verify that, if $j \leq n$, then there exists a number r such that $(i+1)m+1 \mid r$ for all $i \leq j$ and such that r is smallest with this property (with respect to divisibility). The number r obtained will simply be the product of the numbers $(i+1)m+1$. But at this stage, we don't know how to state this fact in Heyting arithmetic.

Proof of Theorem 3.7 (continuation). We can now prove the last remaining case. Assume that the mapping recipe h is $\mathsf{rec}(f,g) : N^{r+1} \rightsquigarrow N$ with $f : N^r \rightsquigarrow N$ and $g : N^{r+2} \rightsquigarrow N$. By induction we may assume that φ_f represents f and φ_g represents g. Then h is represented by

$$\begin{aligned}\varphi_h :\equiv \exists d : N.\ & \varphi_f[\beta(d,0)/y] \\ & \wedge (\forall i : N.\ i < x_{r+1} \implies \varphi_g[i/x_{r+1}, \beta(d,i)/x_{r+2}, \beta(d,i+1)/y]) \\ & \wedge (y = \beta(d, x_{r+1})).\end{aligned}$$

□

Proof of Theorem 3.9. We prove this by induction on the structure of a mapping recipe. The most interesting case is the case where the mapping recipe is of the form $\mathsf{rec}(f,g)$ with $f : N^r \rightsquigarrow N$, $g : N^{r+2} \rightsquigarrow N$. By the induction hypothesis, we may assume that f and g are provably total. We allow ourselves to use function symbols for f and g and therefore to suppress the formulas witnessing this fact from the notation. We have already seen in the proof of Theorem 3.7 that $\mathsf{rec}(f,g)$ can be represented by the formula

$$\varphi :\equiv (\exists d : N.\ (\beta(d,0) = f(\vec{a}) \wedge (\forall i : N.\ i < x \Rightarrow \beta(d, s(i)) = g(\vec{a}, i, \beta(d,i))) \wedge y = \beta(d,x))).$$

We now verify $\forall x : N.\ \exists y : N.\ \varphi$ by induction on x.

The base case $x = 0$ is trivial, we may take $d := J(f(\vec{a}), f(\vec{a}))$. The induction step follows from part (3) of Theorem 3.14. □

The beta function gives a crude way to code finite lists of numbers in arithmetic, but it isn't sufficiently powerful to, for instance, support a length function which would compute the length of a given list. But, since we're now bootstrapped to use arbitrary primitive-recursion functions in Heyting arithmetic, we can easily improve on the crude coding given by the beta function.

Definition 3.15. A number v is a *well-coded list*, abbreviated $\mathrm{wcl}(v)$, if and only if

(1) $\beta(L(v), i) < L(v)$ for all $i < K(v)$, and
(2) for all v' such that $K(v') = K(v)$ and $\beta(L(v'), i) = \beta(K(v'), i)$ for all $i < K(v)$, $v \leq v'$.

The i-th element of a well-coded list v is $\beta(L(v), i)$. The *length* of a well-coded list v is $K(v)$.

Proposition 3.16. (1) *For any number n and any numbers $a_1, \ldots, a_n$, there is a well-coded list v of length n such that, for all $i < n$, the i-th element of v is a_i.*
(2) *Heyting arithmetic proves the following operations on well-coded lists to be total: determining the length, extracting the i-th element, appending a single element, appending a well-coded list, checking whether a given number occurs (written "$k \in v$").*
(3) *Heyting arithmetic proves that well-coded lists are extensional: If v and v' are well-coded lists with $K(v) = K(v')$ and $\beta(L(v), i) = \beta(L(v'), i)$ for all $i < K(v)$, then $v = v'$.*
(4) *Heyting arithmetic verifies induction for well-coded lists: In the language extended by a predicate symbol P, the following statement is provable.*

$$\big(\forall v : N.\ (\mathrm{wcl}(v) \wedge (\forall k : N.\ \mathrm{wcl}(k) \wedge k \in v \Rightarrow P(k))) \Rightarrow P(v)\big) \implies (\forall v : N.\ \mathrm{wcl}(v) \Rightarrow P(v)).$$

3.3. **Gödel's incompleteness theorems.** adequate Gödel numbering, recursively axiomatizable

Theorem 3.17 (The diagonal lemma)**.** *Let S be a formal system which contains* IQ*. Fix an adequate Gödel numbering for S. Let φ be a formula of S with free variables $x_1 : X_1, \dots, x_r : X_r$ and $n : N$. Then there exists a formula α such that $S \vdash (\alpha \Leftrightarrow \varphi[\underline{\ulcorner \alpha \urcorner}/n])$.*

Proof. Let $\mathrm{diag} : \mathbb{N} \to \mathbb{N}$ be the function which maps the Gödel number of a formula ψ containing a free variable $n : N$ to the Gödel number of $\psi[\underline{\ulcorner \psi \urcorner}/n]$, and maps other inputs to some arbitrarily fixed constant. By our assumption on adequacity, this function is computable. By Theorem 3.7, we may pretend that IQ is equipped with a function symbol for diag.

We set $\gamma :\equiv \varphi[\mathrm{diag}(n)/n]$ (a formula with the same free variables as φ) and $\alpha :\equiv \gamma[\underline{\ulcorner \gamma \urcorner}/n]$. Thus $\mathrm{diag}(\ulcorner \gamma \urcorner) = \ulcorner \alpha \urcorner$. We then have

$$\alpha \equiv \gamma[\underline{\ulcorner \gamma \urcorner}/n] \equiv \varphi[\mathrm{diag}(\underline{\ulcorner \gamma \urcorner})/n] \dashv\vdash_{x_1,\dots,x_r} \varphi[\underline{\ulcorner \alpha \urcorner}/n]. \qquad \square$$

We'll often apply the diagonal lemma to IQ, even if we're interested in stronger systems.

Definition 3.18. A formal system S is *complete* if and only if, for any formula φ in S, $S \vdash \varphi$ or $S \vdash \neg\varphi$.

Completeness of a formal system is vastly different from the condition that $S \vdash (\varphi \vee \neg\varphi)$ for all formulas φ. The latter condition is trivially satisfied in any formal system which uses classical logic and can be paraphrased as "S believes any statement to be true or false". This is quite weaker than "S proves or disproves any statement".

From a classical point of view, completeness of a formal system is a very desirable property: The best case would be that we have an algorithm which solves the *Entscheidungsproblem*, producing for any statement either a proof or a disproof. The second-best case would be that the formal system we use to formalize our reasoning in is at least strong enough to *possess* a proof or disproof for any statement, even if we don't have a mechanical way to determine what is the case. This property of a formal system is what's classically called *completeness*. Gödel's first incompleteness theorem shows that any system which is suitable to use as a formal systems for doing general mathematics in is incomplete.

We should note that because we work in an intuitionistic metatheory, our definition of completeness is stronger than usually conceived. We therefore introduce the following weaker notion:

Definition 3.19. A formal system S is *anonymously complete* if and only if, for any formula φ in S, it's *not not* the case that $S \vdash \varphi$ or $S \vdash \neg\varphi$.

Theorem 3.20 (Gödel's first incompleteness theorem in the stronger version by Rosser)**.** *Let S be a formal system which contains* IQ *and which is recursively axiomatizable with respect to a fixed Gödel numbering. Then:*

If S is complete, then S is inconsistent.

Taking the contrapositive, if S is consistent, then S is not complete (and not even anonymously complete).

Gödel's proof of his theorem proceeded as follows. By the diagonal lemma, there exists a formula γ of IQ such that

$$\mathrm{IQ} \vdash (\gamma \Leftrightarrow \neg \mathrm{Prov}_S(\underline{\ulcorner \gamma \urcorner})).$$

Intuitively, the formula γ expresses that γ is not provable; the diagonal lemma allowed us to put the informal statement "This statement is not provable" into a formal form.

We can then verify that S is inconsistent if it proves γ: Assume $S \vdash \gamma$. Then there is a number p such that $\mathrm{Proof}_S(p, \ulcorner \gamma \urcorner) = 1$. By what it means for the function $\mathrm{Proof}_S : \mathbb{N}^2 \to \mathbb{N}$ to be representable in IQ, therefore $\mathrm{IQ} \vdash \mathrm{Proof}_S(\underline{p}, \underline{\ulcorner \gamma \urcorner}) = \underline{1}$. Thus $\mathrm{IQ} \vdash \mathrm{Prov}_S(\underline{\ulcorner \gamma \urcorner})$. Therefore $\mathrm{IQ} \vdash \neg\gamma$ and in particular $S \vdash \neg\gamma$. By the assumption $S \vdash \gamma$, it follows that $S \vdash \bot$.

We can't, however, verify that S is inconsistent if it proves $\neg\gamma$. If we could do that, Theorem 3.20 would follow. Gödel's proof showed the following statement: Any ω-consistent formal system which contains IQ and is recursively axiomatizable with respect to a fixed Gödel numbering is incomplete. We don't want to give further details, but heartily recommend Gödel's original paper give citation. It doesn't have any prerequisites in mathematical logic (because mathematical logic didn't really exist then) and is very readable.

Proof of Theorem 3.20. Rosser's insight was to employ a slight variant of Prov_S:

$$\mathrm{Prov}_S^R(m) :\equiv \big(\exists p : N.\ \mathrm{Proof}_S(p, m) \wedge \forall q : N.\ (q \leq p \Rightarrow \neg \mathrm{Proof}_S(q, \mathrm{neg}(m)))\big).$$

In this definition, the symbol neg denotes the function $\mathbb{N} \to \mathbb{N}$ which maps the Gödel number of a formula to the Gödel number of its negation (and which maps inputs which aren't Gödel numbers of formulas to some arbitrarily fixed constant). By our assumptions on the Gödel numbering of S, this function is computable and therefore representable in IQ (and hence S).

