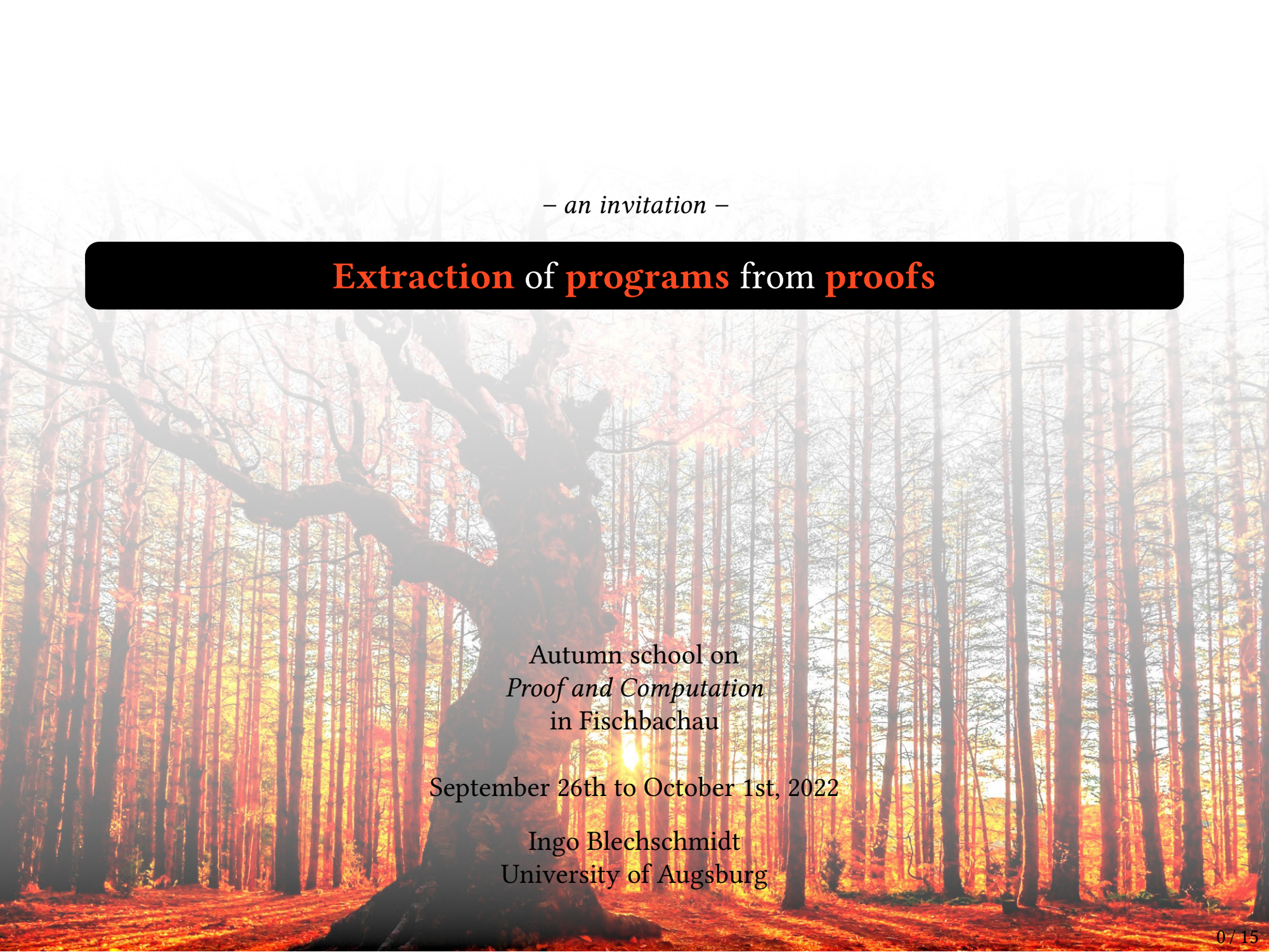
– an invitation –

Extraction of programs from proofs



Autumn school on
Proof and Computation
in Fischbachau

September 26th to October 1st, 2022

Ingo Blechschmidt
University of Augsburg

Thm. For every number $n \in \mathbb{N}$, there is a prime larger than n.

Proof. Any prime factor of $n! + 1$ will do.

Thm. For every number $n \in \mathbb{N}$, there is a prime larger than n.

Proof. Any prime factor of $n! + 1$ will do.

"Every constructive theorem has a computable witness."

Thm. For every number $n \in \mathbb{N}$, there is a prime larger than n.

Proof. Any prime factor of $n! + 1$ will do.

"Every constructive theorem has a computable witness."

$$\begin{array}{ccc} \mathrm{HA} \vdash \varphi & \Longrightarrow & \exists e.\ e \Vdash \varphi \\ \text{constructive proof} & \longmapsto & \text{realizer} \end{array}$$

Thm. For every number $n \in \mathbb{N}$, there is a prime larger than n.

Proof. Any prime factor of $n! + 1$ will do.

"Every constructive theorem has a computable witness."

$$\begin{array}{ccc} \mathrm{HA} \vdash \varphi & \Longrightarrow & \exists e.\ e \Vdash \varphi \\ \text{constructive proof} & \longmapsto & \text{realizer} \end{array}$$

- Integrated developments
  SAT checking, …
- Computability theory
  induction $\widehat{=}$ *recursion, …*
- Metatheory of constructive systems
  provability results, …
- Philosophy of proof and computation
  realizability in the real world, …

Thm. For every number $n \in \mathbb{N}$, there is a prime larger than n.

Proof. Any prime factor of $n! + 1$ will do.

"Every constructive theorem has a computable witness."

$$\begin{array}{ccc} \mathrm{HA} \vdash \varphi & \Longrightarrow & \exists e.\ e \Vdash \varphi \\ \text{constructive proof} & \longmapsto & \text{realizer} \end{array}$$

- Integrated developments
  SAT checking, …
- Computability theory
  induction $\widehat{=}$ recursion, …
- Metatheory of constructive systems
  provability results, …
- Philosophy of proof and computation
  realizability in the real world, …

Thm. Every infinite sequence $\alpha : \mathbb{N} \to \mathbb{N}$ is *good* in that there are numbers $i < j$ such that $\alpha(i) \leq \alpha(j)$.

Proof. By LEM, there is a minimal value $\alpha(i)$. Set $j := i + 1$.

"Every *theorem has a computable* witness.*"

* with monadic side effects

Thm. For every number $n \in \mathbb{N}$, there is a prime larger than n.

Proof. Any prime factor of $n! + 1$ will do.

"Every constructive theorem has a computable witness."

$$\begin{array}{ccc} \mathrm{HA} \vdash \varphi & \Longrightarrow & \exists e.\ e \Vdash \varphi \\ \text{constructive proof} & \longmapsto & \text{realizer} \end{array}$$

- Integrated developments
  SAT checking, …
- Computability theory
  induction $\widehat{=}$ recursion, …
- Metatheory of constructive systems
  provability results, …
- Philosophy of proof and computation
  realizability in the real world, …

Thm. Every infinite sequence $\alpha : \mathbb{N} \to \mathbb{N}$ is *good* in that there are numbers $i < j$ such that $\alpha(i) \leq \alpha(j)$.

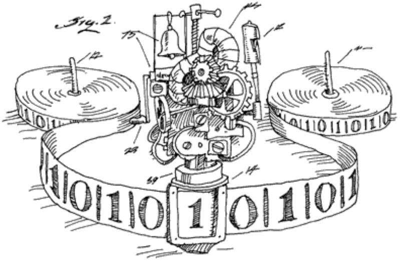
Proof. By LEM, there is a minimal value $\alpha(i)$. Set $j := i + 1$.

