Proof Theory, Logic and Algebra

Amir Akbar Tabatabai
Bernoulli institute, University of Groningen

TACL 2022, Praia de Mira

The Last Part of the Previous Lecture

- We saw the definition of two arithmetical theories namely Heyting and Peano arithmetic.

The Last Part of the Previous Lecture

- We saw the definition of two arithmetical theories namely Heyting and Peano arithmetic.
- We were curios about the consistency of the arithmetical theories.

The Last Part of the Previous Lecture

- We saw the definition of two arithmetical theories namely Heyting and Peano arithmetic.
- We were curios about the consistency of the arithmetical theories.
- We argued that there are non-intuitive consistency problems as they are inconsistent with our world.

The Last Part of the Previous Lecture

- We saw the definition of two arithmetical theories namely Heyting and Peano arithmetic.
- We were curios about the consistency of the arithmetical theories.
- We argued that there are non-intuitive consistency problems as they are inconsistent with our world.
- As an example, we met the arithmetical theory $\mathsf{HA} + CT$, where CT is the Church thesis:

$$\mathsf{HA} + \forall x \exists y A(x, y) \rightarrow \exists e \forall x A(x, e \cdot x)$$

stating that if you have a total relation, then you can come up with a computable function witnessing that.

The Last Part of the Previous Lecture

- We saw the definition of two arithmetical theories namely Heyting and Peano arithmetic.
- We were curios about the consistency of the arithmetical theories.
- We argued that there are non-intuitive consistency problems as they are inconsistent with our world.
- As an example, we met the arithmetical theory $\mathsf{HA} + CT$, where CT is the Church thesis:

$$\mathsf{HA} + \forall x \exists y A(x, y) \rightarrow \exists e \forall x A(x, e \cdot x)$$

stating that if you have a total relation, then you can come up with a computable function witnessing that. The theory is describing the alternative constructive world, where every construction is computable. This is a fragment of what is called the Russian arithmetic.

The Last Part of the Previous Lecture

- Is this theory consistent?

The Last Part of the Previous Lecture

- Is this theory consistent? It is not clear as in the usual classical world we are in, some functions like the characteristic function for the halting predicate are uncomputable.

The Last Part of the Previous Lecture

- Is this theory consistent? It is not clear as in the usual classical world we are in, some functions like the characteristic function for the halting predicate are uncomputable.
- How to prove the consistency of HA + CT? Isn't the recursive world of constructions, **Rec**, useful?

Elementary Analysis

It is possible to define an elementary theory of intuitionistic analysis, EL, where we can argue about the infinite sequences of numbers:

Elementary Analysis

It is possible to define an elementary theory of intuitionistic analysis, EL, where we can argue about the infinite sequences of numbers:

- Add another sort of variables for infinite sequences of numbers, denoted by $\alpha, \beta, \cdots$ and add the term $\alpha(x)$.

Elementary Analysis

It is possible to define an elementary theory of intuitionistic analysis, EL, where we can argue about the infinite sequences of numbers:

- Add another sort of variables for infinite sequences of numbers, denoted by $\alpha, \beta, \cdots$ and add the term $\alpha(x)$.
- Add some basic machinery of defining sequences by explicit definition and recursion,
- Add the following axiom of choice for quantifier-free formulas $A(x, y)$

$$\forall x \exists y A(x, y) \to \exists \alpha \forall x A(x, \alpha(x))$$

to Heyting arithmetic in this new language.

The Brouwerian Analysis

Consider the theory of analysis EL + CP, where CP, the continuity principle is:

$$\forall\alpha\exists y A(\alpha, y) \to \forall\alpha\exists yz\forall\beta\,[(\forall w \leq z\ \alpha(w) = \beta(w)) \to A(\beta, y)]$$

This axioms is inconsistent from the classical point of view as it simply says that all total functions from the sequences to numbers are continuous in the sense that the value on α only depends on finitely many values of $\alpha(n)$'s. However, using the excluded middle, we have

$$\forall\alpha\exists y[((\forall w\alpha(w) = 0) \to y = 0) \wedge ((\neg\forall w\alpha(w) = 0) \to y = 1)]$$

This is of course depending on all the inputs of α and not just any finite number of them. However, the intuitionistic version is describing the world where every construction is continuous.