By the diagonal lemma, there exists a formula ρ of IQ such that

$$\mathrm{IQ} \vdash (\rho \Leftrightarrow \neg \mathrm{Prov}_S^R(\underline{\ulcorner \rho \urcorner})).$$

We show that $S \vdash \rho$ implies $S \vdash \bot$. Let p be the Gödel number of a proof of ρ. For any number q, either q is the Gödel number of a (valid) proof of $\neg\rho$ or not. Thus either there is a number $q \leq p$ such that q is a proof of $\neg\rho$ or there is no such number. In the first case we trivially have $S \vdash \bot$. In the second case $S \vdash \mathrm{Prov}_S^R(\underline{\ulcorner \rho \urcorner})$.[6] Since $S \vdash \neg\mathrm{Prov}_S^R(\underline{\ulcorner \rho \urcorner})$, we obtain $S \vdash \bot$.

We now show that $S \vdash \neg\rho$ implies $S \vdash \bot$. Let a be the Gödel number of a proof of $\neg\rho$. Then, exactly as above, we could verify $S \vdash \mathrm{Prov}_S^R(\underline{\ulcorner \neg\rho \urcorner})$ (or $S \vdash \bot$); but this won't help us. Instead, we verify in a very similar manner the more refined statement

$$S \vdash \big(\mathrm{Proof}_S(\underline{a}, \underline{\ulcorner \neg\rho \urcorner}) \wedge \forall b : N.\ (b \leq \underline{a} \Rightarrow \neg \mathrm{Proof}_S(b, \underline{\ulcorner \rho \urcorner}))\big)$$

(or $S \vdash \bot$). Using this, we can verify $S \vdash \neg\mathrm{Prov}_S^R(\underline{\ulcorner \rho \urcorner})$, by formalizing the following argument: "Assume $\mathrm{Prov}_S^R(\underline{\ulcorner \rho \urcorner})$. Then there is a number p such that $\mathrm{Proof}_S(p, \underline{\ulcorner \rho \urcorner})$ and such that $\neg\mathrm{Proof}_S(q, \underline{\ulcorner \neg\rho \urcorner})$ for all $q \leq p$. Since $\mathrm{Proof}_S(\underline{a}, \underline{\ulcorner \neg\rho \urcorner})$, $\underline{a} > p$. Since $\neg\mathrm{Proof}_S(b, \underline{\ulcorner \rho \urcorner})$ for all $b \leq \underline{a}$, $p > \underline{a}$. Thus $\bot$." Thus $S \vdash \rho$. But $S \vdash \neg\rho$. Hence $S \vdash \bot$.

Summarizing, we have that both $S \vdash \rho$ and $S \vdash \neg\rho$ imply $S \vdash \bot$. Since S is assumed to be complete, we may deduce $S \vdash \bot$. □

[6] Here we use the fact that IQ, and therefore S, shows for any number n the formula $(\forall m : N.\ m \leq \underline{n} \Rightarrow \alpha) \Leftrightarrow (\alpha[\underline{0}/m] \wedge \cdots \wedge \alpha[\underline{n}/m])$. This fact can be proven by (external) induction on n.

Theorem 3.21 (Gödel's second incompleteness theorem). *todo*

Theorem 3.22 (Löb's theorem). *Let S be a formal system as in Gödel's second incompleteness theorem. Let φ be a formula of S such that $S \vdash (\mathrm{Prov}(\ulcorner\varphi\urcorner) \Rightarrow \varphi)$. Then $S \vdash \varphi$.*

Proof. By the diagonal lemma, there exists a formula ψ such that

$$S \vdash (\psi \Leftrightarrow (\mathrm{Prov}(\ulcorner\psi\urcorner) \Rightarrow \varphi)).$$

By HBL (1) and HBL (3), $S \vdash (\mathrm{Prov}(\ulcorner\psi\urcorner) \Rightarrow \mathrm{Prov}(\ulcorner\mathrm{Prov}(\ulcorner\psi\urcorner) \Rightarrow \varphi\urcorner))$. By HBL (3), todo □

Theorem 3.23 (Parikh's result on long proofs). *todo*

comments on some complete systems

3.4. Gödel's completeness theorem. definition structure, model

Definition 3.24. Models M and M' of a system S are *elementarily equivalent* if and only if, for any formula φ of S without free variables, $M \models \varphi$ iff $M' \models \varphi$.

Example 3.25. The usual set $\mathbb{N}$ of natural numbers together with the usual zero element, the usual successor function, usual addition, and usual multiplication is a model of Heyting arithmetic. In a classical metatheory, this model is even a model of Peano arithmetic; however, intuitionistically, this can't be shown.[7]

Theorem 3.26 (Gödel's completeness theorem). *Let S be a classical consistent system over a countable signature. Then there is a classical model of S. This model can even be chosen to be countable.*

Example 3.27. Gödel's second incompleteness theorem shows that $\mathrm{PA} + \mathrm{Incon}(\mathrm{PA})$ is consistent (if $\mathrm{PA} + \mathrm{Incon}(\mathrm{PA}) \vdash \bot$, then $\mathrm{PA} \vdash \neg\mathrm{Incon}(\mathrm{PA})$; by definition, $\neg\mathrm{Incon}(\mathrm{PA}) \equiv \mathrm{Con}(\mathrm{PA})$). By Gödel's completeness theorem, this theory has a model M. In this model, there is an element p such that M believes that p is the Gödel number of a correct PA-proof of $\bot$. Since PA proves $\neg\mathrm{Proof}(\underline{p}, \ulcorner\bot\urcorner)$ for any number $n \in \mathbb{N}$ (this is by definition what it means for the function Proof to be representable in PA), this element p can't be a *standard number*, that is it can't be of the form $[\![s]\!]([\![s]\!](\cdots([\![0]\!])))$. The nonstandard numbers are greater than any standard number; therefore p can be said to be (the coding of an) "infinitely long proof of the inconsistency of PA". The model M doesn't detect this nonstandardness, of course; from the point of view of M, the element p is a perfectly fine natural number.

Example 3.28. If we assume that ZFC is consistent, then Gödel's completeness theorem yields a *countable* model M of ZFC. Because ZFC proves that there are uncountable sets (ZFC, and also intuitionistic variants of ZFC, proves that there is no surjection $\mathbb{N} \to \mathcal{P}(\mathbb{N})$), the model believes to possess sets which have uncountably many elements. But from the outside, this belief is wrong. This curious phenomenon is known as *Skolem's paradox*. There is no contradiction;

[7] There is a model of intuitionistic mathematics, the *effective topos*, in which there is precisely one model of Heyting arithmetic, namely the usual one. Any model of Peano arithmetic is also a model of Heyting arithmetic, so would have to coincide with $\mathbb{N}$; but $\mathbb{N}$ isn't a model of Peano arithmetic (provably so, in the effective topos). See Theorem 4.25 for the precise statement.

it's simply the case that for elements X of M which M believe to be uncountable, the model doesn't contain a bijection from (what M believes to be) the natural numbers to X.

It's a fundamental fact that first-order logic is riddled with "nonstandard models", models which are not elementarily equivalent to specific "intendent models". Indeed, it's an instructive exercise to show that any consistent classical system which satisfies the assumptions of Gödel's first incompleteness theorem has an uncountable number of pairwise different models. This fact can both be seen as a kind of defect, pressing one to turn to other formalizations of logic, and as a wondrous phenomenon giving rise to a fascinating theory.

It should be noted that there are mathematical universes in which, for exactly the same definitions, nonstandard models don't occur: It's a theorem of Benno van den Berg and Jaap van Oosten that inside the *effective topos*, there is (up to isomorphism) precisely one model of Heyting arithmetic [**?**]. We'll prove this theorem below, as Theorem 4.25. properly cite https://www.staff.science.uu.nl/~ooste110/realizability/arithcat.pdf

4. Realizability theory

4.1. **Motivation.** Let's converse in a classical metatheory for a moment. Assume that we know

$$\forall x : \mathbb{N}.\ \exists y : \mathbb{N}.\ R(x, y) \tag{$\star$}$$

for some relation R. Then, either by the countable axiom of choice or by picking smallest witnesses, there is a function $f : \mathbb{N} \to \mathbb{N}$ such that $\forall x : \mathbb{N}.\ R(x, f(x))$. Now suppose that we don't merely know that ($\star$) is true, but that ($\star$) is *provable*. We could then hope that f is *computable*. We could even hope that if ($\star$) is provable by restricted means, for instance in a weak fragment of Peano arithmetic, then f has only moderate growth (for instance, that f is primitive-recursive).

Taken on face value, this hope is doomed. For instance, the statement "any Turing machine halts or doesn't halt" is provable (for instance, in Peano arithmetic). However, there can't be a computable function f such that $f(n)$ is zero or one, depending on whether the n-th Turing machien halts or doesn't halt, as *halting oracles* don't exist.

Realizability theory is a way of fulfilling a more precisely stated variant of this hope. Other reasons to be interested in realizability theory are:

Proof mining. Realizability theory can be used to mechanically carry out *proof mining*, extracting further information such as algorithms or upper bounds from proofs. In some cases, this information is extremely valuable to subjects such as functional analysis or convex analysis.

Dream axioms. Realizability theory can be used to explore anti-classical dream axioms such as "any function $\mathbb{N} \to \mathbb{N}$ is computable", "any function $\mathbb{R} \to \mathbb{R}$ is continuous", or "there is precisely one model of Heyting arithmetic". As classically trained mathematicians, we deem these statements to be wildly false. Realizability theory presents a consistent world in which they are true, the former even trivially true. We can't explore the consequences of these axioms in a classical theory, since there they imply $\bot$; but we can, and it's fruitful to do so, using intuitionistic logic.

We subscribe to Andrej Bauer's *pluralism* and Joel David Hamkin's *multiverse view* on mathematics: Classical mathematics is a very nice context to do mathematics in, but there are also other environments, on par with classical mathematics, which are too interesting and which contain beautiful mathematics. The various flavors of realizability theory provide such environments, and there are others as well. It's partly a historical accident that we've chosen to declare classical mathematics as the "one true" context to do mathematics in.

Irrespective of philosophical convictions, using realizability theory and other tools it's possible to explore worlds of mathematics which are different from the world we have chosen as our metatheory. Familiarity with other worlds allows us to appreciate all of them more deeply.

