Goodstein Sequences, Fast Growing Functions and Arithmetical Independence Results

Stanley S. Wainer
(University of Leeds, UK)

Goodstein Centenary Meeting, Leicester, Dec. 2012
Math Kolloquium Munich, February 2013

First Order Theories – Metamathematics

Mathematics today consists of many different branches or "axiomatized theories", such as Number Theory, Group Theory, or even Set Theory (designed as a foundation for "all" mathematics).

Gödel's Completeness Theorem (1930) means that, once the axioms are written down, the rules of logic will then generate all logically valid (first order) consequences of them. Thus a "formalized theory" T is a precisely defined system or "machine":

Axioms of T	+	Logic

for churning out theorems about T.

Metamathematics is the mathematics of such theories T.

Hilbert's programme – first prove T consistent? – is it complete?

Peano Arithmetic

Number theory is fundamental to all of mathematics. The formalized theory is usually called Peano Arithmetic (PA). Its language is based on the symbols $=, 0, 1, +, \cdot$ and consists of all formulas built up from these by applying the logical connectives $\neg, \vee, \wedge, \rightarrow$ and quantifiers $\exists, \forall$. Its deceptively simple axioms are:

Peano Axioms

$x + 1 \neq 0$; $x + 0 = x$; $x + (y + 1) = (x + y) + 1$;
$x \cdot 0 = 0$; $x \cdot (y + 1) = (x \cdot y) + x$.

Induction

$$A(0) \wedge \forall x(A(x) \rightarrow A(x + 1)) \rightarrow \forall x A(x).$$

All the basic results (and more!) of number theory can be developed in PA. Of particular interest is Fermat's Last Theorem:

$$\forall n \, \forall x \, \forall y \, \forall z \, (n > 2 \rightarrow x^n + y^n \neq z^n).$$

Could Wiles' proof be carried out in PA? A. MacIntyre thinks so.

Gödel's Incompleteness Theorems

The underlying assumption here is that PA is consistent – it has a model which we believe in – don't we?

Theorem (Gödel's First Incompleteness Theorem (1931))

There is a true formula which cannot be proved in PA.

Proof.

By a revolutionary "arithmetization" ("digitization") of the syntax, he adapted the Liar Paradox to construct a formula G which self-referentially expresses "G is not provable".
Then G cannot be provable – otherwise it is and it's not! □

Theorem (Gödel's Second Incompleteness Theorem (1931))

The consistency of PA (impossibility of deriving a contradiction) is also expressible in the language of arithmetic, but cannot be proved in PA.

Gentzen (1936, 1943) It requires transfinite induction up to ε_0.

A Mathematical Incompleteness

Are there any genuine *mathematical* examples of incompleteness?

Goodstein Sequences (1944) – Kirby and Paris (1982)

- Take any number a, for example $a = 16$.
- Write a in "complete base-2", thus $a = 2^{2^2}$.
- Subtract 1, so the base-2 representation is $a - 1 = 2^{2+1} + 2^2 + 2^1 + 1$.
- Increase the base by 1, to produce the next stage $a_1 = 3^{3+1} + 3^3 + 3^1 + 1 = 112$.
- Continue subtracting 1 and increasing the base: $a, a_1, a_2, a_3, \ldots$. In the example: 16, 112, 1284, 18653, ...

Theorem (Part 1 – Goodstein, Part 2 – Kirby & Paris)

(1) Every Goodstein sequence eventually terminates in 0.
(2) But this is not provable in PA.

Some (small – exponential) Ordinals

Transfinite Ordinals provide a way of counting beyond the integers:

$$0, 1, 2, 3, 4, \ldots \omega, \omega + 1, \omega + 2, \ldots \omega \cdot 2$$

$$\omega \cdot 2 + 1, \omega \cdot 2 + 2, \ldots \omega \cdot 3, \ldots\ldots \omega^2$$

$$\omega^2 + 1, \omega^2 + 2, \ldots \omega^2 + \omega, \ldots\ldots \omega^2 \cdot 2$$

$$\ldots \omega^3, \ldots\ldots \omega^\omega, \ldots\ldots \omega^{\omega^\omega}, \ldots\ldots \omega^{\omega^{\omega^\omega}}, \ldots \varepsilon_0$$

If, throughout one of these ordinals α, we replace ω by n, then we obtain a "complete base-n" representation. Subtracting 1, and then putting the ω back, one gets a smaller ordinal $P_n(\alpha)$.

E.G. With $\alpha = \omega^{\omega^\omega}$ and $n = 2$ we get $a = 2^{2^2} = 16$.
Then $a - 1 = 2^{2+1} + 2^2 + 2^1 + 1$ and $P_n(\alpha) = \omega^{\omega+1} + \omega^\omega + \omega^1 + 1$.

The Fast Growing "Hardy" Functions

Definition

$$H_0(n) = n \quad \text{and} \quad H_\alpha(n) = H_{P_n(\alpha)}(n+1)\,.$$

Theorem (Cichon (1983))

The length of any Goodstein sequence starting with a to the complete base n is

$$H_\alpha(n) - n$$

where α is the result of replacing base n by ω in a.
$H_{\varepsilon_0}(n)$ bounds the lengths of all G-sequences (for large enough n).

Theorem (Kreisel (1951); Schwichtenberg, Wainer (1970-72))

The H_α-functions measure the computational complexity of PA.
So H_{ε_0} is not computable "within" PA.

Goodstein's Foresight

Thus we cannot compute the lengths of all G-sequences within PA.

So it cannot be proved in PA that "Every G-sequence terminates" .