Information Extraction

We can ask some interesting questions even on the level of the usual theories.

Information Extraction

We can ask some interesting questions even on the level of the usual theories.

Kreisel's Idea

Is knowing the proof of a proposition brings more information than knowing only the mere truth?

Information Extraction

We can ask some interesting questions even on the level of the usual theories.

Kreisel's Idea

Is knowing the proof of a proposition brings more information than knowing only the mere truth?

For instance, if we know the truth of $\forall x \exists y A(x, y)$, then we know that for any n, there is an m such that $A(n, m)$. But when we have a proof of $\forall x \exists y A(x, y)$, does it include more information? Like an algorithm to compute an m reading the n? If yes, does it imply something about the complexity of the algorithm?

Information Extraction

Semantics is the shadow. It forgets the whole structure of a proof to make everything easier and the cost is losing every information except the mere truth. But, isn't it too crude to have it all or loose it all? Maybe we have to come up with some models of proofs as we did yesterday to forget some structures to makes everything easier but keep some to make it interesting and informative enough. The motto is:

Information Extraction

Semantics is the shadow. It forgets the whole structure of a proof to make everything easier and the cost is losing every information except the mere truth. But, isn't it too crude to have it all or loose it all? Maybe we have to come up with some models of proofs as we did yesterday to forget some structures to makes everything easier but keep some to make it interesting and informative enough. The motto is:

> Don't go from the free category to a preorder. There are many interesting middle points to stop in.

Some Basic Facts about Arithmetic

- Define $x \leq y$ as an abbreviation for $\exists z(x + z = y)$.

Some Basic Facts about Arithmetic

- Define $x \leq y$ as an abbreviation for $\exists z(x + z = y)$.
- Any quantifier in the form $\forall x(x \leq t \rightarrow A(x))$ and $\exists x(x \leq t \wedge A(x))$ is called a bounded quantifier and will be denoted by $\forall x \leq t\, A(x)$ and $\exists x \leq t\, A(x)$, respectively.

Some Basic Facts about Arithmetic

- Define $x \leq y$ as an abbreviation for $\exists z(x + z = y)$.
- Any quantifier in the form $\forall x(x \leq t \rightarrow A(x))$ and $\exists x(x \leq t \wedge A(x))$ is called a bounded quantifier and will be denoted by $\forall x \leq t\, A(x)$ and $\exists x \leq t\, A(x)$, respectively.
- A formula is called bounded if any quantifier in it can be replaced by a bounded quantifier up to the provability in HA.

Some Basic Facts about Arithmetic

- Define $x \leq y$ as an abbreviation for $\exists z(x + z = y)$.
- Any quantifier in the form $\forall x(x \leq t \to A(x))$ and $\exists x(x \leq t \wedge A(x))$ is called a bounded quantifier and will be denoted by $\forall x \leq t\, A(x)$ and $\exists x \leq t\, A(x)$, respectively.
- A formula is called bounded if any quantifier in it can be replaced by a bounded quantifier up to the provability in HA.
- For any bounded formula $A(\vec{x})$, we have $\mathrm{HA} \vdash \forall \vec{x}(A(\vec{x}) \vee \neg A(\vec{x}))$.

Some Basic Facts about Arithmetic

- Define $x \leq y$ as an abbreviation for $\exists z(x + z = y)$.
- Any quantifier in the form $\forall x(x \leq t \rightarrow A(x))$ and $\exists x(x \leq t \wedge A(x))$ is called a bounded quantifier and will be denoted by $\forall x \leq t\, A(x)$ and $\exists x \leq t\, A(x)$, respectively.
- A formula is called bounded if any quantifier in it can be replaced by a bounded quantifier up to the provability in HA.
- For any bounded formula $A(\vec{x})$, we have $\mathrm{HA} \vdash \forall \vec{x}(A(\vec{x}) \vee \neg A(\vec{x}))$.
- The theory PA is conservative over HA for formulas in the form $\forall x \exists y A(x, y)$, where $A(x, y)$ is bounded.