Metaproperties. There are many statements φ such that Peano arithmetic fails to prove either of φ and $\neg\varphi$, while still believing $\varphi \vee \neg\varphi$ to be true. In contrast, Heyting arithmetic and many other intuitionistic systems have the *disjunction property*:

$$\text{If } \mathrm{HA} \vdash \varphi \vee \psi, \text{ then } \mathrm{HA} \vdash \varphi \text{ or } \mathrm{HA} \vdash \psi.$$

In fact, Heyting arithmetic even has the *existence property*:

$$\text{If } \mathrm{HA} \vdash (\exists x : N.\ \varphi), \text{ then there is a number } x_0 \in \mathbb{N} \text{ such that } \mathrm{HA} \vdash \varphi[\underline{x_0}/x].$$

Both of these properties can be verified using realizability theory. Realizability theory can also be used to verify that Heyting arithmetic does *not* prove some specific statements, formalizing the intution "for a statement to be intuitionistically provable, it must be possible to write a program witnessing its truth".

Consistency proofs. Realizability theory allows to establish some relative consistency results. For instance, the consistency of Heyting arithmetic (and therefore Peano arithmetic) can be reduced to the consistency of Gödel's system T ("the first functional programming language").

Computability theory. Realizability theory provides a specially-adopted language for efficiently expressing and proving results in computability theory. For instance, in a typical introductory course on theoretical computer science one will encounter the result "the union of regular languages if effectively regular", which means that not only is the union of regular languages again regular, but also that the finite automaton witnessing the regularity of the union can be computed given witnessing automata of the individual languages.

We'll learn how, using realizability theory, it suffices to give an intuitionistic proof of the weaker-looking proposition "the union of regular languages is regular" to establish this result. The technique is perfectly general and not restricted to this particular example.

Computable analysis. todo

4.2. **Background on computability theory.** We assume that the reader is superficially familiar with Turing machines.

If M is a Turing machine and x is a natural number, we say "$M(x)$ is defined" if and only if the execution of M on a tape which initially consists of x ones and zeros thereafter halts. In this case, we write "$M(x) = y$" if and only if, after halting, the tape begins with y ones followed exclusively by zeros.

We recall the following fundamental facts from computability theory.

Theorem 4.1. *A partial function $\mathbb{N} \rightharpoonup \mathbb{N}$ is computable in the sense of Definition 3.10 if and only if it has the same behavior as a Turing machine.*

Theorem 4.2. *There is no* halting oracle*, a Turing machine which given (a code for a) Turing machine correctly halts with output 1 or 0, depending on whether the given machine halts or doesn't halt.*

Theorem 4.3. *There is an enumeration $M_0, M_1, \ldots$ of all Turing machines such that*

(1) *there exists a* universal Turing machine *U, a machine which is capable of simulating any Turing machine on any input:*
$$U(\langle n, x\rangle) = M_n(m)$$
The angle brackets denote the pairing function J from Lemma 3.13.

(2) *There exists a machine S such that*
$$S(\langle n, x\rangle) \text{ is defined and } M_{S(\langle n,x\rangle)}(y) = M_n(\langle x, y\rangle).$$

(3) *There exists a machine E such that*
$$E(p) \text{ is defined and } M_{E(p)}(x) = M_p(\langle E(p), x\rangle).$$
The machine E allows to build self-referential machines.

If a Turing machine M is the n-th Turing machine in this enumeration, we say that n is the *index* of M.

4.3. **Kleene's number realizability.** alternate universe, can reason in it; mention that it's the first-order part of the internal language of the effective topos

Definition 4.4 (Kleene's number realizability)**.** We recursively define a relation $(\Vdash)$ between numbers and formulas of arithmetic by the following clauses. We write "$\Vdash \varphi$" if and only if there is a number r such that $r \Vdash \varphi$; in this case, we say that φ is *realized* by r.

$$\begin{array}{lcl}
r \Vdash \top & :\Longleftrightarrow & \top \\
r \Vdash \bot & :\Longleftrightarrow & \bot \\
r \Vdash s = t & :\Longleftrightarrow & [\![s]\!] = [\![t]\!] \\
r \Vdash (\varphi \wedge \psi) & :\Longleftrightarrow & (K(r) \Vdash \varphi) \wedge (L(r) \Vdash \varphi) \\
r \Vdash (\varphi \vee \psi) & :\Longleftrightarrow & (K(r) = 0 \wedge L(r) \Vdash \varphi) \vee (K(r) = 1 \wedge L(r) \Vdash \psi) \\
r \Vdash (\varphi \Rightarrow \psi) & :\Longleftrightarrow & \forall s : \mathbb{N}.\ (s \Vdash \varphi) \Rightarrow (M_r(s) \text{ is defined and } M_r(s) \Vdash \psi) \\
r \Vdash (\forall x : N.\ \varphi) & :\Longleftrightarrow & \forall x_0 : \mathbb{N}.\ (M_r(x_0) \text{ is defined and } M_r(x_0) \Vdash \varphi[\underline{x_0}/x]) \\
r \Vdash (\exists x : N.\ \varphi) & :\Longleftrightarrow & L(r) \Vdash \varphi[\underline{K(r)}/x]
\end{array}$$

The functions K and L are the projection functions from Lemma 3.13.

Lemma 4.5. *Let r be a number and φ be a closed formula of arithmetic. Then:*

(1) *$r \Vdash \neg\varphi$ if and only if there is no realizer of φ.*

(2) $r \Vdash \neg\neg\varphi$ *if and only if it's* not not *the case that there exists a realizer of* φ.

Proof. Instructive unraveling of the definition. □

The realizers of negated statements *bear no relevance* to the realized statement: If φ is not realizable, then *any* number is a realizer for $\neg\varphi$. Similarly, if φ is *not not* realizable, then *any* number is a realizer for $\neg\neg\varphi$. These observations express an important property of realizability. On the one hand, we'll make good use of them. On the other hand, they also show that we can't think of realizers as expressing "the mathematical content" of a proof. For instance, the realizer for Fermat's last theorem ($\forall n, x, y, z.\ n \geq 3 \wedge x, y, z \geq 1 \Rightarrow \neg(x^n + y^n = z^n)$) is a *trivial Turing machine*. In contrast, Wiles and Taylor's proof of Fermat's last theorem can't by any stretch of imagination be called trivial. This conundrum is *Schwichtenberg's paradox*.

Example 4.6. A (formal translation of the) statement "for any number n, there is a prime number $p > n$" is realized by (the index of a) Turing machine which given a number n outputs a number u such that $K(u)$ is a prime number with $K(u) > n$ (and such that $L(u)$ is a realizer for the statement "$\underline{K(u)}$ is a prime number greater than $\underline{n}$").

Example 4.7. The statement "any number is prime or not prime" is realized by (the index of a) Turing machine which given a natural number n outputs either $\langle 0, u\rangle$ or $\rangle 1, u\rangle$, depending on whether n is prime or not. The number u should be a realizer of the statement "$\underline{n}$ is prime" respectively "$\underline{n}$ is not prime", but this doesn't pose a restriction.

Example 4.8. The statement "for any number n, the n-th Turing machine halts or doesn't halt" is not realized. Indeed, a realizer would be a Turing machine which given a Turing machine decides whether it halts or not and outputs $\langle 0, m\rangle$ in the first case, where m is the number of the halting step, and $\langle 1, u\rangle$ in the second case, where u is an arbitrary number. (This uses that a formal rendition of "M halts" is of the form "there is a number m such that M halted after step m.) From such a Turing machine, we could trivially obtain a halting oracle.

Theorem 4.9 (Soundness of intuitionistic reasoning for realizability)**.** (1) *Let* φ *be a closed formula of arithmetic. If* $\mathrm{HA} \vdash \varphi$*, then* $\Vdash \varphi$.

(2) *Assume that Heyting arithmetic shows* $\varphi \vdash_{\vec{x}} \psi$*. Let* $\vec{x}_0$ *be natural numbers. If* $\Vdash \varphi[\vec{x}_0/\vec{x}]$*, then* $\Vdash \psi[\vec{x}_0/\vec{x}]$.

Proof. It's very instructive to verify this for oneself. Claim (2) follows from (1); to establish claim (1), one shows by induction on the structure of proofs that $\varphi \vdash_{\vec{x}} \psi$ implies $\Vdash (\forall \vec{x} : \vec{N}.\ (\varphi \Rightarrow \psi))$. □

We'll also put the following variants of realizability to good use.

