Peano arithmetic - models and unprovability

Petr Glivický

Department of theoretical informatics and mathematical logic
Charles University in Prague

petrglivicky@gmail.com

Spring School of Algebra 2010

Content

1. The Goodstein theorem
2. The minimum from mathematical logic
3. The world of the finite mathematics
   - Axiomatization of $\mathbb{N}$
   - On the edge of the world
4. Proving unprovability
5. Models of PA and independent statements
   - Nonstandard models
   - Independent statements

The Goodstein theorem

Motivation example

Definition

The m-th Goodstein sequence is defined recursively:

- $G_m(1) = m$
- $G_m(n)$: *write* $G_m(n-1)$ *in hereditary base-n notation, change all ciphers n to* $n+1$ *and substract* 1.

Example

For m=19 we have $G_{19}(1) = 19$. *To compute* $G_{19}(2)$ *we write* $G_{19}(1) = 19$ *in hereditary base-2 notation:*

$$19 = 2^{2^2} + 2^1 + 1$$

change all 2s to 3s and substract one:

$$G_{19}(2) = 3^{3^3} + 3^1 + 1 - 1$$

Goodstein sequences start to grow very quickly:

Example

$2^{2^2}+2+1$	19
$3^{3^3}+3$	$7,625,597,484,990$
$4^{4^4}+3$	$\approx 1.3\cdot 10^{154}$
$5^{5^5}+2$	$\approx 1.8\cdot 10^{2184}$
$6^{6^6}+1$	$\approx 2.6\cdot 10^{36,305}$
7^{7^7}	$\approx 3.8\cdot 10^{695,974}$
$7\cdot 8^{(7\cdot 8^7+7\cdot 8^6+7\cdot 8^5+7\cdot 8^4+7\cdot 8^3+7\cdot 8^2+7\cdot 8+7)}+$ $+7\cdot 8^{(7\cdot 8^7+7\cdot 8^6+7\cdot 8^5+7\cdot 8^4+7\cdot 8^3+7\cdot 8^2+7\cdot 8+6)}+\ldots$ $+7\cdot 8^{(8+2)}+7\cdot 8^{(8+1)}+7\cdot 8^8$ $+7\cdot 8^7+7\cdot 8^6+7\cdot 8^5+7\cdot 8^4$ $+7\cdot 8^3+7\cdot 8^2+7\cdot 8+7$	$\approx 6\times 10^{15,151,335}$

Theorem (Goodstein)

Each Goodstein sequence eventually hits 0, i.e. $(\forall m)(\exists n)G_m(n) = 0$.

Definition

Goodstein function $\mathcal{G}$ *is defined as follows:*
$\mathcal{G}(m) := min\{n; G_m(n) = 0\}$.

$\mathcal{G}$ grows rapidly:
$\mathcal{G}(3) = 6$
$\mathcal{G}(4) = 3 \cdot 2^{402653211} - 2$
$\mathcal{G}(5)$ can't be expressed without a special notation
$\mathcal{G}(12) >$ Graham's number

Idea of proof of Goodstein theorem:
In hereditary n-base expansion of $G_m(n)$ replace all ciphers n by ordinal ω. The result denote $\Omega_m(n)$.

Example

$2^{2^2}+2+1$	$\omega^{\omega^\omega}+\omega+1$
$3^{3^3}+3$	$\omega^{\omega^\omega}+\omega$
$4^{4^4}+3$	$\omega^{\omega^\omega}+3$
$5^{5^5}+2$	$\omega^{\omega^\omega}+2$
$6^{6^6}+1$	$\omega^{\omega^\omega}+1$
7^{7^7}	ω^{ω^ω}
...	$7\cdot\omega^{(7\cdot\omega^7+7\cdot\omega^6+7\cdot\omega^5+7\cdot\omega^4+7\cdot\omega^3+7\cdot\omega^2+7\cdot\omega+7)}+$ $+7\cdot\omega^{(7\cdot\omega^7+7\cdot\omega^6+7\cdot\omega^5+7\cdot\omega^4+7\cdot\omega^3+7\cdot\omega^2+7\cdot\omega+6)}+\ldots$ $+7\cdot\omega^3+7\cdot\omega^2+7\cdot\omega+7$

The sequence $\Omega_m(n)$ is strictly decreasing sequence of ordinals and $\Omega_m(n)\geq G_m(n)$. Hence $G_m(n)$ must in finitely many steps hit 0.

Goodstein theorem is a statement about natural numbers. But to prove it we used infinite ordinals.

Question

Can we prove Goodstein theorem without refering to infinity?