"Every *theorem has a computable* witness.*"

* with monadic side effects

Ada Lovelace,
the world's first
computer programmer

* 1815 † 1852



Lecture I:

Realizability theory

for extracting programs from constructive proofs

Heyting arithmetic

The **language of arithmetic** has

- as its single sort: N
- as function symbols: 0, S, $+$, $\cdot$
- as its single relation symbol: $=$

Heyting arithmetic has as axioms (the universal closure of)

$$\neg(0 = Sx)$$

$$S(x) = S(y) \Rightarrow x = y$$

$$x + 0 = x \qquad\qquad x \cdot 0 = 0$$

$$x + S(y) = S(x + y) \qquad\qquad x \cdot S(y) = (x \cdot y) + x$$

together with the **induction scheme** (one axiom for each formula φ)

$$\varphi(0) \wedge \big(\forall x : N.\ \varphi(x) \Rightarrow \varphi(S(x))\big) \quad \Longrightarrow \quad \forall x : N.\ \varphi(x)$$

and the rules of **sequence calculus**.

Sequence calculus

$$\frac{}{\varphi \vdash_{\vec{x}} \varphi} \qquad \frac{\varphi \vdash_{\vec{x}} \psi}{\varphi[\vec{s}/\vec{x}] \vdash_{\vec{y}} \psi[\vec{s}/\vec{x}]} \qquad \frac{\varphi \vdash_{\vec{x}} \psi \qquad \psi \vdash_{\vec{x}} \chi}{\varphi \vdash_{\vec{x}} \chi}$$

$$\frac{}{\varphi \vdash_{\vec{x}} \top} \qquad \frac{}{\varphi \wedge \psi \vdash_{\vec{x}} \varphi} \qquad \frac{}{\varphi \wedge \psi \vdash_{\vec{x}} \psi} \qquad \frac{\varphi \vdash_{\vec{x}} \psi \qquad \varphi \vdash_{\vec{x}} \chi}{\varphi \vdash_{\vec{x}} \psi \wedge \chi}$$

$$\frac{}{\bot \vdash_{\vec{x}} \varphi} \qquad \frac{}{\varphi \vdash_{\vec{x}} \varphi \vee \psi} \qquad \frac{}{\psi \vdash_{\vec{x}} \varphi \vee \psi} \qquad \frac{\varphi \vdash_{\vec{x}} \chi \qquad \psi \vdash_{\vec{x}} \chi}{\varphi \vee \psi \vdash_{\vec{x}} \chi}$$

$$\frac{\varphi \wedge \psi \vdash_{\vec{x}} \chi}{\varphi \vdash_{\vec{x}} \psi \Rightarrow \chi}$$

$$\frac{\varphi \vdash_{\vec{x},y} \psi}{\exists y : Y . \varphi \vdash_{\vec{x}} \psi} \ (y \text{ not occurring in } \psi) \qquad \frac{\varphi \vdash_{\vec{x},y} \psi}{\varphi \vdash_{\vec{x}} \forall y : Y . \psi} \ (y \text{ not occurring in } \varphi)$$

$$\frac{}{\top \vdash_x x = x} \qquad \frac{}{(\vec{x} = \vec{y}) \wedge \varphi \vdash_{\vec{z}} \varphi[\vec{y}/\vec{x}]}$$

Number realizability

$e \Vdash s = t$ iff $s = t$.

$e \Vdash \top$ iff true.

$e \Vdash \bot$ iff false.

$e \Vdash (\varphi \wedge \psi)$ iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and $\pi_1 \cdot e \Vdash \varphi$ and $\pi_2 \cdot e \Vdash \psi$.

$e \Vdash (\varphi \vee \psi)$ iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and
if $\pi_1 \cdot e = 0$ then $\pi_2 \cdot e \Vdash \varphi$, and
if $\pi_1 \cdot e \neq 0$ then $\pi_2 \cdot e \Vdash \psi$.

$e \Vdash (\varphi \Rightarrow \psi)$ iff for every $r \in \mathbb{N}$ such that $r \Vdash \varphi$, $e \cdot r \downarrow$ and $e \cdot r \Vdash \psi$.

$e \Vdash (\forall n : N.\ \varphi(n))$ iff for every $n_0 \in \mathbb{N}$, $e \cdot n_0 \downarrow$ and $e \cdot n_0 \Vdash \varphi(n_0)$.

$e \Vdash (\exists n : N.\ \varphi(n))$ iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and $\pi_2 \cdot e \Vdash \varphi(\pi_1 \cdot e)$.

$e \Vdash (\forall f : N^N.\ \varphi(f))$ iff for every $f_0 : \mathbb{N} \to \mathbb{N}$ and every $r_0 \in \mathbb{N}$ such that
f_0 is computed by the r_0-th machine,
$e \cdot r_0 \downarrow$ and $e \cdot r_0 \Vdash \varphi(f_0)$.

$e \Vdash (\exists f : N^N.\ \varphi(f))$ iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and the $(\pi_1 \cdot e)$-th machine
computes a function $f_0 : \mathbb{N} \to \mathbb{N}$ and $\pi_2 \cdot e \Vdash \varphi(f_0)$.

Thm. If $\mathrm{HA} \vdash \varphi$, then there is a number $e \in \mathbb{N}$ such that $e \Vdash \varphi$.

Number realizability

$e \Vdash s = t$ iff $s = t$.

$e \Vdash \top$ iff true.

$e \Vdash \bot$ iff false.

$e \Vdash (\varphi \wedge \psi)$ iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and $\pi_1 \cdot e \Vdash \varphi$ and $\pi_2 \cdot e \Vdash \psi$.

$e \Vdash (\varphi \vee \psi)$ iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and
if $\pi_1 \cdot e = 0$ then $\pi_2 \cdot e \Vdash \varphi$, and
if $\pi_1 \cdot e \neq 0$ then $\pi_2 \cdot e \Vdash \psi$.

$e \Vdash (\varphi \Rightarrow \psi)$ iff for every $r \in \mathbb{N}$ such that $r \Vdash \varphi$, $e \cdot r \downarrow$ and $e \cdot r \Vdash \psi$.

$e \Vdash (\forall n : N.\ \varphi(n))$ iff for every $n_0 \in \mathbb{N}$, $e \cdot n_0 \downarrow$ and $e \cdot n_0 \Vdash \varphi(n_0)$.

$e \Vdash (\exists n : N.\ \varphi(n))$ iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and $\pi_2 \cdot e \Vdash \varphi(\pi_1 \cdot e)$.

$e \Vdash (\forall f : N^N.\ \varphi(f))$ iff for every $f_0 : \mathbb{N} \to \mathbb{N}$ and every $r_0 \in \mathbb{N}$ such that
f_0 is computed by the r_0-th machine,
$e \cdot r_0 \downarrow$ and $e \cdot r_0 \Vdash \varphi(f_0)$.

$e \Vdash (\exists f : N^N.\ \varphi(f))$ iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and the $(\pi_1 \cdot e)$-th machine
computes a function $f_0 : \mathbb{N} \to \mathbb{N}$ and $\pi_2 \cdot e \Vdash \varphi(f_0)$.

Thm. If $\mathrm{HA} \vdash \varphi$, then there is a number $e \in \mathbb{N}$ such that $e \Vdash \varphi$.

Number realizability

$e \Vdash s = t$ iff $s = t$.

$e \Vdash \top$ iff true.

$e \Vdash \bot$ iff false.

$e \Vdash (\varphi \wedge \psi)$ iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and $\pi_1 \cdot e \Vdash \varphi$ and $\pi_2 \cdot e \Vdash \psi$.

$e \Vdash (\varphi \vee \psi)$ iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and
if $\pi_1 \cdot e = 0$ then $\pi_2 \cdot e \Vdash \varphi$, and
if $\pi_1 \cdot e \neq 0$ then $\pi_2 \cdot e \Vdash \psi$.