Definition 4.10. We write "$\Vdash^p \varphi$" if and only if there is a number r such that $r \Vdash^p \varphi$. The relation $(\Vdash^p)$ is recursively defined by same clauses as $(\Vdash)$, only that for the cases $\Rightarrow$ and $\forall$ we

demand additional existence of proofs:

$$
\begin{aligned}
r \Vdash^p \top &\quad :\Longleftrightarrow \quad \top \\
r \Vdash^p \bot &\quad :\Longleftrightarrow \quad \bot \\
r \Vdash^p s = t &\quad :\Longleftrightarrow \quad [\![s]\!] = [\![t]\!] \\
r \Vdash^p (\varphi \wedge \psi) &\quad :\Longleftrightarrow \quad (K(r) \Vdash^p \varphi) \wedge (L(r) \Vdash^p \varphi) \\
r \Vdash^p (\varphi \vee \psi) &\quad :\Longleftrightarrow \quad (K(r) = 0 \wedge L(r) \Vdash^p \varphi) \vee (K(r) = 1 \wedge L(r) \Vdash^p \psi) \\
r \Vdash^p (\varphi \Rightarrow \psi) &\quad :\Longleftrightarrow \quad \big(\forall s : \mathbb{N}.\ (s \Vdash^p \varphi) \Rightarrow (M_r(s) \text{ is defined and } M_r(s) \Vdash^p \psi)\big) \wedge \\
&\qquad\qquad \mathrm{HA} \vdash (\varphi \Rightarrow \psi) \\
r \Vdash^p (\forall x : N.\ \varphi) &\quad :\Longleftrightarrow \quad \big(\forall x_0 : \mathbb{N}.\ (M_r(x_0) \text{ is defined and } M_r(x_0) \Vdash^p \varphi[\underline{x_0}/x])\big) \wedge \\
&\qquad\qquad \mathrm{HA} \vdash (\forall x : N.\ \varphi) \\
r \Vdash^p (\exists x : N.\ \varphi) &\quad :\Longleftrightarrow \quad L(r) \Vdash^p \varphi[\underline{K(r)}/x]
\end{aligned}
$$

Definition 4.11. We define *Aczel's slash predicate* $(|)$ for closed formulas of arithmetic by the following clauses.

$$
\begin{aligned}
| \top &\quad :\Longleftrightarrow \quad \top \\
| \bot &\quad :\Longleftrightarrow \quad \bot \\
| s = t &\quad :\Longleftrightarrow \quad [\![s]\!] = [\![t]\!] \\
| (\varphi \wedge \psi) &\quad :\Longleftrightarrow \quad (| \varphi) \wedge (| \psi) \\
| (\varphi \vee \psi) &\quad :\Longleftrightarrow \quad (| \varphi) \vee (| \psi) \\
| (\varphi \Rightarrow \psi) &\quad :\Longleftrightarrow \quad \big((| \varphi) \Rightarrow (| \psi)\big) \wedge (\mathrm{HA} \vdash (\varphi \Rightarrow \psi)) \\
| (\forall x : N.\ \varphi) &\quad :\Longleftrightarrow \quad \big(\forall x_0 : \mathbb{N}.\ (| \varphi[\underline{x_0}/x])\big) \wedge (\mathrm{HA} \vdash (\forall x : N.\ \varphi)) \\
| (\exists x : N.\ \varphi) &\quad :\Longleftrightarrow \quad \exists x_0 : \mathbb{N}.\ (| \varphi[\underline{x_0}/x])
\end{aligned}
$$

Proposition 4.12. *Let φ be a closed formula of arithmetic. If $| \varphi$ or $\Vdash^p \varphi$, then $\mathrm{HA} \vdash \varphi$. Conversely, if $\mathrm{HA} \vdash \varphi$, then $| \varphi$ and $\Vdash^p \varphi$.*

Proof. The first claim is by an easy induction on the structure of φ. The definitions of $|$ and $\Vdash^p$ are made exactly in such a way that the cases which would be nontrivial ($\forall$ and $\Rightarrow$) are in fact trivial. To verify the converse, one proceeds as in the proof of **??**. □

4.4. **Metaproperties of Heyting arithmetic.**

Theorem 4.13. *Heyting arithmetic has the* disjunction property*: If $\mathrm{HA} \vdash \varphi \vee \psi$, then $\mathrm{HA} \vdash \varphi$ or $\mathrm{HA} \vdash \psi$.*

proof

Theorem 4.14. *Heyting arithmetic has the* existence property*: If $\mathrm{HA} \vdash (\exists x : N.\ \varphi)$, then there is a natural number n_0 such that $\mathrm{HA} \vdash \varphi[\underline{n_0}/x]$.*

proof

Theorem 4.15. *Assume that* $\mathrm{HA} \vdash (\forall x : N.\ \exists y : N.\ \varphi)$. *Then there is a computable function* $f : \mathbb{N} \to \mathbb{N}$ *(even provably total in* HA*) such that, for all numbers* n, $\mathrm{HA} \vdash \varphi[\underline{n}/x, \underline{f(n)}/y]$ *(even* $\mathrm{HA} \vdash (\forall n : N.\ \varphi[n/x, f(n)/y])$*).*

proof

Theorem 4.16. *Peano arithmetic is not a conservative extension of Heyting arithmetic in the strict sense that there are formulas* φ *such that* $\mathrm{PA} \vdash \varphi$ *but not* $\mathrm{HA} \vdash \varphi$.

proof

Lemma 4.17. *Let* φ *be a closed formula of arithmetic.*

(1) *If* φ *is built using only* $\top\ \bot\ \wedge\ =$*, then, for any number* r, $r \Vdash \varphi$ *if and only if* $\mathbb{N} \models \varphi$.
(2) *If* φ *is a geometric formula (so built using only* $\top\ \bot\ \wedge\ \vee\ \exists\ =$*), then* $\Vdash \varphi$ *if and only if* $\mathbb{N} \models \varphi$*. (The realizers of such statements are still rather trivial and devoid of particular computational content, but they're not completely arbitrary as in (a).)*

Proof. By induction on the structure of φ. □

realizability as a formula translation
more examples

4.5. **Going beyond the natural numbers.** The realizability interpretation can be extended to talk about more general objects than natural numbers.

Definition 4.18. An *assembly* is a set X together with a relation $(\Vdash_X) \subseteq \mathbb{N} \times X$ such that for every $x \in X$, there is a number n such that $n \Vdash_X x$. We say that n is a *realizer* for x. We'll occasionally write "$|X|$" for the underlying set of an assembly X.

An assembly can be pictured as a set for which we know how to represent its elements in a computer. As is often the case in computer science, the same abstract element $x \in X$ may be coded by many different realizers.

Example 4.19. The set $\mathbb{N}$ together with the diagonal relation (declaring that $n \Vdash_{\mathbb{N}} m$ if and only if $n = m$) is an assembly, commonly denoted "$\mathbb{N}$".

Example 4.20. The set of all computable functions $\mathbb{N} \to \mathbb{N}$ can be made into an assembly, by declaring that the realizers of a function $f : \mathbb{N} \to \mathbb{N}$ are the indices of Turing machines computing f. It's a fact from computability theory that one cannot compute canonical realizers for such functions; therefore this example really needs the flexibility of assemblies allowing multiple realizers for the same abstract element.

Definition 4.21. A *modest set* is an assembly X such that realizers represent precisely one element: If $n \Vdash_X x$ and $n \Vdash_X y$, then $x = y$.

Modest sets are modest in the sense that the underlying sets of modest sets are countable, at least if the metalogic is classical. The precise statement is that for any modest set X, there is a partial surjection $\mathbb{N} \rightharpoonup |X|$, sending a number to the (unique if existing) abstract element it realizes.

4.6. **Exploring the formal Church–Turing thesis.** Classically, there are of course many functions which are not computable, such as the halting function or the Busy Beaver function:

$$n \longmapsto \begin{cases} 1, & \text{if } M_n \text{ halts on empty input,} \\ 0, & \text{otherwise} \end{cases}$$

$$n \longmapsto \max\{v \in \mathbb{N} \mid v \text{ is the output of a halting Turing machine with} \leq n \text{ states}\}$$

These two descriptions yield well-defined total functions only thanks to the law of excluded middle, which guarantees that any Turing machine halts or doesn't halt. It turns out that *all* examples of non-computable functions necessarily require some logical principle going beyond intuitionistic logic in order to verify that they're total.

This is because intuitionistically, it's consistent to assume that *any* function $\mathbb{N} \to \mathbb{N}$ is computable. This is the fundamental axiom of *recursive mathematics*, one of the many schools of constructive mathematics. It is valid in the realizability model.

Definition 4.22. The *formal Church–Turing thesis* (CT) is the statement that any function $\mathbb{N} \to \mathbb{N}$ is computable by a Turing machine. Put in the language of HA^ω:

$$\forall f : N^N.\ \exists e : N.\ \forall x : N.\ f(x) = U(\langle e, x \rangle).$$

The application of U, the universal Turing machine, has to be coded as an arithmetical formula as discussed in Section 3.1.

It's not possible to formalize the formal Church–Turing thesis as

$$\text{“}\forall f : N^N.\ \exists e : N.\ \forall x : N.\ f(x) = M_e(x)\text{”},$$

as the notation M_e is only defined for numerals of the meta language.

Proposition 4.23. *The formal Church–Turing thesis is realized.*

Proof. Instructive exercise. □

cite kls: Georg Kreisel, Daniel Lacombe, and Joseph R. Shoenfield (1957), “Partial recursive functionals and effective operations.” In Constructivity in mathematics: proceedings of the colloquium held in Amsterdam, 1957 (A. Heyting, ed.), 195–207, North Holland Publishing Co, and ceitin: “Algorithmic operators in constructive metric spaces.” Trudy Mat. Inst. Steklov., 67, 295–361

also cite Roger /Recursive Functions and Effective Computability/ (page 362f.) and Beeson /Foundations of Constructive Mathematics/ (page 62)

also cite Thm. 9.2.1 of Longley/Normann

Theorem 4.24 (Kreisel–Lacombe–Shoenfield [?], Ceitin [?])**.** *Assume Markov's Principle in the metatheory. In the realizability model, any function $\mathbb{N}^{\mathbb{N}} \to \mathbb{N}$ is pointwise continuous. More precisely:*

$$\Vdash \forall f : \mathbb{N}^{(\mathbb{N}^{\mathbb{N}})}.\ \forall \alpha : \mathbb{N}^{\mathbb{N}}.\ \exists M : \mathbb{N}.\ \forall \beta : \mathbb{N}^{\mathbb{N}}.\ (\forall m < M.\ \alpha(m) = \beta(m)) \Rightarrow f(\alpha) = f(\beta).$$

Proof. We are to construct a Turing machine which inputs

(1) a realizer e for a function $f : |\mathbb{N}^{\mathbb{N}}| \to \mathbb{N}$ and

(2) a realizer r for a function $\alpha : \mathbb{N} \to \mathbb{N}$

and outputs a number M such that $f(\alpha) = f(\beta)$ for all computable $\beta : \mathbb{N} \to \mathbb{N}$ with $\alpha(m) = \beta(m)$ for $m < M$. Recall that $|\mathbb{N}^{\mathbb{N}}|$ is the set of all computable functions $\mathbb{N} \to \mathbb{N}$. The machine should also output a realizer for that statement, but given that it's true, realizers for it are trivial.

