Peano Arithmetic in Constructive Type Theory and Tennenbaum's Theorem

Marc Hermes

29. November 2021

SAARLAND UNIVERSITY
COMPUTER SCIENCE
SIC Saarland Informatics Campus

- This work is build on the Coq library of undecidability proofs [Forster et al., 2020]
- Followed classical presentations of Tennenbaum's Theorem [Smith, 2014]
- I want to thank Prof. Dr. Weber, Dominik Kirst, Prof. Dr. Smolka.
and the members of the PSL for conversations and inputs.

Questions of the Talk

What are the computable models of Peano arithmetic?

Why care about constructive mathematics?

1. Setup (Tennenbaum) → 2. Constr. Math -- Break --> 3. Tennenbaum again

1. Setup

Peano Arithmetic

We have a first-order language.

- Logical symbols:

$$\wedge, \vee, \rightarrow, \neg, =, \forall, \exists$$

- Non-logical symbols:

$$O, S, \oplus, \otimes$$

And Axioms:

$$\begin{aligned} Sx &\neq O & Sx = Sy &\rightarrow x = y \\ x \oplus O &= x & (Sx) \oplus y &= S(x \oplus y) \\ x \otimes O &= O & (Sx) \times y &= y \oplus (x \otimes y) \end{aligned}$$

$$\varphi(O) \rightarrow (\forall x.\, \varphi(x) \rightarrow \varphi(Sx)) \rightarrow \forall x.\, \varphi(x)$$

Peano Arithmetic

The intended interpretation is over $\mathbb{N}$

$\mathbb{N}$

interprete

0	0
S	$n \mapsto n+1 : \mathbb{N} \to \mathbb{N}$
$\oplus$	$(x,y) \mapsto x+y : \mathbb{N}^2 \to \mathbb{N}$
$\otimes$	$(x,y) \mapsto x \cdot y : \mathbb{N}^2 \to \mathbb{N}$

Models of PA

We can generalize to more models.

0 ⟼ (interprete) $0^{\mathcal{M}} \in \mathcal{M}$

S ⟼ $S^{\mathcal{M}} : \mathcal{M} \to \mathcal{M}$

$\oplus$ ⟼ $+^{\mathcal{M}} : \mathcal{M}^2 \to \mathcal{M}$

$\otimes$ ⟼ $\times^{\mathcal{M}} : \mathcal{M}^2 \to \mathcal{M}$

s.t. $\mathcal{M}$ satisfies the PA axioms

Non-standard Model of PA

Compactness Theorem

If every finite $\Gamma \subseteq \mathcal{T}$ has a model, then so has $\mathcal{T}$.

$$PA^* := PA + (c>1), (c>2), (c>3), \ldots$$

finite $\Gamma \subseteq PA^*$ has only finite $c>n_1, \ldots, c>n_k$

$\Rightarrow$ $\mathbb{N}$ is a model of Γ for $c^{\mathbb{N}} := \max\{n_k\} + 1$

$\Rightarrow$ PA^* has a model $\mathcal{M}$

$\mathcal{M}$ is also a model of PA, but $\mathcal{M} \not\cong \mathbb{N}$

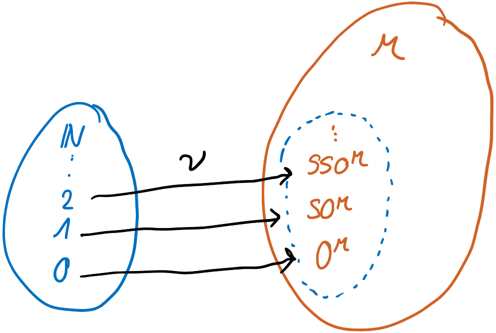
since $c^{\mathcal{M}} > \mathbb{N}$

Models of PA

$\mathbb{N}$ is still quite special:

$\nu(0) := 0^{\mathcal{M}}$

$\nu(n+1) := S^{\mathcal{M}}(\nu(n))$



ν inj. and homom.