$e \Vdash (\varphi \Rightarrow \psi)$ iff for every $r \in \mathbb{N}$ such that $r \Vdash \varphi$, $e \cdot r \downarrow$ and $e \cdot r \Vdash \psi$.

$e \Vdash (\forall n : N.\ \varphi(n))$ iff for every $n_0 \in \mathbb{N}$, $e \cdot n_0 \downarrow$ and $e \cdot n_0 \Vdash \varphi(n_0)$.

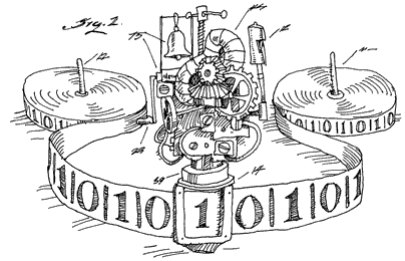
$e \Vdash (\exists n : N.\ \varphi(n))$ iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and $\pi_2 \cdot e \Vdash \varphi(\pi_1 \cdot e)$.

$e \Vdash (\forall f : N^N.\ \varphi(f))$ iff for every $f_0 : \mathbb{N} \to \mathbb{N}$ and every $r_0 \in \mathbb{N}$ such that
f_0 is computed by the r_0-th machine,
$e \cdot r_0 \downarrow$ and $e \cdot r_0 \Vdash \varphi(f_0)$.

$e \Vdash (\exists f : N^N.\ \varphi(f))$ iff $\pi_1 \cdot e \downarrow$ and $\pi_2 \cdot e \downarrow$ and the $(\pi_1 \cdot e)$-th machine
computes a function $f_0 : \mathbb{N} \to \mathbb{N}$ and $\pi_2 \cdot e \Vdash \varphi(f_0)$.

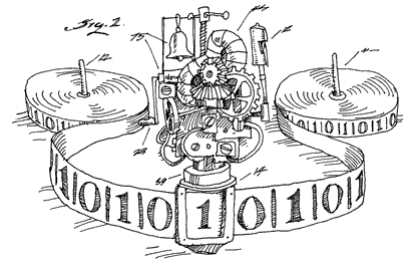
Thm. If $\mathrm{HA} \vdash \varphi$, then there is a number $e \in \mathbb{N}$ such that $\mathrm{HA} \vdash (\underline{e} \Vdash \varphi)$.

Exploring the realizability model



	statement	classical?	realizable?
1	Every number is prime or not prime.	✓ (trivially)	✓
2	After every number there is a prime.	✓	✓
3	Every map $\mathbb{N} \to \mathbb{N}$ has a zero or not.	✓ (trivially)	✗
4	Every map $\mathbb{N} \to \mathbb{N}$ is computable.	✗	?
5	Every map $\mathbb{R} \to \mathbb{R}$ is continuous.	✗	?
6	Markov's principle holds.	✓ (trivially)	?
7	Countable choice holds.	✓	?
8	Heyting arithmetic is categorical.	✗	?
9	A statement holds iff it is realized.	✗	?

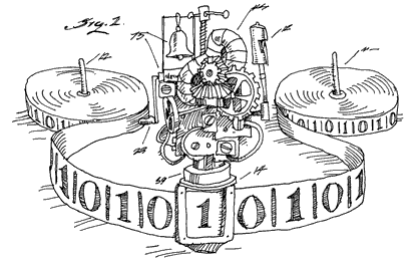
Exploring the realizability model



statement	classical?	realizable?
1 Every number is prime or not prime.	✓ (trivially)	✓
2 After every number there is a prime.	✓	✓
3 Every map $\mathbb{N} \to \mathbb{N}$ has a zero or not.	✓ (trivially)	✗
4 Every map $\mathbb{N} \to \mathbb{N}$ is computable.	✗	?
5 Every map $\mathbb{R} \to \mathbb{R}$ is continuous.	✗	?
6 Markov's principle holds.	✓ (trivially)	?
7 Countable choice holds.	✓	?
8 Heyting arithmetic is categorical.	✗	?
9 A statement holds iff it is realized.	✗	?

"$\Vdash$ 1" amounts to: There is a machine which determines of any given number whether it is prime or not.

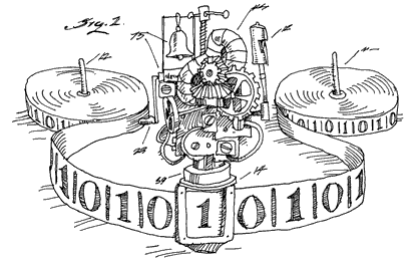
Exploring the realizability model



statement	classical?	realizable?
1 Every number is prime or not prime.	✓ (trivially)	✓
2 After every number there is a prime.	✓	✓
3 Every map $\mathbb{N} \to \mathbb{N}$ has a zero or not.	✓ (trivially)	✗
4 Every map $\mathbb{N} \to \mathbb{N}$ is computable.	✗	?
5 Every map $\mathbb{R} \to \mathbb{R}$ is continuous.	✗	?
6 Markov's principle holds.	✓ (trivially)	?
7 Countable choice holds.	✓	?
8 Heyting arithmetic is categorical.	✗	?
9 A statement holds iff it is realized.	✗	?

"$\Vdash$ 2" amounts to: There is a machine which, given a number n, computes a prime larger than n.

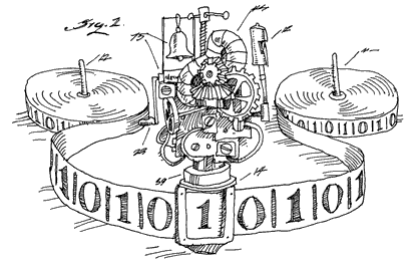
Exploring the realizability model



statement	classical?	realizable?
1 Every number is prime or not prime.	✓ (trivially)	✓
2 After every number there is a prime.	✓	✓
3 Every map $\mathbb{N} \to \mathbb{N}$ has a zero or not.	✓ (trivially)	✗
4 Every map $\mathbb{N} \to \mathbb{N}$ is computable.	✗	?
5 Every map $\mathbb{R} \to \mathbb{R}$ is continuous.	✗	?
6 Markov's principle holds.	✓ (trivially)	?
7 Countable choice holds.	✓	?
8 Heyting arithmetic is categorical.	✗	?
9 A statement holds iff it is realized.	✗	?

"$\Vdash$ 3" amounts to: There is a machine which, given a machine computing a map $f : \mathbb{N} \to \mathbb{N}$, determines whether f has a zero or not.

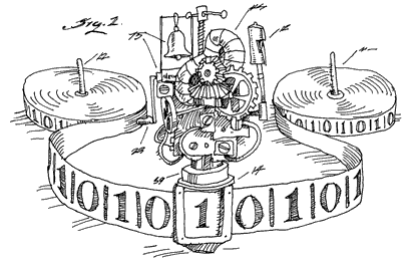
Exploring the realizability model



statement	classical?	realizable?
1 Every number is prime or not prime.	✓ (trivially)	✓
2 After every number there is a prime.	✓	✓
3 Every map $\mathbb{N} \to \mathbb{N}$ has a zero or not.	✓ (trivially)	✗
4 Every map $\mathbb{N} \to \mathbb{N}$ is computable.	✗	✓ (trivially)
5 Every map $\mathbb{R} \to \mathbb{R}$ is continuous.	✗	?
6 Markov's principle holds.	✓ (trivially)	?
7 Countable choice holds.	✓	?
8 Heyting arithmetic is categorical.	✗	?
9 A statement holds iff it is realized.	✗	?