We'll repeatedly use that M_e satisfies the following extensionality property: If r and s are both realizers for some (total) function $\mathbb{N} \to \mathbb{N}$ (that is, if r and s are indices of Turing machines computing that function), then the computations of $M_e(r)$ and $M_e(s)$ both terminate and yield the same result. So the machine M_e does have access to the source code (the index) of its given function and can use it, for instance, to short-circuit based on some syntactical analyses. It is, however, restricted in its use of the source code by the extensionality condition. This leads to the intuition that the only thing of real consequence which M_e can do is simulate its argument on various inputs. Because the computation $M_e(r)$ needs to terminate in finitely many steps, only finitely many runs of r can be simulated. This is the intuitive reason why $f(\alpha)$ depends only on an initial segment of α.

Here's an outline of how we'll prove the theorem. Given realizers e and r as above, we'll specially craft a Turing machine M_s which will behave just like M_r up to some input value and which won't terminate on inputs larger than this threshold (a "ticking time bomb"). We'll ensure that, nevertheless, the computation $M_e(s)$ does halt after some finite number of steps. This number of steps will be the number M we're looking for.

If v is a finite list of natural numbers, we write $v^{\$}$ for some canonical index of a Turing machine such that $M_{v^{\$}}(m)$ is the element v_m if the length of v is greater than m, and zero otherwise.

The Turing machine we're looking for proceeds as follows.

> Input a realizer e for f and a realizer r for α. By employing the machine E of Theorem 4.3, construct a machine with index s (computing a partial function $\mathbb{N} \rightharpoonup \mathbb{N}$) which proceeds as follows:
>
> Input a natural number n.
> Check whether the computation $M_e(s)$ halts in $\leq n$ steps.
> If not: Output $M_r(n)$.
> If yes: Check whether $M_e(s) = M_e(r)$.
> If not: Output $M_r(n)$.
> If yes: Determine the number w of steps needed for computing $M_e(s)$.
> Search for a finite extension v of the list $[M_r(0), \ldots, M_r(w-1)]$ such that $M_e(v^{\$}) \neq M_e(r)$ in a systematic fashion.
> When found, output $M_{v^{\$}}(n)$.
>
> Output the number of steps needed for computing $M_e(s)$.

Let e be a realizer for a function $f : |\mathbb{N}^{\mathbb{N}}| \to \mathbb{N}$ and r be a realizer for a function $\alpha : \mathbb{N} \to \mathbb{N}$. We'll now verify the following claims about the machine M_s we described.

(1) The computation $M_e(s)$ does *not not* terminate.
(2) The computation $M_e(s)$ terminates. In the following, let M be the number of steps needed for computing $M_e(s)$.

(3) $M_e(s) = M_e(r)$.
(4) $f(\alpha) = f(\gamma)$ for all computable functions $\gamma : \mathbb{N} \to \mathbb{N}$ such that $\alpha(m) = \gamma(m)$ for all $m < M$ and such that there is a number Q such that $\gamma(m) = 0$ for all $m \geq Q$.
(5) $f(\alpha) = f(\beta)$ for all computable functions $\beta : \mathbb{N} \to \mathbb{N}$ such that $\alpha(m) = \beta(m)$ for all $m < M$.

Regarding the first claim, if $M_e(s)$ fails to terminate, then by construction M_s behaves just like M_r. By the extensionality property of M_e, the computation $M_e(s)$ therefore has to terminate (with the same value as $M_e(r)$), a contradiction. By Markov's Principle, the computation $M_e(s)$ therefore halts in some number M of steps.

If $M_e(s) \neq M_e(r)$, then again by construction M_s behaves just like M_r. Thus $M_e(s) = M_e(r)$, a contradiction.

Let γ be a function as above. If $f(\alpha) \neq f(\gamma)$, then the search undertook by M_s will succeed in finding a suitable finite list v, because there is at least one suitable finite list, namely $[\gamma(0), \ldots, \gamma(Q-1)]$. Thus $M_s(n)$ will be $M_{v^\$}(n)$ for $n \geq M$, and also for $n < M$ since $\beta(n) = \alpha(n)$ for $n < M$. Thus M_s behaves just like $M_{v^\$}$. Extensionality ensures $M_e(s) = M_e(v^\$)$, contradicting the facts $M_e(s) = M_e(r)$ and $M_e(v^\$) \neq M_e(r)$.

Finally, let β be a function as above. Let r' be a realizer for β. Let M' be the number of steps for computing $M_e(s')$, where s' is the index of a machine which is constructed just like M_s, but with all occurences of r replaced by r'. Let $\gamma : \mathbb{N} \to \mathbb{N}$ be the function which behaves like β for inputs smaller than $\max\{M, M'\}$ and which is zero for all other inputs. Then $f(\beta) = f(\gamma)$ by the analog of claim (4) for β instead of α and $f(\gamma) = f(\alpha)$ by claim (4). □

no uniform continuity
no uniform continuity even for functions $\mathbb{B}^{\mathbb{N}} \to \mathbb{N}$, but mention other models

The following theorem is to be read in the setting of an intuitionistic set theory. We'll later learn that its statement and its proof can be interpreted in the internal language of the effective topos.

cite Benno van den Berg and Jaap van Oosten (https://www.staff.science.uu.nl/~ooste110/realizability/arithcatsubmit.pdf); and cite McCarty and Tennenbaum

Theorem 4.25 (Categoricity of arithmetic)**.** *Assuming Markov's Principle and the formal Church–Turing thesis, there is (up to unique isomorphism) precisely one model of Heyting arithmetic.*

Proof. Let M be a model of Heyting arithmetic. The canonical map $\mathbb{N} \to M$ sending n to $[\![s^n(0)]\!]$ is injective and preserves zero, addition, and multiplication. We're therefore left with the task to show that this map is surjective, that is, that every element of M is standard.

So let $c : M$ be an arbitrary element. We'll verify that c is *not not* standard. By Markov's Principle, this suffices to establish that c is standard, since for a fixed number $n \in \mathbb{N}$ the statement "$c = [\![s^n(0)]\!]$" is decidable, because Heyting arithmetic proves $\forall x, y : N.\ x = y \vee x \neq y$.

Assume that c is not standard. We define the sets

$$R := \{n : \mathbb{N} \mid M \models (M_n(n) \text{ halts in less than } c \text{ steps with result } 0)\},$$
$$A := \{n : \mathbb{N} \mid M_n(n) \text{ halts with value } 0\},$$
$$B := \{n : \mathbb{N} \mid M_n(n) \text{ halts with value } 1\}.$$

Then $A \subseteq R$, since if $M_n(n)$ halts with value 0 in m steps, where m is a natural number, then this statement is provable in Heyting arithmetic (even intuitionistic Robinson arithmetic) and therefore valid in M. Thus $n \in R$ by $M \models \underline{m} < c$.

Similarly $B \subseteq \mathbb{N} \setminus R$.

Since Heyting arithmetic proves for any n and x that either $M_n(n)$ halts in less than x steps with result 0 or not, the set R is a *detachable* subset of $\mathbb{N}$: For any number $n : \mathbb{N}$ we have $n \notin R$ or $n \in R$. The function $f : \mathbb{N} \to \mathbb{N}$ mapping n to 0 or 1 depending on whether $n \notin R$ or $n \in R$ is therefore a well-defined total function. By the formal Church–Turing thesis, this function is computable.

In computer science parlance, the sets A and B are therefore *recursively separable* (by R). But it's well-known that this isn't the case, by the following argument. Let e be the index of a Turing machine computing f. Thus M_e halts on any input n, with result 0 iff $n \notin R$ and with result 1 iff $n \in R$. In particular, we must have $e \in A$ or $e \in B$. In the first case we have $e \in R$ (because $A \subseteq R$) and $e \notin R$ (because $M_e(e) = 0$). In the second case we have $e \in \mathbb{N} \setminus R$ (because $B \subseteq \mathbb{N} \setminus R$) and $e \in R$ (because $M_e(e) = 1$). Thus we obtain a contradiction. □

Corollary 4.26. *Assuming Markov's Principle and the formal Church–Turing thesis, Peano arithmetic doesn't have any model.*

Proof. Let M be a model of Peano arithmetic. This model is trivially also a model of Heyting arithmetic. By Theorem 4.25, it is isomorphic to the standard model $\mathbb{N}$.

Since Peano arithmetic proves that any Turing machine halts or doesn't halt and $\mathbb{N}$ is a model of Peano arithmetic, it's actually true that any Turing machine halts or doesn't halt. Therefore the function

$$\mathbb{N} \longrightarrow \mathbb{N},\ n \longmapsto \begin{cases} 1, & \text{if } M_n \text{ halts on empty input,} \\ 0, & \text{else} \end{cases}$$

is well-defined and total. By the formal Church–Turing thesis, it is computable by a Turing machine. This contradicts the basic fact that there is no halting oracle. □

If we predicate our notion of truth on what a mathematician accepting Markov's Principle believes to be valid in the effective topos, we can therefore enjoy the following anticlassical phenomena.

Firstly, unlike in a classical context where we can show that there are precisely $|P(\mathbb{N})|$ models of Heyting arithmetic (up to elementary equivalence), there is precisely one model of Heyting arithmetic, the standard model. Thus the axioms of Heyting arithmetic do uniquely capture what they were originally set out to capture, the intended model.

In fact, a careful analysis of what the proof of Theorem 4.25 actually required shows that even the weak fragment of Heyting arithmetic with the induction scheme restricted to Σ_1-formulas has $\mathbb{N}$ as its unique model [?]. Since this fragment is finitely axiomatizable,[8] this observation shows that the notion of natural numbers can be uniquely captured by finitely many axioms.

[8]Since any quantifer-free formula with two free variables n and a can be put into the form $M_e(n, a) = 0$ for some number e, it suffices to have the induction axiom for the single (open) formula $\exists a : N.\ M_e(n, a) = 0$.

Secondly, Peano arithmetic is "quasi-inconsistent" in that it doesn't have any models. (Of course, Peano arithmetic is still consistent in that it doesn't prove $\bot$, as the equiconsistency of HA and PA is a theorem of Heyting arithmetic and much weaker systems.)