$\Rightarrow$ embedding of $\mathbb{N}$ into $\mathcal{M}$

Consequence:

$\mathbb{N} \vDash \exists x : \alpha_0(x) \implies \mathcal{M} \vDash \exists x : \alpha_0(x)$

$\alpha_0(n) \rightsquigarrow \alpha_0(\nu(n))$

(no $\forall, \exists$ e.g. polynomial equation

$\mathbb{N}$ countable, has computable operations

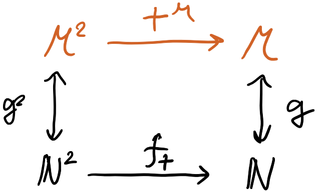
Computable Models

- There is a bijection $g : \mathbb{N} \to \mathcal{M}$
- The operations on $\mathcal{M}$ are computable.

$+^{\mathcal{M}}$ is computable

$\Updownarrow$

$f_+ : \mathbb{N}^2 \to \mathbb{N}$ is "computable"



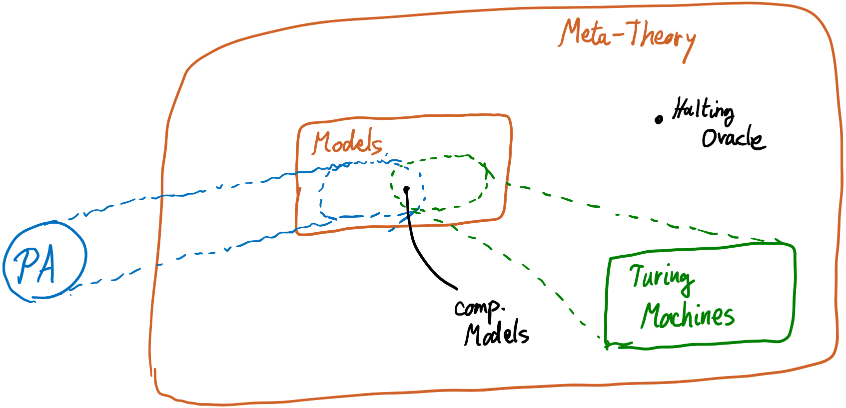
Tennebaum's Theorem (classical) [Tennenbaum, 1959, Kaye, 2011, Smith, 2014]

No countable non-standard model of PA is computable.

Still: what do we mean by computable?

Computable Models

One way to make the statement precise is to replace computable with "computable by a Turing machine".

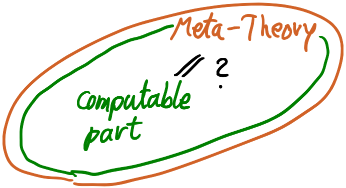


some complicated predicate in our Meta-theory

Definitions and results involving computability:

- $A \subseteq \mathbb{N}$ is decidable $:\Leftrightarrow$ there is a computable f halting on every input with $f(n) = 1 \leftrightarrow n \in A$.
- $A \subseteq \mathbb{N}$ is enumerable $:\Leftrightarrow$ there is a computable f such that $f(n)$ halts iff $n \in A$.
- Theorem: if f, g are computable, then $f \circ g$ is computable.

Can we get rid off it ?



Halting Problem

Given the set of all Turing Machines TM we can define $\mathcal{O}\colon \mathrm{TM} \to \{0, 1, *\}$ by

$$\mathcal{O}(T) := \begin{cases} 1, & T \text{ halts on empty input} \\ 0, & T \text{ does not halt on empty input} \\ *, & \text{else} \end{cases}$$

Is $\mathcal{O}$ defined for all Turing machines? For every given T, we have

- T halts, therefore $\mathcal{O}$ returns 1
- T does not halt, therefore $\mathcal{O}$ returning 0

This shows that $\mathcal{O} : \mathrm{TM} \to \{0, 1\}$ is a function, and since it solves the Halting Problem, it is not computable.

2. Constructive Mathematics

Mathematics without the law of excluded middle (LEM).

Removing axioms is very common in mathematics:

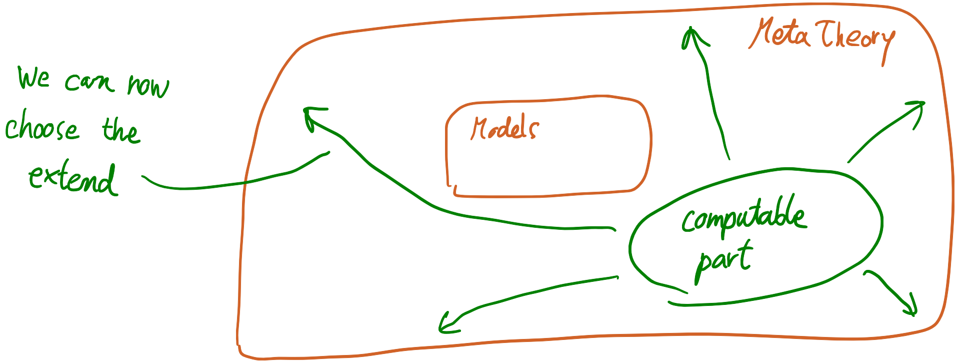
~~$ab = ba$~~ $\rightsquigarrow$ more groups, rings, algebras