A Propositional Approach to the First-order World

So far, we have explained the propositional setting from the categorical point of view. It is of course possible to move to the first-order setting. However, this setting is not as easy as its propositional counterpart. Therefore, we prefer to modify the propositional case to understand some aspects of the first-order proofs. Our main idea is first to pretend that any first-order formula is a propositional formula for which we have a good categorical candidate. Then, we use the BHK interpretation to select out the propositional proofs that are really first-order. Apart from its relative simplicity, this approach has its own benefits.

- First, it is the categorical representation of one of the very powerful techniques in proof theory called realizability.

A Propositional Approach to the First-order World

So far, we have explained the propositional setting from the categorical point of view. It is of course possible to move to the first-order setting. However, this setting is not as easy as its propositional counterpart. Therefore, we prefer to modify the propositional case to understand some aspects of the first-order proofs. Our main idea is first to pretend that any first-order formula is a propositional formula for which we have a good categorical candidate. Then, we use the BHK interpretation to select out the propositional proofs that are really first-order. Apart from its relative simplicity, this approach has its own benefits.

- First, it is the categorical representation of one of the very powerful techniques in proof theory called realizability.
- On the other hand, using the propositional setting uses less structure which means that we can learn more about the theories.

The BHK Interpretation Revisited

- There is a canonical proof for $\top$.
- There is no proof for $\bot$.
- A proof of $A \wedge B$ is a pair of a proof of A and a proof of B.
- A proof of $A \vee B$ is either a proof of A or a proof of B.
- A proof of $A \to B$ is a construction that transforms any proof of A to a proof of B.

The BHK Interpretation Revisited

- There is a canonical proof for $\top$.
- There is no proof for $\bot$.
- A proof of $A \wedge B$ is a pair of a proof of A and a proof of B.
- A proof of $A \vee B$ is either a proof of A or a proof of B.
- A proof of $A \to B$ is a construction that transforms any proof of A to a proof of B.
- A proof of $\forall x A(x)$ is a construction that transforms any element a to a proof of $A(a)$.
- A proof of $\exists x A(x)$ is a pair of an element a and a proof for $A(a)$.

Definition

Let $\mathcal{C}$ be a cartesian closed category with a natural number object N. We assign an object to any formula in the language of arithmetic in the following way:

- $[t = s] = [\bot] = [\top] = 1$,
- $[A \wedge B] = [A] \times [B]$,
- $[A \to B] = [B]^{[A]}$
- $[\forall x A(x)] = [A(x)]^N$
- $[\exists x A(x)] = N \times [A(x)]$

Definition

Let $\mathcal{C}$ be a cartesian closed category with a natural number object N. We assign an object to any formula in the language of arithmetic in the following way:

- $[t = s] = [\bot] = [\top] = 1$,
- $[A \wedge B] = [A] \times [B]$,
- $[A \to B] = [B]^{[A]}$
- $[\forall x A(x)] = [A(x)]^N$
- $[\exists x A(x)] = N \times [A(x)]$

Note that $[A(t)] = [A(s)]$ which captures the idea that our object-assignment is essentially propositional and do not care about the first-order setting. To emphasize this fact, we denote $[A(t_1, \cdots, t_n)]$ by the fix name $[A]$, for any terms $t_1, \cdots, t_n$.

How to Interpret the Realizability

$Hom(1, [A])$ can be read as the set that stores all the potential proofs of A. Now, we employ the BHK interpretation to identify the actual proofs of A. More precisely, we select out some maps in $Hom(1, [A])$ that can act as the actual proofs of A.

Realizability

Definition

For any *sentence* A in the language of arithmetic and any map $f : 1 \to [A]$, we define $f \Vdash A$ inductively in the following way:

Realizability

Definition

For any *sentence* A in the language of arithmetic and any map $f : 1 \to [A]$, we define $f \Vdash A$ inductively in the following way:

- $f \Vdash t = s$ iff $t = s$ holds, for any closed terms t and s,

Realizability

Definition

For any *sentence* A in the language of arithmetic and any map $f : 1 \to [A]$, we define $f \Vdash A$ inductively in the following way:

- $f \Vdash t = s$ iff $t = s$ holds, for any closed terms t and s,
- there is no $f : 1 \to 1$ such that $f \Vdash \bot$,

Realizability

Definition

For any *sentence* A in the language of arithmetic and any map $f : 1 \to [A]$, we define $f \Vdash A$ inductively in the following way:

- $f \Vdash t = s$ iff $t = s$ holds, for any closed terms t and s,
- there is no $f : 1 \to 1$ such that $f \Vdash \bot$,
- $f \Vdash \top$, for any $f : 1 \to 1$,

Realizability

Definition

For any *sentence* A in the language of arithmetic and any map $f : 1 \to [A]$, we define $f \Vdash A$ inductively in the following way:

- $f \Vdash t = s$ iff $t = s$ holds, for any closed terms t and s,
- there is no $f : 1 \to 1$ such that $f \Vdash \bot$,
- $f \Vdash \top$, for any $f : 1 \to 1$,
- $f \Vdash A \wedge B$ iff $p_0 \circ f \Vdash A$ and $p_1 \circ f \Vdash B$,

Realizability

Definition

For any *sentence* A in the language of arithmetic and any map $f : 1 \to [A]$, we define $f \Vdash A$ inductively in the following way:

- $f \Vdash t = s$ iff $t = s$ holds, for any closed terms t and s,
- there is no $f : 1 \to 1$ such that $f \Vdash \bot$,
- $f \Vdash \top$, for any $f : 1 \to 1$,
- $f \Vdash A \wedge B$ iff $p_0 \circ f \Vdash A$ and $p_1 \circ f \Vdash B$,
- $f \Vdash A \to B$ iff for any $g : 1 \to [A]$, if $g \Vdash A$ then $f \cdot g \Vdash B$,

Realizability

Definition

For any *sentence* A in the language of arithmetic and any map $f : 1 \to [A]$, we define $f \Vdash A$ inductively in the following way:

- $f \Vdash t = s$ iff $t = s$ holds, for any closed terms t and s,
- there is no $f : 1 \to 1$ such that $f \Vdash \bot$,
- $f \Vdash \top$, for any $f : 1 \to 1$,
- $f \Vdash A \wedge B$ iff $p_0 \circ f \Vdash A$ and $p_1 \circ f \Vdash B$,
- $f \Vdash A \to B$ iff for any $g : 1 \to [A]$, if $g \Vdash A$ then $f \cdot g \Vdash B$,
- $f \Vdash \forall x A(x)$ iff for any $n \in \mathbb{N}$, $f \cdot \bar{n} \Vdash A(n)$,

Realizability

Definition

For any *sentence* A in the language of arithmetic and any map $f : 1 \to [A]$, we define $f \Vdash A$ inductively in the following way:

- $f \Vdash t = s$ iff $t = s$ holds, for any closed terms t and s,
- there is no $f : 1 \to 1$ such that $f \Vdash \bot$,
- $f \Vdash \top$, for any $f : 1 \to 1$,
- $f \Vdash A \wedge B$ iff $p_0 \circ f \Vdash A$ and $p_1 \circ f \Vdash B$,
- $f \Vdash A \to B$ iff for any $g : 1 \to [A]$, if $g \Vdash A$ then $f \cdot g \Vdash B$,
- $f \Vdash \forall x A(x)$ iff for any $n \in \mathbb{N}$, $f \cdot \bar{n} \Vdash A(n)$,
- $f \Vdash \exists x A(x)$ iff there is a natural number n such that $p_0 \circ f = \bar{n}$ and $p_1 \circ f \Vdash A(n)$.

Some Examples

Example

The map $\lambda p_0 : 1 \to [A]^{[A]\times[B]}$ realizes $A \wedge B \to A$. To show why, we have to show that for any $g : 1 \to [A \wedge B]$, if $g \Vdash A \wedge B$, then $(\lambda p_0) \cdot g \Vdash A$. Note that $(\lambda p_0) \cdot g = p_0 \circ g$. Finally, note that by definition, $g \Vdash A \wedge B$ implies $p_0 \circ g \Vdash A$.

Some Examples

Example

The map $\lambda p_0 : 1 \to [A]^{[A]\times[B]}$ realizes $A \wedge B \to A$. To show why, we have to show that for any $g : 1 \to [A \wedge B]$, if $g \Vdash A \wedge B$, then $(\lambda p_0) \cdot g \Vdash A$. Note that $(\lambda p_0) \cdot g = p_0 \circ g$. Finally, note that by definition, $g \Vdash A \wedge B$ implies $p_0 \circ g \Vdash A$.