Finally, moving from logical phenomena to analytic ones, we have the pleasant fact that any function $\mathbb{R} \to \mathbb{R}$ is pointwise continuous.

However, there are also downsides of this recursive setting. For instance, semantic completeness fails: From a statement being valid in the unique model of Heyting arithmetic (so in all models) we can't deduce that it's provable in Heyting arithmetic. For instance, the statement that it's not true that any Turing machine halts or doesn't halt is true but not provable.

4.7. **Modified realizability.** Gödel's system T
MP is not modified-realized

5. Proof mining

5.1. **Constructive analysis.** It's easy to verify, in an intuitionistic metatheory, that the rational numbers form an ordered field. For any $x : \mathbb{Q}$, we have $x < 0$, $x = 0$, or $x > 0$. Let $\mathbb{Q}_{\geq 0}$ be the subset of nonnegative rational numbers and let $\mathbb{Q}_{>0}$ be the subset of positive rational numbers.

Definition 5.1. A *metric space* is a set X together with a relation $R \subseteq X \times X \times \mathbb{Q}_{\geq 0}$, where we agree to write "$d(x, y) \leq \varepsilon$" instead of "$(x, y, \varepsilon) \in R$", such that:

(1) $d(x, x) \leq 0$ for all $x : X$.
(2) $d(x, y) \leq 0$ implies $x = y$, for all $x, y : X$.
(3) $d(x, y) \leq \varepsilon$ implies $d(y, x) \leq \varepsilon$, for all $x, y : X$, $\varepsilon : \mathbb{Q}_{\geq 0}$.

Definition 5.2. The set $\mathbb{R}_{\mathrm{d}}$ of *Dedekind real numbers* is the set of all pairs (L, U) of sets of rational numbers such that:

(a) L is inhabited.
(ã) U is inhabited.
(b) L is downward-closed: if $x < y$ and $y \in L$, then $x \in L$.
(b̃) U is upward-closed: if $x < y$ and $x \in U$, then $y \in L$.
(c) L is upward-open: if $x \in L$, then $y \in L$ for some $y > x$.
(c̃) U is downward-open: if $y \in U$, then $x \in U$ for some $x < y$.
(d) Relative position: if $x \in L$ and $y \in U$, then $x < y$.
(e) The cut is *located*: if $x < y$, then $x \in L$ or $y \in U$.

Definition 5.3. A *Cauchy process* in a metric space X is a map $\alpha : \mathbb{Q}_{>0} \to P(X)$ such that the set $\alpha(\varepsilon)$ is inhabited for all $\varepsilon : \mathbb{Q}_{>0}$ and such that $\alpha \sim \alpha$, where

$$\alpha \sim \beta \quad :\Longleftrightarrow \quad \forall \varepsilon, \delta : \mathbb{Q}_{>0}.\ \forall x \in \alpha(\varepsilon), y \in \beta(\delta).\ d(x, y) \leq \varepsilon + \delta.$$

The intuition is that all the elements $x \in \alpha(\varepsilon)$ are approximations of the ideal limit represented by α which are accurate up to ε; symbolically $d(x, \alpha) \leq \varepsilon$. As soon as we'll have fixed the meaning of this statement, we'll see that it's actually correct.

Definition 5.4. A *Cauchy series* in a metric space X is a map $x : \mathbb{Q}_{>0} \to X$ such that $d(x(\varepsilon), x(\delta)) \leq \varepsilon + \delta$ for all $\varepsilon, \delta : \mathbb{Q}_{>0}$.

This definition doesn't quite look like the usual definition found in textbooks. The usual definition uses $\mathbb{N}$ in place of $\mathbb{Q}_{>0}$; this difference is not material, since one can convert Cauchy sequences of the one kind into Cauchy sequences of the other. The nontrivial difference is that we require a fixed rate of convergence. If we defined a Cauchy series to be a map $x : \mathbb{N} \to X$ such that there is a function $f : \mathbb{N} \to \mathbb{N}$ with $d(x_k, x_l) \leq 1/(n+1)$ for all $k, l \geq f(n)$, the resulting concept would again be equivalent to Cauchy series in our sense. However, if we required only that for all $n : \mathbb{N}$ there exists a number N such that $d(x_k, x_l) \leq 1/(n+1)$ for all $k, l \geq N$, then the resulting concept would in general not be equivalent in the absence of the countable axiom of choice.

We can picture a Cauchy process as a non-deterministic variant of a Cauchy series. While a Cauchy series has to commit itself to one specific approximation for each error bound ε, a Cauchy process may yield different approximations $x \in \alpha(\varepsilon)$ each time it's asked. The only condition is that the supplied approximations are consistent in that $\alpha \sim \alpha$ (thus in particular $d(x, x') \leq 2\varepsilon$ for all $x, x' \in \alpha(\varepsilon)$). For instance, a physical experiment might yield a different experimental value each time it's performed.

Definition 5.5. A Cauchy process α in a metric space X *converges* to a point $x_0 : X$ if and only if

$$\forall \varepsilon : \mathbb{Q}_{>0}.\ \forall x \in \alpha(\varepsilon).\ d(x, x_0) \leq \varepsilon.$$

A metric space X is *complete* if and only if any Cauchy process in X converges to some point.

The alternative condition that any Cauchy *sequence* converges is weaker and not very sensible in the absence of the countable axiom of choice.

Proposition 5.6. *There is a universal (left-adjoint) way of completing any metric space, by associating to X the space*

$$CX := (\textit{set of all Cauchy processes})/\sim$$

with metric defined by

$$d([\alpha], [\beta]) \leq q \quad :\Longleftrightarrow \quad \forall \varepsilon, \delta : \mathbb{Q}_{>0}.\ \forall x \in \alpha(\varepsilon), y \in \beta(\delta).\ d(x, y) \leq q + \varepsilon + \delta.$$

Proof. The claim is that CX is a complete metric space and that any uniformly continuous map $X \to Y$ into a complete metric space extends in a unique fashion to a uniformly continous map $CX \to Y$.

Here we'll only verify that CX is complete. Let $A : \mathbb{Q}_{>0} \to CX$ be a Cauchy process. Define a Cauchy process $\beta : \mathbb{Q}_{>0} \to X$ by

$$\beta(\varepsilon) := \{x \in \mathbb{Q} \mid \exists \varepsilon', \varepsilon'' : \mathbb{Q}_{>0}.\ \exists \alpha \in A(\varepsilon').\ \varepsilon' + \varepsilon'' \leq \varepsilon \wedge x \in \alpha(\varepsilon'')\}.$$

Then we can verify that A converges to $[\beta]$ in CX. □

In the absence of the countable axiom of choice, the metric space $\widetilde{C}X$ of Cauchy *sequences* in X (up to equivalence) can't be verified to be complete in our sense. In fact, it can't even be shown to be complete in the usual sense that any Cauchy sequence converges. The reason is that, given a Cauchy sequence $(A_\varepsilon)_\varepsilon$ in $\widetilde{C}X$, we have to *choose* representatives $x^{(\varepsilon)}$ such that $A_\varepsilon = [(x^{(\varepsilon)})_\varepsilon]$. Only then we can pass to a *diagonal sequence* like $(x^{(\varepsilon/2)})_{\varepsilon/2}$.

Definition 5.7. The *space of real numbers* $\mathbb{R}$ is the completion of $\mathbb{Q}$, that is the space of $\mathbb{Q}$-valued Cauchy processes modulo equivalence. We define:

$$\begin{aligned}
[\alpha] < [\beta] &:\Longleftrightarrow \exists \varepsilon, \delta : \mathbb{Q}_{>0}.\ \exists x \in \alpha(\varepsilon), y \in \beta(\delta).\ x < y - \varepsilon - \delta \\
x \# y &:\Longleftrightarrow x < y \vee y < x \\
x > y &:\Longleftrightarrow y < x \\
x \leq y &:\Longleftrightarrow \neg(x > y) \\
x \geq y &:\Longleftrightarrow y \leq x
\end{aligned}$$

Our definition of the less-than relation is independent from the particular representatives by the following lemma.

Lemma 5.8. *The following statements about $\mathbb{Q}$-valued Cauchy processes α, β are equivalent:*

(1) $[\alpha] < [\beta]$.
(2) $\exists \varepsilon, \delta : \mathbb{Q}_{>0}.\ \exists x \in \alpha(\varepsilon), y \in \beta(\delta).\ x < y - \varepsilon - \delta$.
(3) $\exists \varepsilon, \delta : \mathbb{Q}_{>0}.\ \exists x \in \alpha(\varepsilon), y \in \beta(\delta).\ x < y - 3\varepsilon - 3\delta$.
(4) $\exists \mu : \mathbb{Q}_{>0}.\ \forall \omega, \eta \leq \mu.\ \forall x \in \alpha(\omega), y \in \beta(\eta).\ x < y - \omega - \eta$.

Lemma 5.9. *The following statements about $\mathbb{Q}$-valued Cauchy processes α, β are equivalent:*

(1) $\alpha \# \beta$.
(2) $\exists \varepsilon, \delta : \mathbb{Q}_{>0}.\ \exists x \in \alpha(\varepsilon), y \in \beta(\delta).\ |x - y| > \varepsilon + \delta$.
(3) $\exists \varepsilon, \delta : \mathbb{Q}_{>0}.\ \exists x \in \alpha(\varepsilon), y \in \beta(\delta).\ |x - y| > 3\varepsilon + 3\delta$.
(4) $\exists \mu : \mathbb{Q}_{>0}.\ \forall \omega, \eta \leq \mu.\ \forall x \in \alpha(\omega), y \in \beta(\eta).\ |x - y| > \omega + \eta$.