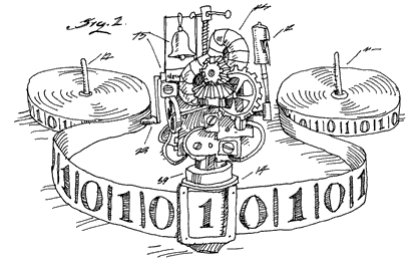
"$\Vdash$ 4" amounts to: There is a machine which, given a machine computing a map $f : \mathbb{N} \to \mathbb{N}$, outputs a machine computing f.

Exploring the realizability model



	statement	classical?	realizable?
1	Every number is prime or not prime.	✓ (trivially)	✓
2	After every number there is a prime.	✓	✓
3	Every map $\mathbb{N} \to \mathbb{N}$ has a zero or not.	✓ (trivially)	✗
4	Every map $\mathbb{N} \to \mathbb{N}$ is computable.	✗	✓ (trivially)
5	Every map $\mathbb{R} \to \mathbb{R}$ is continuous.	✗	✓ (if MP)
6	Markov's principle holds.	✓ (trivially)	?
7	Countable choice holds.	✓	?
8	Heyting arithmetic is categorical.	✗	?
9	A statement holds iff it is realized.	✗	?

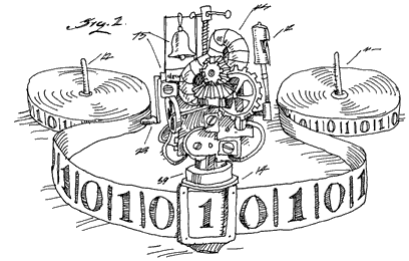
Exploring the realizability model



statement	classical?	realizable?
1 Every number is prime or not prime.	✓ (trivially)	✓
2 After every number there is a prime.	✓	✓
3 Every map $\mathbb{N} \to \mathbb{N}$ has a zero or not.	✓ (trivially)	✗
4 Every map $\mathbb{N} \to \mathbb{N}$ is computable.	✗	✓ (trivially)
5 Every map $\mathbb{R} \to \mathbb{R}$ is continuous.	✗	✓ (if MP)
6 Markov's principle holds.	✓ (trivially)	✓ (if MP)
7 Countable choice holds.	✓	?
8 Heyting arithmetic is categorical.	✗	?
9 A statement holds iff it is realized.	✗	?

"$\Vdash$ 6" amounts to: There is a machine which, given a machine computing a map $f : \mathbb{N} \to \mathbb{N}$ and given the promise that it is *not not* the case that f has a zero, determines a zero of f.

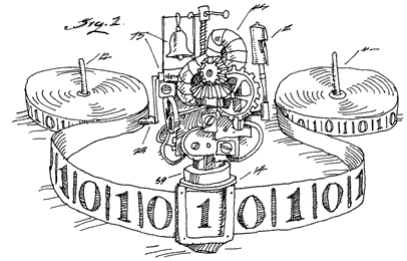
Exploring the realizability model



statement	classical?	realizable?
1 Every number is prime or not prime.	✓ (trivially)	✓
2 After every number there is a prime.	✓	✓
3 Every map $\mathbb{N} \to \mathbb{N}$ has a zero or not.	✓ (trivially)	✗
4 Every map $\mathbb{N} \to \mathbb{N}$ is computable.	✗	✓ (trivially)
5 Every map $\mathbb{R} \to \mathbb{R}$ is continuous.	✗	✓ (if MP)
6 Markov's principle holds.	✓ (trivially)	✓ (if MP)
7 Countable choice holds.	✓	✓ (always!)
8 Heyting arithmetic is categorical.	✗	?
9 A statement holds iff it is realized.	✗	?

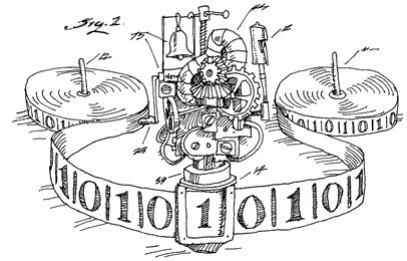
"$\Vdash$ 7" amounts to: There is a machine which, given a machine computing for every $x \in \mathbb{N}$ some $y \in A$ together with a realizer of $\varphi(x, y)$, outputs a machine computing a suitable choice function $\mathbb{N} \to A$.

Exploring the realizability model



	statement	classical?	realizable?
1	Every number is prime or not prime.	✓ (trivially)	✓
2	After every number there is a prime.	✓	✓
3	Every map $\mathbb{N} \to \mathbb{N}$ has a zero or not.	✓ (trivially)	✗
4	Every map $\mathbb{N} \to \mathbb{N}$ is computable.	✗	✓ (trivially)
5	Every map $\mathbb{R} \to \mathbb{R}$ is continuous.	✗	✓ (if MP)
6	Markov's principle holds.	✓ (trivially)	✓ (if MP)
7	Countable choice holds.	✓	✓ (always!)
8	Heyting arithmetic is categorical.	✗	✓ (if MP)
9	A statement holds iff it is realized.	✗	?

Exploring the realizability model



	statement	classical?	realizable?
1	Every number is prime or not prime.	✓ (trivially)	✓
2	After every number there is a prime.	✓	✓
3	Every map $\mathbb{N} \to \mathbb{N}$ has a zero or not.	✓ (trivially)	✗
4	Every map $\mathbb{N} \to \mathbb{N}$ is computable.	✗	✓ (trivially)
5	Every map $\mathbb{R} \to \mathbb{R}$ is continuous.	✗	✓ (if MP)
6	Markov's principle holds.	✓ (trivially)	✓ (if MP)
7	Countable choice holds.	✓	✓ (always!)
8	Heyting arithmetic is categorical.	✗	✓ (if MP)
9	A statement holds iff it is realized.	✗	✓

Metatheory of Heyting arithmetic

1. **Unprovability results:**

   There are instances of LEM which HA does not prove, such as "every Turing machine terminates or does not terminate".

2. **Disjunction property:**

   If HA proves $\varphi \vee \psi$, then HA proves φ or HA proves ψ.

3. **Existence property:**

   If HA proves $\exists n : N.\ \varphi(n)$, then there is a number $n_0 \in \mathbb{N}$ such that HA proves $\varphi(\underline{n_0})$.

4. **Growth rate:**

   If HA proves $\forall x : N.\ \exists y : N.\ \varphi(x, y)$, then there exists a **higher primitive recursive** function $f_0 : \mathbb{N} \to \mathbb{N}$ such that for all $x_0 \in \mathbb{N}$, HA proves $\varphi(\underline{x_0}, \underline{f_0(x_0)})$.

Range of machine models

1. **Turing machines**
2. **Untyped lambda calculus**
3. **Infinite-time Turing machines**
4. **Gödel's System T**
5. **Machines in the real world** – *philosophical*

Range of machine models

1. **Turing machines**
   "Every map $\mathbb{N} \to \mathbb{N}$ is computable" is realized by cat.
2. **Untyped lambda calculus**
3. **Infinite-time Turing machines**
4. **Gödel's System T**
5. **Machines in the real world** – *philosophical*

Range of machine models

1. **Turing machines**
   "Every map $\mathbb{N} \to \mathbb{N}$ is computable" is realized by cat.

2. **Untyped lambda calculus**
   "Every map $\mathbb{N} \to \mathbb{N}$ is computable" is *not* realized.

3. **Infinite-time Turing machines**

4. **Gödel's System T**

5. **Machines in the real world** – *philosophical*

Range of machine models

1. **Turing machines**
   "Every map $\mathbb{N} \to \mathbb{N}$ is computable" is realized by cat.

2. **Untyped lambda calculus**
   "Every map $\mathbb{N} \to \mathbb{N}$ is computable" is *not* realized.

3. **Infinite-time Turing machines**
   "Every map $\mathbb{N} \to \mathbb{N}$ has a zero or not" is realized by infinite search.