~~parallel axiom~~ $\rightsquigarrow$ non-euclidean geometries

~~LEM~~ $\rightsquigarrow$??? more axioms, possible theories

Freedom

Without LEM we have an agnostic meta-theory regarding computability



Constructive Mathematics

- Constructive mathematics started with [Brouwer, 1907].
- Contributors: Heyting, Kolmogorov, Markov, Bishop, Weyl, Friedman ...
- Appears naturally as the internal logic of some topoi.
- Important applications in computer science.
- Recent AMS price awarded to a introductory paper by [Bauer, 2017].

Things to get used to:

- No more truth-semantics.
- In general, double-negations stick around.
- Showing $\neg \forall x. P(x)$ does not prove $\exists x. \neg P(x)$.
- There are several notions of finite and infinite.
- Possible to assume that all functions $\mathbb{R} \to \mathbb{R}$ are continuous.

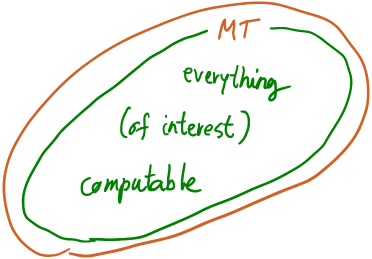
$\neg\neg A$ "A cannot be proven false"
„potentially A"

Intermission

Break for discussion

3. Tennenbaum's Theorem

Overview again



We do this by assuming CT:

„every func. $\mathbb{N} \to \mathbb{N}$ is Turing comp."

So for every $f : \mathbb{N} \to \mathbb{N}$ the axiom asserts there is a TM T_f computing it

Most importantly: Model $\equiv$ computable Model

Notions in Computatbility

No more need to specify „computable f" !

For any predicate P on $\mathbb{N}$, it is

- decidable iff $\exists (f : \mathbb{N} \to \mathbb{N})\, \forall n.\, (P(n) \leftrightarrow f(n) = 0)$.
- enumerable iff $\exists (f : \mathbb{N} \to \mathbb{N} \cup \{*\})\, \forall n.\, (P(n) \leftrightarrow \exists m.\, f(m) = n)$.

Any type X is

- discrete iff equality $=$ on X is decidable.
- apart iff apartness $\neq$ in X is decidable.
- enumerable iff $\exists (f : \mathbb{N} \to X \cup \{*\})\, \forall x\, \exists n.\, f(n) = x$.
- witnessing iff X has a witness operator.

Q-Representability

Classical result (c.f. [Smith, 2013]):

Q-Representability

If $f : \mathbb{N} \to \mathbb{N}$ is (Turing) computable, then there is a binary Σ_1 formula $\varphi_f(x, y)$ such that for every $n : \mathbb{N}$

$$Q \vdash \forall y. \varphi_f(\overline{n}, y) \leftrightarrow \overline{f(n)} = y$$

By CT, every function $\mathbb{N} \to \mathbb{N}$ is (Turing) computable, so we get:

CT_Q

Every function $f : \mathbb{N} \to \mathbb{N}$ is representable in Q by some binary Σ_1 formula φ_f.

Representibility Theorem

Representibility Theorem (RT_Q)

Any enumerable (decidable) predicate on $\mathbb{N}$ is weakly (strongly) representable in Q.

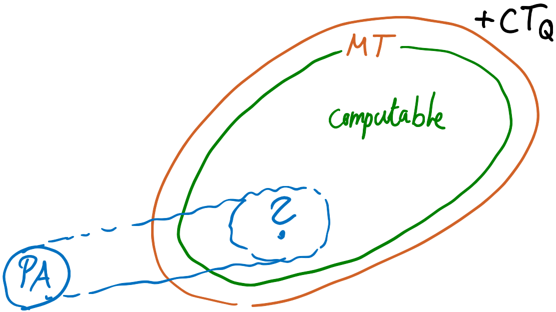
For p There is some $\varphi_p(x)$ s.t.