The minimum from mathematical logic

Structures and theories

There are two basic concepts in mathematical logic:

Structures:
$\mathcal{S} = \langle S, \mathcal{R}, \mathcal{F} \rangle$
Formulas are true/false in $\mathcal{S}$.
$\mathcal{S} \models \varphi$

Theories:
T is set of formulas (axioms of T).
Formulas are provable/unprovable in T.
$T \vdash \varphi$

Definition

Structure $\mathcal{S}$ is a model of a theory T if every axiom of T is true in $\mathcal{S}$.

Definition

Theory T is axiomatization of a structure $\mathcal{S}$ if any statement φ is true in $\mathcal{S}$ if and only if it is provable in T.

The world of the finite mathematics

Natural questions about natural numbers

Question

What is the most importent structure in the mathematics?
Answer: $\mathbb{N}= \langle \mathbb{N}, 0, S, +, \cdot, \leq \rangle$

Question

Can we axiomatize $\mathbb{N}$? More precisely can we effectively (= recursively) write down the list of axioms for $\mathbb{N}$?
Answer: *No.*

Theorem

Let T be recursively axiomatized extension of Robinson arithmetic, then T is incomplete.

The world of the finite mathematics

Robinson arithmetic

Question

Can we construct at least some axiomatic system which is good enough, i.e. proves most of important statements which are true in $\mathbb{N}$?

First attempt: Robinson arithmetic (Q)

Definition

Robinson arithmetic (Q) is the theory with axioms:

$$Sx \neq 0 \qquad x + 0 = x$$
$$0 \neq x \to (\exists y)(x = Sy) \qquad x + Sy = S(x + y)$$
$$Sx = Sy \to x = y \qquad x \cdot 0 = 0$$
$$x \leq y \leftrightarrow (\exists z)(z + x = y) \qquad x \cdot Sy = x \cdot y + x$$

Q doesn't prove even basic properties of $+$, $\cdot$ and $\leq$ which are true in $\mathbb{N}$ (associativity, comutativity or linearity).

The world of the finite mathematics

Peano arithmetic

Second attempt: Peano arithmetic (PA)

Definition

Peano arithmetic (PA) consists of all axioms of Q and from infinitely many instances of the induction scheme (one for each formula φ):

$$I_\varphi: \quad \varphi(0) \,\&\, (\forall y)(\varphi(y) \to \varphi(Sy)) \to (\forall x)\varphi(x)$$

Quiet succesfull: we hardly find φ such that $\mathbb{N} \models \varphi$ and $\mathrm{PA} \nvdash \varphi$.
PA is really strong theory: it is another presentation of finite set theory. PA is the **world of the finite mathematics**.

Theorem

PA is equiinterpretable with ZF_{fin}. Inside PA one can define predicates Set and $\in$ such that all axioms of ZF_{fin} relativised to the domain Set are provable in PA.

Remark

For the additive structure of natural numbers $\langle \mathbb{N}, 0, S, +, \leq \rangle$ *we can find an axiomatization - Presburger arithmetic* (Pr).

The world of the finite mathematics

On the edge of the world

We have already seen that there must be statements true in $\mathbb{N}$ which are unprovable in PA, i.e. $\mathcal{S} := \mathrm{Th}(\mathbb{N}) \setminus \mathrm{Thm}(\mathrm{PA}) \neq \emptyset$.

Formulas from $\mathcal{S}$ are exactly the statements about natural numbers which can't be proven without refering to the infinity.

Question

Does Goodstein theorem belong to $\mathcal{S}$? Are there any (other) interesting statements which do? What about Fermats Last Theorem (FLT) or the Twin Prime Conjecture (TPC)?

In order to verify that $\mathrm{GT} \in \mathcal{S}$ we have to prove it is unprovable in PA.

Proving unprovability

Provability, consistence and independence

Definition

Let φ be a formula and T a theory:

- *φ is unprovable in T ($T \nvdash \varphi$) if there is no proof of φ in T.*
- *φ is consistent with T if $\neg\varphi$ is unprovable in T.*
- *φ is independent in T if both φ and $\neg\varphi$ are unprovable in T.*

Example

- *The commutativity law is independent in the group theory, it's not independent but consistent in the theory of abelian groups.*
- *Continuum hypothesis or axiom of choice are independent in Zermelo-Fraenkel set theory.*
- *Euclids fifth postulate is independent in the geometrical theory given by the first four Euclids postulates.*

Proving unprovability

Question

How can we prove that some statement φ is unprovable in a theory T?

Answer: We have to construct model $\mathcal{M}$ of T such that $\mathcal{M} \models \neg\varphi$.