4. **Gödel's System T**

5. **Machines in the real world** – *philosophical*

Range of machine models

1. **Turing machines**
   "Every map $\mathbb{N} \to \mathbb{N}$ is computable" is realized by cat.

2. **Untyped lambda calculus**
   "Every map $\mathbb{N} \to \mathbb{N}$ is computable" is *not* realized.

3. **Infinite-time Turing machines**
   "Every map $\mathbb{N} \to \mathbb{N}$ has a zero or not" is realized by infinite search.

4. **Gödel's System T**
   Markov's principle is not realized.

5. **Machines in the real world** – *philosophical*

Range of machine models

1. **Turing machines**
   "Every map $\mathbb{N} \to \mathbb{N}$ is computable" is realized by cat.

2. **Untyped lambda calculus**
   "Every map $\mathbb{N} \to \mathbb{N}$ is computable" is *not* realized.

3. **Infinite-time Turing machines**
   "Every map $\mathbb{N} \to \mathbb{N}$ has a zero or not" is realized by infinite search.

4. **Gödel's System T**
   Markov's principle is not realized.

5. **Machines in the real world** – *philosophical*
   "Every map $\mathbb{R} \to \mathbb{R}$ is continuous" is realized if, in the physical world, only finitely many computational steps can be carried out in finite time and if it is possible to form tamper-free private communication channels.

A classical logic fairy tale

Narrator. Once upon a time, in a kingdom far, far away, the queen of the land and of all Möbius strips called for her royal philosopher.

Queen. Philosopher! I ask you to carry out the following order. Get me the Philosopher's Stone, or alternatively find out how one could produce arbitrary amounts of gold with it!

Philosopher. But my queen! I haven't studied anything useful! How could I fulfill this order?

Queen. That is not my concern. I'll see you again tomorrow. Should you not accomplish the task, I will take your head off.

Narrator. After a long and wakeful night the philosopher was called to the queen again.

Queen. Tell me! What do you have to report?

Philosopher. It was not easy and I needed to follow lots of obscure references, but finally I actually found out how to use the Philosopher's Stone to produce arbitrary amounts of gold. But only I can conduct this procedure, your royal highness.

Queen. Alright. So be it.

Narrator. And so years passed by, during which the philosopher imagined herself to be safe. The queen searched for the stone on her own, but as long as she hadn't found it, the philosopher didn't need to worry. Yet one day the impossible happened: The queen has found the stone! And promptly called for her philosopher.

Queen. Philosopher, look! I have found the Philosopher's Stone! Now live up to your promise! *[She hands over the stone.]*

Philosopher. Thank you. *[She inspects the stone.]* This is indeed the Philosopher's Stone. Many years ago you asked me to either acquire the Philosopher's Stone or find out how to produce arbitrary amounts of gold using it. Now it's my pleasure to present to you the Philosopher's Stone. *[She returns the stone.]*

Lecture II:
Proof transformations

for extracting constructive proofs from classical proofs

A case study in double negation

How to extract constructive proofs from classical proofs as the following?

1. **Thm.** Every infinite sequence $\alpha : \mathbb{N} \to \mathbb{N}$ is *good* in that there are numbers $i < j$ such that $\alpha(i) \leq \alpha(j)$.

   Proof. By LEM, there is a minimal value $\alpha(i)$. Set $j := i + 1$.

A case study in double negation

How to extract constructive proofs from classical proofs as the following?

1. **Thm.** Every infinite sequence $\alpha : \mathbb{N} \to \mathbb{N}$ is *good* in that there are numbers $i < j$ such that $\alpha(i) \leq \alpha(j)$.

   Proof. By LEM, there is a minimal value $\alpha(i)$. Set $j := i + 1$.

2. **Thm.** Every infinite binary sequence contains repeated terms.

   Proof. By the infinite box principle, infinitely many terms are zeros or are ones. In either case the claim follows.

A case study in double negation

How to extract constructive proofs from classical proofs as the following?

1. **Thm.** Every infinite sequence $\alpha : \mathbb{N} \to \mathbb{N}$ is *good* in that there are numbers $i < j$ such that $\alpha(i) \leq \alpha(j)$.

   Proof. By LEM, there is a minimal value $\alpha(i)$. Set $j := i + 1$.

2. **Thm.** Every infinite binary sequence contains repeated terms.

   Proof. By the infinite box principle, infinitely many terms are zeros or are ones. In either case the claim follows.

Lemma. Let X be an inhabited set of natural numbers.

1. Assuming LEM, the set X contains a minimal element.

A case study in double negation

How to extract constructive proofs from classical proofs as the following?

1. **Thm.** Every infinite sequence $\alpha : \mathbb{N} \to \mathbb{N}$ is *good* in that there are numbers $i < j$ such that $\alpha(i) \leq \alpha(j)$.

   Proof. By LEM, there is a minimal value $\alpha(i)$. Set $j := i + 1$.

2. **Thm.** Every infinite binary sequence contains repeated terms.

   Proof. By the infinite box principle, infinitely many terms are zeros or are ones. In either case the claim follows.

Lemma. Let X be an inhabited set of natural numbers.

1. Assuming LEM, the set X contains a minimal element.

Proof of 1. There is some $n \in X$. By LEM, either $\exists k \in X.\ k < n$ or not. In the first case, we continue by induction. Else n is minimal.

A case study in double negation

How to extract constructive proofs from classical proofs as the following?

1. **Thm.** Every infinite sequence $\alpha : \mathbb{N} \to \mathbb{N}$ is *good* in that there are numbers $i < j$ such that $\alpha(i) \leq \alpha(j)$.

   Proof. By LEM, there is a minimal value $\alpha(i)$. Set $j := i + 1$.

2. **Thm.** Every infinite binary sequence contains repeated terms.

   Proof. By the infinite box principle, infinitely many terms are zeros or are ones. In either case the claim follows.

Lemma. Let X be an inhabited set of natural numbers.

1. Assuming LEM, the set X contains a minimal element.
2. If X is **detachable**, then X contains a minimal element.

Proof of 1. There is some $n \in X$. By LEM, either $\exists k \in X.\ k < n$ or not. In the first case, we continue by induction. Else n is minimal.

A case study in double negation

How to extract constructive proofs from classical proofs as the following?

1. **Thm.** Every infinite sequence $\alpha : \mathbb{N} \to \mathbb{N}$ is *good* in that there are numbers $i < j$ such that $\alpha(i) \leq \alpha(j)$.

   Proof. By LEM, there is a minimal value $\alpha(i)$. Set $j := i + 1$.

2. **Thm.** Every infinite binary sequence contains repeated terms.

   Proof. By the infinite box principle, infinitely many terms are zeros or are ones. In either case the claim follows.

Lemma. Let X be an inhabited set of natural numbers.

1. Assuming LEM, the set X contains a minimal element.
2. If X is **detachable**, then X contains a minimal element.

Proof of 2. There is some $n \in X$. By assumption, either $\exists k \in X.\ k < n$ or not. In the first case, we continue by induction. Else n is minimal.

A case study in double negation

How to extract constructive proofs from classical proofs as the following?

1. **Thm.** Every infinite sequence $\alpha : \mathbb{N} \to \mathbb{N}$ is *good* in that there are numbers $i < j$ such that $\alpha(i) \leq \alpha(j)$.

   Proof. By LEM, there is a minimal value $\alpha(i)$. Set $j := i + 1$.

2. **Thm.** Every infinite binary sequence contains repeated terms.

   Proof. By the infinite box principle, infinitely many terms are zeros or are ones. In either case the claim follows.

Lemma. Let X be an inhabited set of natural numbers.

1. Assuming LEM, the set X contains a minimal element.
2. If X is **detachable**, then X contains a minimal element.
3. It is **not not** the case that X contains a minimal element.