Proposition 5.10. (1) *The statement "$\forall x : \mathbb{R}.\ \neg(x = y) \Rightarrow x \# y$" is equivalent to the limited principle of omniscience.*
(2) *Let $x, y : \mathbb{R}$. Then $\neg(x \# y)$ if and only if $x = y$.*
(3) *Let $x : \mathbb{R}$. Let $a, b : \mathbb{R}$ be such that $a < b$. Then $x > a$ or $x < b$.*

fill in proof
discuss other constructions of $\mathbb{R}$
discuss status of the intermediate value theorem
cite https://arxiv.org/abs/1510.00639 for recent results on Cauchy reals

5.2. **Proof mining in analysis.** dialectica interpretation

5.3. **Proof mining in algebra.** dynamical methods for eliminating prime ideals

6. Topos theory

6.1. **Locales.** defn frame and frame morphism
remark: arbitrary meets, Heyting implication
example: from topological spaces
defn locale and locale morphism
example: from topological space
example: pt

compactness
remark on Banach–Tarski

6.1.1. *Points.* defn: points
sober, spatial
Hausdorff implies sober, classically
filters

6.1.2. *The classifying locale of a propositional geometric theory.* defn
example: Dedekind reals
remark: $[0,1]$ not compact as a topological space
more examples (from the exercise sheet)
any locale classifies
example: Gelfand–Naimark

6.1.3. *Products and coproducts of locales.* ...

6.1.4. *Sublocales.* defn nucleus
examples: topological subspace, open, closed
categorical characterization
intersection and union of sublocales
dense sublocales
defn: comparison of sublocales
defn smallest dense sublocale
prop: points of a sublocale
ex: $\mathbb{R}_{\neg\neg}$ is pointless
prop: quotient theories $=$ sublocales
ex: special cases
generic model
illusion of points

6.2. **Sites.** Recall that we use "pre notation" for function composition, that is we write "$f \mathbin{⨾} g$" instead of "$g \circ f$".

Definition 6.1. A *site* is a small category $\mathcal{C}$ together with a *coverage* Cov which maps any object U of $\mathcal{C}$ to a set of sets of morphisms with target U, the set of *coverings* of U. The coverage is subject to the following condition:

(0) For any object U, for any covering $M \in \mathrm{Cov}(U)$, and any morphism $p : V \to U$ in $\mathcal{C}$, there is a covering $N \in \mathrm{Cov}(V)$ such that for all $V' \xrightarrow{g} V$ in N there is a morphism $U' \xrightarrow{f} U$ and a morphism $V' \xrightarrow{k} U'$ such that $g \mathbin{⨾} p = k \mathbin{⨾} f$.

$$\begin{array}{ccc} V' & \xrightarrow{k} & U' \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle f} \\ V & \xrightarrow[p]{} & U \end{array}$$

We'll often also require the following closure definitions, but we won't include them in the official definition of what a site is:

(1) For any object U, the singleton set $\{U \xrightarrow{\mathrm{id}_U} U\}$ is a covering of U.
(2) For any object U, any set L of morphisms with target U, and any covering $M \in \mathrm{Cov}(U)$, if for any $f \in M$ there is a covering $N \in \mathrm{Cov}(\mathrm{dom}(f))$ such that $N \setminus f \subseteq L$, then there is a covering $P \in \mathrm{Cov}(U)$ such that $P \subseteq L$.

The principal reason of existence for a site is that it gives rise to the notion of sheaves over it:

Definition 6.2. A *presheaf* on a site $\mathcal{C}$ is a functor $\mathcal{C}^{\mathrm{op}} \to \mathrm{Set}$. A *sheaf* on a site $\mathcal{C}$ is a presheaf F such that the following *sheaf axiom* holds:

> For any object U of $\mathcal{C}$, any covering $M \in \mathrm{Cov}(U)$, and any *matching family* $(s_f)_{f\in M}$ of elements $s_f \in F(\mathrm{dom}(f))$, there exists a unique element $s \in F(U)$ such that $F(f)(s) = s_f$ for all $f \in M$.

With "$\mathrm{dom}(f)$" we mean the domain of f, as in "$f : \mathrm{dom}(f) \to \mathrm{cod}(f)$". A family $(s_f)_{f\in M}$ of elements $s_f \in F(\mathrm{dom}(f))$ is *matching* if and only if for all objects V of $\mathcal{C}$, all morphisms $f, g \in M$, all morphisms $V \xrightarrow{a} \mathrm{dom}(f), V \xrightarrow{b} \mathrm{dom}(g)$ such that $a \setminus f = b \setminus g$, the elements $F(a)(s_f)$ and $F(b)(s_g)$ agree.

Definition 6.3. A *subsheaf* of a sheaf $F : \mathcal{C}^{\mathrm{op}} \to \mathrm{Set}$ is a sheaf $G : \mathcal{C}^{\mathrm{op}} \to \mathrm{Set}$ such that $G(U) \subseteq F(U)$ for all objects U and such that $G(f)(s) = F(f)(s)$ for all morphisms f in $\mathcal{C}$.

Definition 6.4. Let $\mathcal{C}$ be a site. The category $\mathrm{Sh}(\mathcal{C})$ of sheaves over $\mathcal{C}$ (with natural transformations as morphisms) is the *Grothendieck topos over* $\mathcal{C}$.

Example 6.5. Let $\mathcal{C}$ be the category with one object and one morphism (the "terminal category"). Either declare that the unique object of $\mathcal{C}$ doesn't have any coverings or declare that it has precisely one covering, namely the singleton set consisting of the identity morphism. With either declaration $\mathcal{C}$ becomes a site. Any presheaf $\mathcal{C}^{\mathrm{op}} \to \mathrm{Set}$ will satisfy the sheaf condition; the topos $\mathrm{Sh}(\mathcal{C})$ is equivalent to the category Set.

Example 6.6. Let $\mathcal{C}$ be a small category. Equipped with the coverage given by $\mathrm{Cov}(U) = \{\{U \xrightarrow{\mathrm{id}_U} U\}\}$, we obtain a site. Any presheaf $\mathcal{C}^{\mathrm{op}} \to \mathrm{Set}$ is a sheaf for this site. The category of sheaves over C is also denoted by "$\mathrm{PSh}(\mathcal{C})$", to stress that the coverage is trivial.

6.2.1. *Localic sites.*

Example 6.7. A locale X gives rise to a site $\mathrm{Ouv}(X)$ satisfying all three site axioms as follows.

(1) The objects of $\mathrm{Ouv}(X)$ are the opens of X.
(2) $\mathrm{Hom}_{\mathrm{Ouv}(X)}(u, v) = \{\star \mid u \leq v\}$. That is, if $u \leq v$, then we have exactly one morphism $u \to v$, and else we have none.
(3) A set M of morphisms with target u is a covering if and only if $\bigvee_{f\in M} \mathrm{dom}(f) = u$.

For the special case of the site associated to a locale X, the definition of what a sheaf is boils down to the following.

Definition 6.8. A *sheaf* F over a locale X is given by

- a set $F(u)$ for each open $u \in \mathrm{Ouv}(X)$ and
- a map $\mathrm{res}^u_v : F(u) \to F(v)$ for each pair of opens $u, v \in \mathrm{Ouv}(X)$ with $v \leq u$

such that

- the functor identities hold: $\mathrm{res}^u_u = \mathrm{id}_{F(u)}$ for $u \in \mathrm{Ouv}(X)$ and $\mathrm{res}^u_w = \mathrm{res}^u_v \circ \mathrm{res}^v_w$ for opens u, v, w such that $w \leq v \leq u$.
- the sheaf axioms holds: For any open $u \in \mathrm{Ouv}(X)$, any covering $u = \bigvee_i u_i$, and any matching family $(s_i)_i$ of elements $s_i \in F(u_i)$, there exists a unique element $s \in F(u)$ such that $\mathrm{res}^u_{u_i}(s) = s_i$ for all i.

A family $(s_i)_i$ of elements $s_i \in F(u_i)$ is *matching* if and only if $\mathrm{res}^{u_i}_{u_i \wedge u_j}(s_i) = \mathrm{res}^{u_j}_{u_i \wedge u_j}(s_j)$ for all i and j. The elements of $F(u)$ are also called *sections of* F *over* u or more generally *local sections of* F. By slight abuse of notation, the section $\mathrm{res}^u_v(s)$ is often written "$s|_v$", even if s doesn't happen to be a function.

Example 6.9. Let X be a topological space. Let A be an arbitrary set. We endow A with the discrete topology. Then the functor $F : \mathrm{Ouv}(X)^{\mathrm{op}} \to \mathrm{Set}$ with

$$F(U) = \{\varphi : U \to A \mid \varphi \text{ is continuous}\}$$

and $\mathrm{res}^U_V(f) := f|_V$ (restriction of f to V) is a sheaf, the *constant sheaf* associated with A. The continuity condition amounts to the condition that φ is locally constant. This example can be generalized to locales instead of topological spaces and even to arbitrary sites.

Example 6.10. Let X be a topological space. Then the functor $C : \mathrm{Ouv}(X)^{\mathrm{op}} \to \mathrm{Set}$ with

$$C(U) = \{\varphi : U \to \mathbb{R} \mid \varphi \text{ is continuous}\}$$

and restriction maps as in Example 6.9 is a sheaf. (With $\mathbb{R}$, we mean the topological space of the Dedekind reals.) A section $s \in C(U)$ can be pictured as a "variable real number" or as a "parameter-dependent real number". We'll later see that the sheaf C can be obtained by constructing, internally to $\mathrm{Sh}(X)$, the set of (Dedekind) real numbers.

Example 6.11. The sheaf C of Example 6.10 is a subsheaf of the sheaf F of arbitrary real-valued functions with

$$F(U) = \{\varphi : U \to \mathbb{R}\}.$$

More generally, for any property $P(\varphi)$ of functions which is local in the sense that $P(\varphi)$ if and only if $P(\varphi|_{U_i})$ for all i, the sheaf with $U \mapsto \{\varphi : U \to \mathbb{R} \mid P(\varphi)\}$ is a subsheaf of F. In this way we obtain, for instance, the sheaf of locally bounded functions or (if the space X is a manifold) the sheaf of smooth functions. If the property P is not local, then the resulting presheaf will in general not be a sheaf.