Example

$A(t) \to \exists x A(x)$, where t is a closed term with the interpretation n is realized by the map $\lambda f : 1 \to (N \times [A])^{[A]}$, where $f = (\bar{n} \times id_{[A]}) \circ (\langle !, id_{[A]} \rangle)$. The reason is that for any $g : 1 \to [A]$, if $g \Vdash A(t)$, then $(\lambda f) \cdot g = f \circ g = \langle \bar{n}, g \rangle$ and we have $\langle \bar{n}, g \rangle \Vdash \exists x A(x)$.

The Soundness Theorem

Soundness Theorem

If HA $\vdash A$, then there exists $f : 1 \to [A]$ such that $f \Vdash A$.

The Soundness Theorem

Soundness Theorem

If HA $\vdash A$, then there exists $f : 1 \to [A]$ such that $f \Vdash A$.

Proof.

We have to provide a morphism for any axiom of HA. The logical part is easy. The basic axioms are realized by $\lambda!$ as the realizability is reduced to the validity in natural numbers. For instance, $\lambda! \Vdash \forall x(s(x) \neq 0)$, because $(\lambda!) \cdot \bar{n} =! \Vdash s(n) \neq 0$ as $s(n) \neq 0$. For induction, use primitive recursion (initiality of the natural number object) and the external induction in natural numbers. □

The Soundness Theorem

Soundness Theorem

If HA $\vdash A$, then there exists $f : 1 \to [A]$ such that $f \Vdash A$.

Proof.

We have to provide a morphism for any axiom of HA. The logical part is easy. The basic axioms are realized by $\lambda!$ as the realizability is reduced to the validity in natural numbers. For instance, $\lambda! \Vdash \forall x(s(x) \neq 0)$, because $(\lambda!) \cdot \bar{n} =! \Vdash s(n) \neq 0$ as $s(n) \neq 0$. For induction, use primitive recursion (initiality of the natural number object) and the external induction in natural numbers. □

Note that this f is constructed by the proof of A in HA. This is the shadow of the proof in the category $\mathcal{C}$.

The Consistency of HA + CT

Corollary

HA + CT *is consistent.*

The Consistency of HA + *CT*

Corollary

HA + *CT* *is consistent.*

Proof.

It is enough to show that Church thesis is realizable in **Rec**.

$$\forall x \exists y A(x, y) \to \exists e \forall x A(x, e \cdot x)$$

The algorithm to realize it is the algorithm that maps the realizer p to $\langle \lambda n.p_0(p \cdot n), \lambda n.p_1(p \cdot n) \rangle$ is realized by e. □

Realizability vs Truth

Lemma

Let A be an $\exists$-free sentence. Then:

- *For any $f : 1 \to [A]$, if $f \Vdash A$, then A holds.*
- *There is $f : 1 \to [A]$ such that if A holds, then $f \Vdash A$.*

Realizability vs Truth

Lemma

Let A be an $\exists$-free sentence. Then:

- *For any $f : 1 \to [A]$, if $f \Vdash A$, then A holds.*
- *There is $f : 1 \to [A]$ such that if A holds, then $f \Vdash A$.*

Proof.

Use induction on the structure of A. For atoms, use $f =!$. The conjunction and the universal quantifier cases are easy. For implication, if $f \Vdash A \to B$ and A is valid, then by induction hypothesis, there is $g : 1 \to [A]$ such that $g \Vdash A$. By definition, $f \cdot g \Vdash B$. Again by the induction hypothesis, B holds. For the other part, just use induction hypothesis to come up with $h : 1 \to [B]$ such that if B holds, then $g \Vdash A$. Set $f = \lambda h \circ ! : 1 \to [B]^{[A]}$. If $A \to B$ holds, then $f \Vdash A \to B$, because if $g \Vdash A$, then by induction hypothesis A holds and hence B holds which implies $h \Vdash B$. On the other hand, as $f \cdot g = (h \circ !) \circ g = h$ and $h \Vdash B$, we have $f \cdot g \Vdash B$. □

Function Extraction

Corollary

If $\mathsf{HA} \vdash \forall x \exists y A(x, y)$*, for an* $\exists$*-free formula* $A(x, y)$*, then for any cartesian closed category with a natural number object* $\mathcal{C}$*, there exists a representable function* $f : \mathbb{N} \to \mathbb{N}$ *in* $\mathcal{C}$ *such that for any* $n \in \mathbb{N}$*, the formula* $A(n, f(n))$ *holds.*

Proof.