Proof of 2. There is some $n \in X$. By assumption, either $\exists k \in X.\ k < n$ or not. In the first case, we continue by induction. Else n is minimal.

A case study in double negation

How to extract constructive proofs from classical proofs as the following?

1. **Thm.** Every infinite sequence $\alpha : \mathbb{N} \to \mathbb{N}$ is *good* in that there are numbers $i < j$ such that $\alpha(i) \leq \alpha(j)$.

   Proof. By LEM, there is a minimal value $\alpha(i)$. Set $j := i + 1$.

2. **Thm.** Every infinite binary sequence contains repeated terms.

   Proof. By the infinite box principle, infinitely many terms are zeros or are ones. In either case the claim follows.

Lemma. Let X be an inhabited set of natural numbers.

1. Assuming LEM, the set X contains a minimal element.
2. If X is **detachable**, then X contains a minimal element.
3. It is **not not** the case that X contains a minimal element.

Proof of 3. There is some $n \in X$. Assume that X does not contain a minimum. Then it is not the case that $\exists k \in X.\ k < n$, as else $\bot$ by induction. Hence n is minimal. This is a contradiction.

The double-negation embedding

Def. For formulas over a fixed first-order signature, the **$\neg\neg$-translation** $\varphi \mapsto \varphi^{\neg\neg}$ is defined by the following clauses.

$$(\varphi_{\text{atomic}})^{\neg\neg} :\equiv \neg\neg\varphi_{\text{atomic}} \qquad (\varphi \Rightarrow \psi)^{\neg\neg} :\equiv (\varphi^{\neg\neg} \Rightarrow \psi^{\neg\neg})$$

$$\bot^{\neg\neg} :\equiv \neg\neg\bot \qquad \top^{\neg\neg} :\equiv \top$$

$$(\varphi \vee \psi)^{\neg\neg} :\equiv \neg\neg(\varphi^{\neg\neg} \vee \psi^{\neg\neg}) \qquad (\varphi \wedge \psi)^{\neg\neg} :\equiv (\varphi^{\neg\neg} \wedge \psi^{\neg\neg})$$

$$(\exists x : X.\ \varphi)^{\neg\neg} :\equiv \neg\neg(\exists x : X.\ \varphi^{\neg\neg}) \qquad (\forall x : X.\ \varphi)^{\neg\neg} :\equiv (\forall x : X.\ \varphi^{\neg\neg})$$

Ex. $(\forall a{:}X.\, \exists b{:}X.\, a = b \vee \ldots)^{\neg\neg} \equiv (\forall a{:}X.\, \neg\neg\exists b{:}X.\, \neg\neg(\neg\neg(a = b) \vee (\ldots)^{\neg\neg}))$.

The double-negation embedding

Def. For formulas over a fixed first-order signature, the **$\neg\neg$-translation** $\varphi \mapsto \varphi^{\neg\neg}$ is defined by the following clauses.

$$(\varphi_{\text{atomic}})^{\neg\neg} :\equiv \neg\neg\varphi_{\text{atomic}} \qquad (\varphi \Rightarrow \psi)^{\neg\neg} :\equiv (\varphi^{\neg\neg} \Rightarrow \psi^{\neg\neg})$$

$$\bot^{\neg\neg} :\equiv \neg\neg\bot \qquad \top^{\neg\neg} :\equiv \top$$

$$(\varphi \vee \psi)^{\neg\neg} :\equiv \neg\neg(\varphi^{\neg\neg} \vee \psi^{\neg\neg}) \qquad (\varphi \wedge \psi)^{\neg\neg} :\equiv (\varphi^{\neg\neg} \wedge \psi^{\neg\neg})$$

$$(\exists x : X.\ \varphi)^{\neg\neg} :\equiv \neg\neg(\exists x : X.\ \varphi^{\neg\neg}) \qquad (\forall x : X.\ \varphi)^{\neg\neg} :\equiv (\forall x : X.\ \varphi^{\neg\neg})$$

Ex. $(\forall a{:}X.\, \exists b{:}X.\, a = b \vee \ldots)^{\neg\neg} \equiv (\forall a{:}X.\, \neg\neg\exists b{:}X.\, \neg\neg(\neg\neg(a = b) \vee (\ldots)^{\neg\neg}))$.

Prop. Classically, $\varphi \Leftrightarrow \varphi^{\neg\neg}$.

The double-negation embedding

Def. For formulas over a fixed first-order signature, the **$\neg\neg$-translation** $\varphi \mapsto \varphi^{\neg\neg}$ is defined by the following clauses.

$$(\varphi_{\text{atomic}})^{\neg\neg} :\equiv \neg\neg\varphi_{\text{atomic}} \qquad (\varphi \Rightarrow \psi)^{\neg\neg} :\equiv (\varphi^{\neg\neg} \Rightarrow \psi^{\neg\neg})$$
$$\bot^{\neg\neg} :\equiv \neg\neg\bot \qquad \top^{\neg\neg} :\equiv \top$$
$$(\varphi \vee \psi)^{\neg\neg} :\equiv \neg\neg(\varphi^{\neg\neg} \vee \psi^{\neg\neg}) \qquad (\varphi \wedge \psi)^{\neg\neg} :\equiv (\varphi^{\neg\neg} \wedge \psi^{\neg\neg})$$
$$(\exists x : X.\ \varphi)^{\neg\neg} :\equiv \neg\neg(\exists x : X.\ \varphi^{\neg\neg}) \qquad (\forall x : X.\ \varphi)^{\neg\neg} :\equiv (\forall x : X.\ \varphi^{\neg\neg})$$

Ex. $(\forall a{:}X.\, \exists b{:}X.\, a = b \vee \ldots)^{\neg\neg} \equiv (\forall a{:}X.\, \neg\neg\exists b{:}X.\, \neg\neg(\neg\neg(a = b) \vee (\ldots)^{\neg\neg}))$.

Prop. Classically, $\varphi \Leftrightarrow \varphi^{\neg\neg}$.

Thm. For every formula φ and set of formulas Γ:

1. Minimally, $\neg\neg(\varphi^{\neg\neg}) \Rightarrow \varphi^{\neg\neg}$.
2. Minimally, $\varphi^{\neg\neg} \Leftrightarrow \neg\neg\varphi$ in case that φ is geometric ($R\top\bot\wedge\vee\exists\bigvee$).
3. If Γ entails φ classically, then $\Gamma^{\neg\neg}$ entails $\varphi^{\neg\neg}$ minimally.

The double-negation embedding

Def. For formulas over a fixed first-order signature, the **$\neg\neg$-translation** $\varphi \mapsto \varphi^{\neg\neg}$ is defined by the following clauses.

$$(\varphi_{\text{atomic}})^{\neg\neg} :\equiv \neg\neg\varphi_{\text{atomic}} \qquad (\varphi \Rightarrow \psi)^{\neg\neg} :\equiv (\varphi^{\neg\neg} \Rightarrow \psi^{\neg\neg})$$
$$\bot^{\neg\neg} :\equiv \neg\neg\bot \qquad \top^{\neg\neg} :\equiv \top$$
$$(\varphi \vee \psi)^{\neg\neg} :\equiv \neg\neg(\varphi^{\neg\neg} \vee \psi^{\neg\neg}) \qquad (\varphi \wedge \psi)^{\neg\neg} :\equiv (\varphi^{\neg\neg} \wedge \psi^{\neg\neg})$$
$$(\exists x : X.\ \varphi)^{\neg\neg} :\equiv \neg\neg(\exists x : X.\ \varphi^{\neg\neg}) \qquad (\forall x : X.\ \varphi)^{\neg\neg} :\equiv (\forall x : X.\ \varphi^{\neg\neg})$$

Ex. $(\forall a{:}X.\, \exists b{:}X.\, a = b \vee \ldots)^{\neg\neg} \equiv (\forall a{:}X.\, \neg\neg\exists b{:}X.\, \neg\neg(\neg\neg(a = b) \vee (\ldots)^{\neg\neg}))$.