Example

- *To prove that commutativity doesn't follow from group axioms it suffices to find any nonabelian group.*
- *Hyperbolic geometry witnesses that Euclids fifth postulate isn't provable from first four postulates.*

Models of PA

Nonstandard models and their properties

We know that $\mathbb{N}$ is model of PA. It is called standard model.

Proposition

There are another models of PA than $\mathbb{N}$. These models are called nonstandard models.

We will consider only countable models of PA (there are 2^{ω} many mutualy nonisomorphic). Let $\mathcal{M}$ be arbitrary countable nonstandard model of PA.

Proposition

- *The smallest substructure of $\mathcal{M}$ is $\mathbb{N}$.*
- *$\mathbb{N}$ isn't definable in $\mathcal{M}$.*
- *The order type of $\mathcal{M}$ is $\mathbb{N} + \mathbb{Q} \cdot \mathbb{Z}$.*

$\mathbb{N}$ isn't the only initial segment of $\mathcal{M}$ which is itself model of PA.

Theorem

There are 2^{ω} many initial segments of $\mathcal{M}$ which are themselves models of PA. They are called peano cuts of $\mathcal{M}$.

The order in $\mathcal{M}$ is very simple. Addition and multiplication are much more complicated.

Theorem (Tennenbaum 1959)

Operations $+$ and $\cdot$ in any countable nonstandard model $\mathcal{M}$ of PA are nonrecursive.

Models of PA are very difficult to construct.
Reasons:

- $\mathrm{PA} \approx \mathrm{ZF}_{fin}$
- They can't be constructed ($+$ and $\cdot$ can't be given effectively)

Question

Can we „construct" models of PA which will witness about unprovability of some interesting statements? For instance Goodstein theorem, FLT and TPC?

Independent statements in PA

Logical and combinatorical statements

First class of PA-independent statements: „Logical“ statements
Gödel formula $\nu =$„I'm unprovable in PA“ or $Con_{\mathrm{PA}} =$ „PA is consistent“ - they are true in $\mathbb{N}$ but unprovable in PA.
Independence was proven by Kurt Gödel in his famous Gödel's incompleteness theorems.

These independent statements are senseless from arithmetical point of view (they tell us no interesting information about natural numbers).

Question

Are there any more meaningful independent statements?

Second class of PA-independent statements: Combinatorial statements

Strengthened finite Ramsey theorem: $(\forall x, c, d, e)(\exists y)[x, y] \overset{*}{\to} (e)^d_c$.

where the $\overset{*}{\to}$ notation above means: for every coloring of the set of d-element subsets of $[x, y]$ by c colors there is at least e-element subset $H \subset [x, y]$ relatively large ($|H| > min(H)$) which is homogenous for the coloring (all d-element subsets of H have the same color).

Proved by Paris and Harington.The proof uses cuts and technology of detectors and the extreme speed of the growth of the function $\mathcal{R}(x, c, d, e) := min\{y; [x, y] \overset{*}{\to} (e)^d_c\}$.

Independent statements in PA

Goodstein theorem and Hercules and hydra

Third class of PA-independent statements: Structure killing

Goodstein theorem:

Theorem (Kirby, Paris 1982)

$\mathrm{PA} \nvdash (\forall m)(\exists n) G_m(n) = 0.$

Idea of the proof: Cut the nonstandard model of PA between $\mathcal{G}(m)$ and $\mathcal{G}(m+1)$, then $G_{m+1}(n)$ will never hit 0. This can be done because the gap between $\mathcal{G}(m)$ and $\mathcal{G}(m+1)$ is huge.

Hercules and hydra:

Theorem (Kirby, Paris 1982)

1. *Every Herculeses strategy kills the hydra in finitely many steps.*
2. $\mathrm{PA} \nvdash$ *„Every Herculeses recursive strategy kills hydra in finitely many steps.“*

No other statements are known to be unprovable in PA.

There is no fruitful method of model construction for PA (like forcing in *ZFC*).

Question

Can we say at least something about provability of FLT or TPC?

Independent statements in PA

FLT and TPC

Theorem (Mlček 1976)

TPC is independent in the weak arithmetic Ar+ „primes are unbounded“.

Ar extends Robinson's arithmetic by axioms for associativity, commutativity and other nice properties of $+$, $\cdot$ and $\leq$. It also contains induction scheme for all additive formulas (extends Presburger arithmetic).

Theorem (Glivický, Wiles 2007) :-)

FLT is true in $\mathbb{N}$ *but unprovable in Exp*$(\mathbb{N})$.

Here *Exp*$(\mathbb{N})$ is extension of *Th*$(\mathbb{N})$ by axiomatic definition of exponentiation.

Thanks

Thank you for your attention.