Example 6.12. The presheaf of bounded functions on a topological space X, mapping an open subset U to the set of bounded real-valued functions $U \to \mathbb{R}$, is in general not a sheaf.

Example 6.13. Let X be a topological space. Then the functor $1 : \mathrm{Ouv}(X)^{\mathrm{op}} \to \mathrm{Set}$ with $1(U) = \{\heartsuit\}$ and the only possible restriction maps is a sheaf. It is the terminal object in $\mathrm{Sh}(X)$.

Example 6.14. Let X be a topological space. Then the functor $F : \mathrm{Ouv}(X)^{\mathrm{op}} \to \mathrm{Set}$ with $F(U) = \emptyset$ for all open subsets U is *not* in general a sheaf. But the related functor $0 : \mathrm{Ouv}(X)^{\mathrm{op}} \to \mathrm{Set}$ with

$$0(U) = \{\heartsuit \mid U = \emptyset\}$$

is. This sheaf is the initial object in $\mathrm{Sh}(X)$.

A sheaf can be pictured as a collection of "variable elements". Whereas an ordinary element is fixed once and for all, the value of a variable element depends on where we are on a space (topological space, locale, or site). This point of view is neatly illustrated by the CGP Grey sheaf of continents [?]. https://xorshammer.com/2016/07/24/the-cgp-grey-topos-of-continents/

6.2.2. *Syntactic sites.* Associated to any geometric theory $\mathbb{T}$, not necessarily a propositional one, there is the *syntactic site* $\mathcal{C}_{\mathbb{T}}$. Just as the Lindenbaum algebra of a propositional geometric theory is used to construct its classifying locale, the syntactic site of an arbitrary geometric theory will be used to construct its classifying topos. In the special case that $\mathbb{T}$ happens to be propositional, the classifiying topos of $\mathbb{T}$ will be canonically equivalent to the topos of sheaves over the classifying locale of $\mathbb{T}$.

The objects of $\mathcal{C}_{\mathbb{T}}$ are formal expressions of the form $\{\vec{x}.\ \varphi\}$, where $\vec{x}$ is an arbitrary context and φ is a formula in this context. We identify two such expressions if they only differ by the choice of variable names.

translate:

hat als Morphismen $\{\vec{x}.\ \varphi\} \to \{\vec{y}.\ \psi\}$ Äquivalenzklassen von *funktionalen Formeln* θ im Kontext $\vec{x}, \vec{y}$ (dabei seien ohne Einschränkung $\vec{x}$ und $\vec{y}$ disjunkt). Eine Formel θ in diesem Kontext heißt genau dann *funktional*, wenn $\mathbb{T}$ zeigt, dass

$$\theta \vdash_{\vec{x},\vec{y}} \varphi \wedge \psi, \qquad \varphi \vdash_{\vec{x}} \exists \vec{y}.\ \theta, \qquad \theta \wedge \theta[\vec{y}'/\vec{y}] \vdash_{\vec{x},\vec{y},\vec{y}'} \vec{y}' = \vec{y}.$$

Zwei solche Formeln θ, θ' sind genau dann äquivalent, wenn $\mathbb{T}$ zeigt, dass

$$\theta \wedge \theta'[\vec{y}'/\vec{y}] \vdash_{\vec{x},\vec{y},\vec{y}'} \vec{y} = \vec{y}'.$$

Die Komposition $\{\vec{x}.\ \varphi\} \xrightarrow{[\theta]} \{\vec{y}.\ \psi\} \xrightarrow{[\xi]} \{\vec{z}.\ \chi\}$ ist $[\exists \vec{y}.\ \theta \wedge \xi]$.

hat als Überdeckungen eines Objekts $\{\vec{y}.\ \psi\}$ genau diejenigen Morphismenmengen M, für die $\mathbb{T}$ zeigt:

$$\psi \vdash_{\vec{y}} \bigvee_{(\{\vec{x}.\ \varphi\} \xrightarrow{[\theta]} \{\vec{y}.\ \psi\}) \in M} \exists \vec{x}.\ \theta$$

6.2.3. *Open subsites.* Associated to an object U of a site $\mathcal{C}$, there is the *open subsite* $\mathcal{C}/U$. It is named that way because in the special case that $\mathcal{C}$ is the site induced by a locale X, the open subsite will be (canonically equivalent, even isomorphic to) the site induced by the corresponding sublocale.

As a category, the open subsite $\mathcal{C}/U$ is the slice category; its objects are morphisms $V \to U$ in $\mathcal{C}$, and its morphisms are given by

$$\mathrm{Hom}_{\mathcal{C}/U}((V \xrightarrow{p} U), (W \xrightarrow{q} U)) := \{f \in \mathrm{Hom}_{\mathcal{C}}(V, W) \mid f \setminus q = p\}.$$

A set M of morphisms in $\mathcal{C}/U$ with common target is deemed a covering if and only if the set of underlying morphisms in $\mathcal{C}$ is a covering of $\mathcal{C}$.

6.3. **The internal language of a topos.** defn Kripke–Joyal semantics
omnibus theorem
simplification rules

6.3.1. *First steps with the topos of sheaves over a space.*

6.3.2. *Exploring the little Zariski topos.*

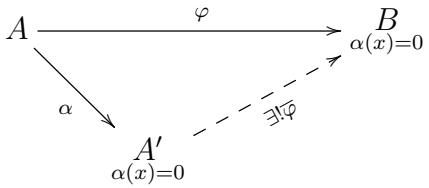
6.3.3. *The classifying topos of a geometric theory.* definition
theorem
mention examples

6.4. **Constructions in a topos.** power, hom, naturals, product, coproduct, quotient
object of truth values
integers, rationals
real numbers in a topos
example: intermediate value theorem

6.5. **The spectrum of a ring as a topos.** In this section, we give a ring-theoretic motivation for (affine) schemes which illustrates the versatility of toposes.

In commutative algebra, one often encounters the following problem: Let A be a ring (for us always commutative with a unit, where the case $1 = 0$ is not excluded). Let $x \in A$ be an element. Is there a universal way of "killing x"? That is, is there a ring A' together with a ring homomorphism $\alpha : A \to A'$ with $\alpha(x) = 0$, such that for any ring B and any ring homomorphism $\varphi : A \to B$ with $\varphi(x) = 0$ there is a unique ring homomorphism $\overline{\varphi} : A' \to B$ such that $\alpha \setminus \overline{\varphi} = \varphi$?

This problem is always solvable, and the solution is well-known: It's the quotient ring $A/(x)$ together with the canonical projection.



The situation is different with the following similar problem. We call that a ring is local if and only if any invertible finite sum contains an invertible summand, or more explicitly if and only if

$$1 \neq 0 \quad \text{and} \quad \forall x, y.\ x + y \text{ inv.} \Rightarrow (x \text{ inv. or } y \text{ inv.}).$$

A homomorphism of rings is local if and only if it reflects invertibility ($\varphi(x)$ inv. $\Rightarrow$ x inv.). Assuming classical logic and the axiom of choice, one can prove that a ring is local if and only if it possesses exactly one maximal ideal; this is the classical definition of a local ring. A localization $A[S^{-1}]$ is local if and only if the saturation of S (the set of those elements of A which

become invertible in $A[S^{-1}]$) is a filter. The preimage of a filter under a ring homomorphism is a filter.

Let A be a ring. Is there a *universal localization* of A? That is, a local ring A' together with a ring homomorphism $\alpha : A \to A'$ such that for any local ring B and any ring homomorphism $\varphi : A \to B$ there is a unique ring homomorphism $\overline{\varphi} : A' \to B$ which is local?

In order to work towards a solution, let's see how we could construct such a ring A' if we only required the factorization condition for a particular homomorphism $\varphi : A \to B$ into a particular local ring B. In this case it seems natural to factor φ over $A' := A[F^{-1}]$, where $F := \{x \in A \,|\, \varphi(x) \in B^\times\}$ is the preimage of the filter of units in B. It's easy to verify that we indeed obtain an induced local homomorphism $A[F^{-1}] \to B$ and that the composition $A \to A[F^{-1}] \to B$ equals φ.

The obvious problem with this construction is that any homomorphism requires a custom-tailored filter. If there only was a *generic filter*, capable of specializing into any concrete one! If we allow the solution A' to exist in a different topos, then the problem is always solvable; if we want to remain in the topos of sets, we have the following result.

Proposition 6.15. *Let A be a ring.*

(1) *There exists a universal localization of A in the sense described above if and only if A possesses exactly one filter.*
(2) *Sufficient for A to possess exactly one filter is that A is local and that any non-nilpotent element is invertible. Assuming classical logic and the axiom of choice, the converse holds as well.*

Proof. If A possesses exactly one filter F, one can check that the canonical morphism $A \to A[F^{-1}]$ is the universal localization. Conversely, if there exists a universal localization $\alpha : A \to A'$, then A has at least one filter, namely $F := \alpha^{-1}[(A')^\times]$, and given any filters G and H, we can show $G \subseteq H$ (and analogously $H \subset G$) as follows: Let $x \in G$. Then x is invertible in $A[G^{-1}]$. By locality of the induced map $A' \to A[G^{-1}]$, it is invertible in A'. Since ring homomorphisms preserve units, it is invertible in $A[H^{-1}]$ and is therefore an element of H.

For the second statement, let A be local and assume that any non-nilpotent element is invertible. Then $A^\times$ is a filter. Any filter contains $A^\times$ and the reverse inclusion follows from the assumption.

Let x be an element which is not invertible. Then the ring $A[x^{-1}]$ is not the zero ring. Zorn's lemma can be used to show that $A[x^{-1}]$ has a filter ("every nonzero ring possesses a maximal ideal"). The preimage of that filter in A is a filter which contains x. continue □

category of *all* rings
solution

6.6. **Internal topos theory.** internal locale
internal category
internal functor-to-Set
internal sheaf
externalization

idempotency

6.7. **Subtoposes and local operators.** definition of local operators
notation for ∇
induced finer coverage

6.8. **Embracing topology.**

6.9. **Deligne's completeness theorem.**