By soundness theorem, there is a map $g : 1 \to [\forall x \exists y A(x, y)]$ such that $g \Vdash \forall x \exists y A(x, y)$. This means that $g : 1 \to (N \times [A])^N$ and for any natural number $n \in \mathbb{N}$, we have $g \cdot \bar{n} \Vdash \exists y A(n, y)$ which means the existence of $m \in \mathbb{N}$ such that $p_0(g \cdot \bar{n}) = \bar{m}$ and $p_1(g \cdot \bar{n}) \Vdash A(n, m)$ which implies $A(m, n)$, as $A(m, n)$ is $\exists$-free. Define $f(n) = m$ if $p_0(g \cdot \bar{n}) = \bar{m}$. This function is of course representable by the map $p_0 \circ (g \cdot id_N)$. □

Corollary

If $\mathsf{HA} \vdash \forall x \exists y A(x, y)$, *for an* $\exists$*-free formula* $A(x, y)$, *then there exists a recursive function* $f : \mathbb{N} \to \mathbb{N}$ *such that for any* $n \in \mathbb{N}$, *the formula* $A(n, f(n))$ *holds.*

Corollary

If $\mathsf{HA} \vdash \forall x \exists y A(x, y)$*, for an* $\exists$*-free formula* $A(x, y)$*, then there exists a recursive function* $f : \mathbb{N} \to \mathbb{N}$ *such that for any* $n \in \mathbb{N}$*, the formula* $A(n, f(n))$ *holds.*

Corollary

There is a formula $A(x)$ *such that* $\mathsf{HA} \nvdash \forall x(A(x) \vee \neg A(x))$.

Corollary

If $\mathsf{HA} \vdash \forall x \exists y A(x, y)$*, for an* $\exists$*-free formula* $A(x, y)$*, then there exists a recursive function* $f : \mathbb{N} \to \mathbb{N}$ *such that for any* $n \in \mathbb{N}$*, the formula* $A(n, f(n))$ *holds.*

Corollary

There is a formula $A(x)$ *such that* $\mathsf{HA} \nvdash \forall x(A(x) \vee \neg A(x))$.

Proof.

Set $A(x) = \mathit{Halt}(x)$ and note that $\forall x(A(x) \vee \neg A(x))$ by definition is

$$\forall x \exists y[(\mathit{Halt}(x) \to y = 0) \wedge (\neg \mathit{Halt}(x) \to y = 1)]$$

It is not hard to see that $[(\mathit{Halt}(x) \to y = 0) \wedge (\neg \mathit{Halt}(x) \to y = 1)]$ is equivalent to an $\exists$-free formula, provably in HA. Hence, by the previous theorem, there must be a computable function of x to witness that y and this is impossible as halting is undecidable. $\square$

Providing a Characterization

To prove the best thing we can, it is reasonable to use the free cartesian closed category with the natural number object $\mathbf{T}$:

Providing a Characterization

To prove the best thing we can, it is reasonable to use the free cartesian closed category with the natural number object $\mathbf{T}$:

Corollary

If HA $\vdash \forall x \exists y A(x, y)$, *for an* $\exists$*-free formula, then there exists a primitive recursive functional* $f : \mathbb{N} \to \mathbb{N}$ *such that for any* $n \in \mathbb{N}$, *the formula* $A(n, f(n))$ *holds. The same also holds for both* HA *and* PA, *if* $A(x, y)$ *is bounded.*

Providing a Characterization

To prove the best thing we can, it is reasonable to use the free cartesian closed category with the natural number object $\mathbf{T}$:

Corollary

If HA $\vdash \forall x \exists y A(x, y)$, *for an* $\exists$*-free formula, then there exists a primitive recursive functional* $f : \mathbb{N} \to \mathbb{N}$ *such that for any* $n \in \mathbb{N}$, *the formula* $A(n, f(n))$ *holds. The same also holds for both* HA *and* PA, *if* $A(x, y)$ *is bounded.*

The converse also holds, but it needs an elaborate normalization proof inside HA.

Thank you for your attention!