(weakly) $\forall n : \mathbb{N} \quad p(n) \iff Q \vdash \varphi_p(\overline{n})$

(strongly) $\forall n : \mathbb{N} \quad p(n) \implies Q \vdash \varphi_p(\overline{n})$

$\neg p(n) \implies Q \vdash \neg \varphi_p(\overline{n})$

Overview again



brings computability closer to PA

CT_Q : every $\mathbb{N} \to \mathbb{N}$ is repres. in Q

What are the ~~comp~~ models of PA ?

Result in Computability Theory

Inseparable enumerable predicates

Assuming RT_Q, there are disjoint enumerable predicates A, B on $\mathbb{N}$ which cannot be separated by a decidable predicate C.

Proof Idea

ϕ_n enumeration of formulas

$A := \{ n \in \mathbb{N} \mid Q \vdash \phi_n(\overline{n}) \}$ $\quad$ $B := \{ n \in \mathbb{N} \mid Q \vdash \neg\phi_n(\overline{n}) \}$

both are enum. since Proofs $Q \vdash$ are enum.

Tennenbaum ingredients

Inseparable Formulas (Insep)

Assuming RT_Q, there are disjoint Σ_1-formulas which cannot be separated by a decidable predicate D on $\mathbb{N}$.

Markov's Principle (MP)

If a function $\mathbb{N} \to \mathbb{N}$ potentially hits 0, it hits 0.

Lemma

Assuming RT_Q and MP, if $\mathcal{M} \not\cong \mathbb{N}$ then there potentially is an element $d : \mathcal{M}$ such that $\{ n : \mathbb{N} \mid n \text{ divides } d \}$ is not decidable.

Tennenbaum's Theorem (constructive)

Assuming RT_Q and MP, if $\mathcal{M}$ has decidable divisibility with respect to numerals, then $\mathcal{M} \simeq \mathbb{N}$.

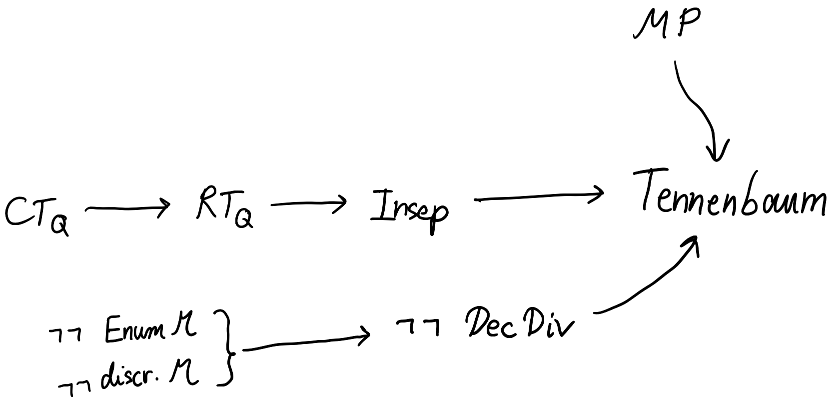
Assume $\mathcal{M} \not\simeq \mathbb{N}$

By the Lemma there is $d : \mathcal{M}$ for which $\{n : \mathbb{N} \mid n \text{ div } d\}$ is not dec. $\lightning$ to assump.

So we have $\neg \mathcal{M} \not\simeq \mathbb{N}$

and therefore $\mathcal{M} \simeq \mathbb{N}$ by MP $\square$

Tennenbaum



Tennenbaum

WCT_Q : Every $f : \mathbb{N} \to \mathbb{N}$ is potentially repr. in Q

$\mathrm{Enum}_\Sigma\, \mathcal{M} \to \mathrm{Witness}\, \mathcal{M}$

$\mathcal{M} \vDash PA \wedge \mathrm{apart}\, \mathcal{M} \to \mathrm{discr.}\, \mathcal{M}$

MP for ν $\rightarrow$ Tennenbaum

$WCT_Q \longrightarrow$ Tennenbaum

$\left.\begin{array}{l}\neg\neg\, \mathrm{Enum}\, \mathcal{M} \\ \neg\neg\, \mathrm{discr.}\, \mathcal{M}\end{array}\right\} \longrightarrow \left\{\begin{array}{l}\neg\neg\, \mathrm{Witness}\, \mathcal{M} \\ \neg\neg\, \mathrm{apart}\, \mathcal{M}\end{array}\right\} \longrightarrow$ Tennenbaum

Wrapping things up

Coq Development

Coq is a proof-assistant. Helps by organizing and keeping track of proofs, some automation and most crucially: checks them for correctness.