Prop. Classically, $\varphi \Leftrightarrow \varphi^{\neg\neg}$.

Thm. For every formula φ and set of formulas Γ:

1. Minimally, $\neg\neg(\varphi^{\neg\neg}) \Rightarrow \varphi^{\neg\neg}$.
2. Minimally, $\varphi^{\neg\neg} \Leftrightarrow \neg\neg\varphi$ in case that φ is geometric ($R\top\bot\wedge\vee\exists\bigvee$).
3. If Γ entails φ classically, then $\Gamma^{\neg\neg}$ entails $\varphi^{\neg\neg}$ minimally.

Cor. If PA proves φ, then HA proves $\varphi^{\neg\neg}$.

The double-negation embedding

Def. For formulas over a fixed first-order signature, the **$\neg\neg$-translation** $\varphi \mapsto \varphi^{\neg\neg}$ is defined by the following clauses.

$$(\varphi_{\text{atomic}})^{\neg\neg} :\equiv \neg\neg\varphi_{\text{atomic}} \qquad (\varphi \Rightarrow \psi)^{\neg\neg} :\equiv (\varphi^{\neg\neg} \Rightarrow \psi^{\neg\neg})$$
$$\bot^{\neg\neg} :\equiv \neg\neg\bot \qquad \top^{\neg\neg} :\equiv \top$$
$$(\varphi \vee \psi)^{\neg\neg} :\equiv \neg\neg(\varphi^{\neg\neg} \vee \psi^{\neg\neg}) \qquad (\varphi \wedge \psi)^{\neg\neg} :\equiv (\varphi^{\neg\neg} \wedge \psi^{\neg\neg})$$
$$(\exists x : X.\ \varphi)^{\neg\neg} :\equiv \neg\neg(\exists x : X.\ \varphi^{\neg\neg}) \qquad (\forall x : X.\ \varphi)^{\neg\neg} :\equiv (\forall x : X.\ \varphi^{\neg\neg})$$

Ex. $(\forall a{:}X.\, \exists b{:}X.\, a = b \vee \ldots)^{\neg\neg} \equiv (\forall a{:}X.\, \neg\neg\exists b{:}X.\, \neg\neg(\neg\neg(a = b) \vee (\ldots)^{\neg\neg}))$.

Prop. Classically, $\varphi \Leftrightarrow \varphi^{\neg\neg}$.

Thm. For every formula φ and set of formulas Γ:

1. Minimally, $\neg\neg(\varphi^{\neg\neg}) \Rightarrow \varphi^{\neg\neg}$.
2. Minimally, $\varphi^{\neg\neg} \Leftrightarrow \neg\neg\varphi$ in case that φ is geometric ($R\top\bot\wedge\vee\exists\bigvee$).
3. If Γ entails φ classically, then $\Gamma^{\neg\neg}$ entails $\varphi^{\neg\neg}$ minimally.

Cor. If PA proves φ, then HA proves $\varphi^{\neg\neg}$.

Rem. Theorem and corollary hold for every **local operator** ∇ in place of $\neg\neg$, in particular for $\neg_{\perp}\neg_{\perp}\varphi := ((\varphi \Rightarrow \perp\!\!\!\perp) \Rightarrow \perp\!\!\!\perp)$ for some arbitrary formula $\perp\!\!\!\perp$.

Barr's theorem / Friedman's trick / A-translation

Thm. Let Γ be a set of geometric sequents over a fixed signature. Let σ be a geometric sequent. Then the following are equivalent:

0. σ holds for the generic model of Γ (in its classifying topos).
1. σ is provable from Γ in geometric logic.
2. σ is provable from Γ in intuitionistic logic.
3. σ is provable from Γ in classical logic.
4. (Assuming ZORN) σ is provable from Γ in classical logic with AC.

Proof of "3 $\Rightarrow$ 2". Write $\sigma \equiv (\alpha \vdash_{\vec{x}} \beta)$. Then intuitionistically,

$$\alpha \Longrightarrow \neg\neg\alpha \Longleftrightarrow \alpha^{\neg\neg} \Longrightarrow \beta^{\neg\neg} \Longleftrightarrow \neg\neg\beta \equiv ((\beta \Longrightarrow \bot) \Rightarrow \bot)$$

Barr's theorem / Friedman's trick / A-translation

Thm. Let Γ be a set of geometric sequents over a fixed signature. Let σ be a geometric sequent. Then the following are equivalent:

0. σ holds for the generic model of Γ (in its classifying topos).
1. σ is provable from Γ in geometric logic.
2. σ is provable from Γ in intuitionistic logic.
3. σ is provable from Γ in classical logic.
4. (Assuming ZORN) σ is provable from Γ in classical logic with AC.

Proof of "3 $\Rightarrow$ 2". Write $\sigma \equiv (\alpha \vdash_{\vec{x}} \beta)$. Then intuitionistically,

$$\alpha \Longrightarrow \neg\neg\alpha \Longleftrightarrow \alpha^{\neg\neg} \Longrightarrow \beta^{\neg\neg} \Longleftrightarrow \neg\neg\beta \equiv ((\beta \Longrightarrow \bot\!\!\!\bot) \Rightarrow \bot\!\!\!\bot)$$

Barr's theorem / Friedman's trick / A-translation

Thm. Let Γ be a set of geometric sequents over a fixed signature. Let σ be a geometric sequent. Then the following are equivalent:

0. σ holds for the generic model of Γ (in its classifying topos).
1. σ is provable from Γ in geometric logic.
2. σ is provable from Γ in intuitionistic logic.
3. σ is provable from Γ in classical logic.
4. (Assuming ZORN) σ is provable from Γ in classical logic with AC.

Proof of "3 $\Rightarrow$ 2". Write $\sigma \equiv (\alpha \vdash_{\vec{x}} \beta)$. Then intuitionistically,

$$\alpha \Longrightarrow \neg\neg\alpha \Longleftrightarrow \alpha^{\neg\neg} \Longrightarrow \beta^{\neg\neg} \Longleftrightarrow \neg\neg\beta \equiv ((\beta \Longrightarrow \beta) \Rightarrow \beta)$$

Barr's theorem / Friedman's trick / A-translation

Thm. Let Γ be a set of geometric sequents over a fixed signature. Let σ be a geometric sequent. Then the following are equivalent:

0. σ holds for the generic model of Γ (in its classifying topos).
1. σ is provable from Γ in geometric logic.
2. σ is provable from Γ in intuitionistic logic.
3. σ is provable from Γ in classical logic.
4. (Assuming ZORN) σ is provable from Γ in classical logic with AC.

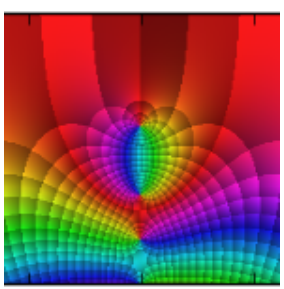
Proof of "3 $\Rightarrow$ 2". Write $\sigma \equiv (\alpha \vdash_{\vec{x}} \beta)$. Then intuitionistically,

$$\alpha \Longrightarrow \neg\neg\alpha \Longleftrightarrow \alpha^{\neg\neg} \Longrightarrow \beta^{\neg\neg} \Longleftrightarrow \neg\neg\beta \equiv ((\beta \Longrightarrow \beta) \Rightarrow \beta) \Longrightarrow \beta.$$

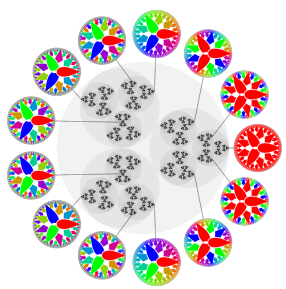
Lecture III:

Extracting constructive proofs from invalid* proofs

Lecture III:
Extracting constructive proofs from invalid* proofs

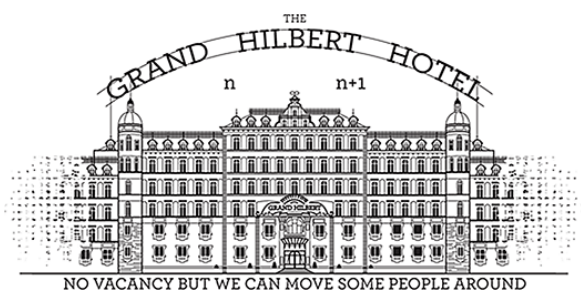


$\mathbb{C}$



$\mathbb{Q}_p$

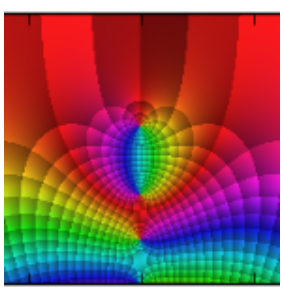
$\mathbb{F}_1$



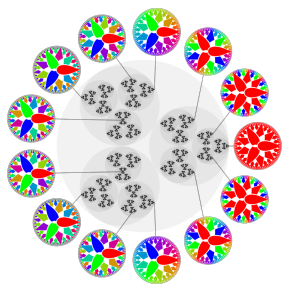
∞

Lecture III:
Extracting constructive proofs from invalid* proofs

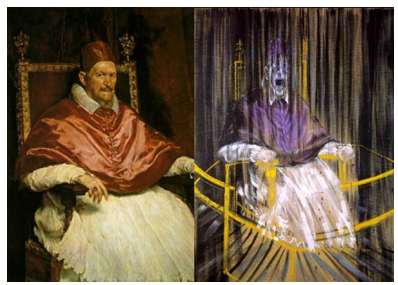
** higher-order proofs of first-order statements using the assumption that a given (perhaps uncountable) set is countable*



$\mathbb{C}$



$\mathbb{Q}_p$

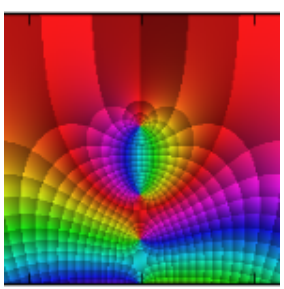


$\mathbb{F}_1$

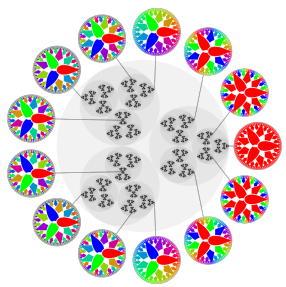
∞

Lecture III:
Extracting constructive proofs from invalid* proofs

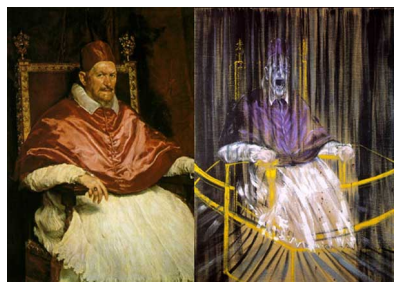
** higher-order proofs of first-order statements using the assumption that a given (perhaps uncountable) set is countable*



$\mathbb{C}$



$\mathbb{Q}_p$



$\mathbb{F}_1$

∞

A quantifier for finite approximations

Let X be a (perhaps uncountable) set. By a **finite approximation** to a surjection $\mathbb{N} \twoheadrightarrow X$, we mean a **finite list** of elements of X. Notation:

- empty list: $[]$
- extension: $[x_1, \ldots, x_n] ::^r x_{n+1} = [x_1, \ldots, x_n, x_{n+1}]$
- refinement relation: $[x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m}] \preceq [x_1, \ldots, x_n]$
- element access: $\sigma[i] =$ element at position i in σ

A quantifier for finite approximations

Let X be a (perhaps uncountable) set. By a **finite approximation** to a surjection $\mathbb{N} \twoheadrightarrow X$, we mean a **finite list** of elements of X. Notation:

- empty list: $[]$
- extension: $[x_1, \ldots, x_n] ::^r x_{n+1} = [x_1, \ldots, x_n, x_{n+1}]$
- refinement relation: $[x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m}] \preceq [x_1, \ldots, x_n]$
- element access: $\sigma[i] =$ element at position i in σ

For monotone predicates P of finite lists, we introduce a **quantifier** ∇ such that "$\nabla^{\tau \preceq \sigma}.\ P(\tau)$" expresses that **no matter how σ evolves to a better approximation τ, eventually $P(\tau)$ will hold**.

$$\frac{P(\sigma)}{\nabla^{\tau \preceq \sigma}.\ P(\tau)}\ (\sigma \in X^*) \qquad \frac{\forall^{x \in X}.\ \nabla^{\tau \preceq (\sigma ::^r x)}.\ P(\tau)}{\nabla^{\tau \preceq \sigma}.\ P(\tau)}\ (\sigma \in X^*)$$

$$\frac{\forall^{\tau \preceq \sigma}.\ a \in \tau \Rightarrow \nabla^{\upsilon \preceq \tau}.\ P(\upsilon)}{\nabla^{\tau \preceq \sigma}.\ P(\tau)}\ (\sigma \in X^*, a \in X)$$

The generic surjection

Def. The **∇-translation** $\varphi \mapsto \varphi^\nabla$ into formulas with a free variable $\sigma : X^*$ (denoting the **current stage**) is defined by the following clauses.

$$
\begin{aligned}
(\varphi_{\text{atomic}})^\nabla &:\equiv \nabla^{\tau \preceq \sigma}.\ \varphi_{\text{atomic}} \\
\bot^\nabla &:\equiv \nabla^{\tau \preceq \sigma}.\ \bot \\
(\varphi \vee \psi)^\nabla &:\equiv \nabla^{\tau \preceq \sigma}.\ (\varphi^\nabla[\tau/\sigma] \vee \psi^\nabla[\tau/\sigma]) \\
(\exists^{x:X}.\ \varphi)^\nabla &:\equiv \nabla^{\tau \preceq \sigma}.\ (\exists^{x:X}.\ \varphi^\nabla[\tau/\sigma]) \\
(\varphi \Rightarrow \psi)^\nabla &:\equiv \forall^{\tau \preceq \sigma}.\ (\varphi^\nabla[\tau/\sigma] \Rightarrow \psi^\nabla[\tau/\sigma]) \\
\top^\nabla &:\equiv \top \\
(\varphi \wedge \psi)^\nabla &:\equiv (\varphi^\nabla \wedge \psi^\nabla) \\
(\forall^{x:X}.\ \varphi)^\nabla &:\equiv (\forall^{x:X}.\ \varphi^\nabla[\sigma/\tau]) \\
(\alpha(n){=}x)^\nabla &:\equiv (\nabla^{\tau \preceq \sigma}.\ (\mathsf{len}(\tau) > n \wedge \tau[n] = x))
\end{aligned}
$$

Ex. $(\forall^{x:X}.\ \exists^{n:\mathbb{N}}.\ \alpha(n){=}x)^\nabla \equiv$
$(\forall^{x:X}.\ \nabla^{\tau \preceq \sigma}.\ \exists^{n:\mathbb{N}}.\ \nabla^{\upsilon \preceq \tau}.\ (\mathsf{len}(\upsilon) > n \wedge \upsilon[n] = x))$.

Thm. [Joyal–Tierney 1984] For **first-order** formulas φ not referring to α, $\varphi^\nabla \Rightarrow \varphi$ intuitionistically.