- Mechanized first-order PA, building on work from the Coq library of undecidability proofs [Forster et al., 2020]
- 4200 lines of code (loc)
- 1100 loc for specifications
- 3200 loc of proofs.
- The equality $=$ of PA was interpreted as equality on the domain type.

Contributions

- Showing a finite fragment of PA undecidable [Kirst and Hermes, 2021].
- To the best of knowledge: first mechanized proof of Tennenbaum's Theorem.
- Discussion and mechanization of two more variants of the theorem. [Makholm, , McCarty, 1987, McCarty, 1988]

Future Work

- Deductive proves of some more work intensive theorems
- Express computability of operations with respect to an abstract notion of computability.
- Equivalence to some version of MP?
- Mechanize the proof of $CT_Q \to RT_Q$ (seems very reachable)
- Show $CT \to CT_Q$ (ambitious)

Final Words

“Dieses Tertium non datur dem Mathematiker zu nehmen, wäre etwa, wie wenn man dem Astronomen das Fernrohr oder dem Boxer den Gebrauch der Fäuste untersagen wollte.”
(Hilbert)

“Restricting a mathematician to a logic with the law of excluded middle is like putting boxing gloves over the hands of a boxer. It greatly restricts what he can do.”

Bibliography I

Bauer, A. (2017).
Five stages of accepting constructive mathematics.
Bulletin of the American Mathematical Society, 54(3):481–498.

Brouwer, L. E. J. (1907).
Over de grondslagen der wiskunde.
Maas & van Suchtelen.

Forster, Y., Larchey-Wendling, D., Dudenhefner, A., Heiter, E., Kirst, D., Kunze, F., Smolka, G., Spies, S., Wehr, D., and Wuttke, M. (2020).
A Coq library of undecidable problems.
In *CoqPL 2020 The Sixth International Workshop on Coq for Programming Languages*.

Kaye, R. (2011).
Tennenbaum's theorem for models of arithmetic.
Set Theory, Arithmetic, and Foundations of Mathematics. Ed. by J. Kennedy and R. Kossak. Lecture Notes in Logic. Cambridge, pages 66–79.

Kirst, D. and Hermes, M. (2021).
Synthetic Undecidability and Incompleteness of First-Order Axiom Systems in Coq.
In Cohen, L. and Kaliszyk, C., editors, *12th International Conference on Interactive Theorem Proving (ITP 2021)*, volume 193 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 23:1–23:20, Dagstuhl, Germany. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

Bibliography II

Makholm, H.
Tennenbaum's theorem without overspill.
Mathematics Stack Exchange.
(version: 2014-01-24).

McCarty, C. (1987).
Variations on a thesis: intuitionism and computability.
Notre Dame Journal of Formal Logic, 28(4):536–580.

McCarty, C. (1988).
Constructive validity is nonarithmetic.
The Journal of Symbolic Logic, 53(4):1036–1041.

Smith, P. (2013).
An introduction to Gödel's theorems.
Cambridge University Press.

Smith, P. (2014).
Tennenbaum's theorem.

Tennenbaum, S. (1959).
Non-archimedean models for arithmetic.
Notices of the American Mathematical Society, 6(270):44.

Variants of Tennenbaum

Both variants need a stronger version of inseparable formulas α, β. They are called HA-inseparable iff Σ_1 with $\mathsf{HA} \vdash_i \neg\exists x.\, \alpha(x) \wedge \beta(x)$. Given the existence of such formulas, we have:

Makholm (constructive)

Every enumerable and discrete $\mathcal{M} \vDash \mathsf{PA}$ has $\forall e{:}\mathcal{M}.\, \neg\neg\mathsf{std}\, e$. [Makholm,]

McCarty

Under a more constructive Tarski semantics, HA is categorical. [McCarty, 1987, McCarty, 1988]