Goodstein clearly saw this in 1944 – but couldn't complete a proof.

That required Kirby and Paris nearly 40 years later.

But Goodstein also showed that, even if one updates the base by an arbitrarily large function $n \mapsto g(n)$ at each stage, the sequences still terminate – and this fact is equivalent to the full principle of transfinite induction up to ε_0. He was aware of Gentzen's work, so must have been very close to the independence result.

Nowadays research on "Mathematical Independence Results" – for a whole range of foundational theories beyond PA – is an industry.

Proof – Embedding PA into PA$^\infty$

First, unravel each PA-induction into an ω-sequence of Cuts: $A(0) \to A(1) \to A(2) \to \cdots \to A(k) \to \cdots$ in PA$^\infty$ with rules:

$$(\exists)\frac{n : N \vdash^{\beta} m : N \quad n : N \vdash^{\beta} A(m), \Gamma}{n : N \vdash^{\alpha} \exists x A(x), \Gamma}$$

$$(\forall)\frac{\{\max(n,k) : N \vdash^{\beta_k} A(k), \Gamma\}_{k \in N}}{n : N \vdash^{\alpha} \forall x A(x), \Gamma}$$

$$(Cut)\frac{n : N \vdash^{\beta} \neg C, \Gamma \quad n : N \vdash^{\beta} C, \Gamma}{n : N \vdash^{\alpha} \Gamma}$$

and computation rules: $n : N \vdash^{\alpha} m : N$ if $m \leq n + 1$ and

$$(C)\frac{n : N \vdash^{\beta} m : N \quad m : N \vdash^{\beta} \Gamma}{n : N \vdash^{\alpha} \Gamma}$$

where $\beta \prec_n \alpha$ and, in $(\forall)$, $\beta_k \prec_{\max(n,k)} \alpha$ for each $k \in N$.

Proof continued – Cut Elimination

- Suppose $C \equiv \exists x B(x)$ is a cut formula to be eliminated.
- Suppose the premises of such a Cut are $n : N \vdash^{\beta} \neg C, \Gamma$ and $n : N \vdash^{\beta} C, \Gamma$.
- Suppose the latter comes by $(\exists)$ from $n : N \vdash^{\gamma} m : N$ and $n : N \vdash^{\gamma} B(m), C, \Gamma$.
- Invert the former premise at m and apply (C) to get $n : N \vdash^{\beta} \neg B(m), \Gamma$.
- Use induction on γ to eliminate C from $n : N \vdash^{\gamma} B(m), C, \Gamma$. The cost is an increase in the ordinal bound, from γ to $\beta + \gamma$.
- From $n : N \vdash^{\beta} \neg B(m), \Gamma$ and $n : N \vdash^{\beta+\gamma} B(m), \Gamma$ obtain $n : N \vdash^{\beta+\beta} \Gamma$ by a "smaller" cut on $B(m)$.
- Therefore a doubling of the ordinal reduces all Cuts on C. Repeating this on all cut formulas of size $\|C\|$, one sees that cut-size is reduced by an exponential increase in the ordinal. Iterated exponents eliminate all cuts!

Proof continued – Bounding Σ_1 Formulas

- Suppose $\mathrm{PA} \vdash \exists x B(x, y)$ with height h and cut-size r.
- Embed into PA^∞: $n : N \vdash^{\omega \cdot h} \exists x B(x, n)$ for each $y := n$.
- Cut-Elim: $n : N \vdash^{\alpha} \exists x B(x, n)$ Cut-free, where $\alpha = \exp^r(\omega \cdot h) \prec \varepsilon_0$.
- Thus $n : N \vdash^{\alpha} m : N$ for some m with $n : N \vdash^{\alpha} B(m, n)$.
- But $\boxed{n : N \vdash^{\alpha} m : N \text{ if and only if } m \leq H_{2^\alpha}(n)}$
- That is, from input n a true witness m is computable, bounded by $H_{2^\alpha}(n)$.

Calibrating Proof-Theoretic Strength

Proof-theoretic analysis, begun by Gentzen (1936), is now a highly sophisticated technical field, measuring "strength" of theories.
In each case an ordinal is computed, and the H_α hierarchy below that ordinal measures the theory's computational complexity.
Thus foundationally important theories are calibrated up the ordinal scale, according to the principles assumed, and the H_α's give connections to independence results (..) in each case.
For example:

- Ordinal $= \psi(\Omega_\omega)$. Π^1_1-Comprehension. (Kruskal+Labels).
- Ordinal $= \psi(\varepsilon_{\Omega+1})$. Non-iterated Inductive Definitions.
- Ordinal $= \Gamma_0$. Predicative Analysis. (Kruskal's Theorem).
- Ordinal $= \varepsilon_0$. PA. (Modified Finite Ramsey Theorem).
- Ordinal $= \omega^3$. IΔ_0(exp). (Finite Ramsey Theorem).

Bounding Functions for $\mathrm{ID}_{<\omega} = \bigcup_i \mathrm{ID}_i$ and Π^1_1-CA_0

Define $\varphi^{(k)} : \Omega_{k+1} \times \Omega_k \to \Omega_k$ by:

$$\varphi^{(k)}_\alpha(\beta) = \begin{cases} \beta + 1 & \text{if } \alpha = 0 \\ \varphi^{(k)}_\gamma \circ \varphi^{(k)}_\gamma(\beta) & \text{if } \alpha = \gamma + 1 \\ \varphi^{(k)}_{\alpha_\beta}(\beta) & \text{if } \alpha = \sup \alpha_\xi \ (\xi \in \Omega_k) \\ \sup \varphi^{(k)}_{\alpha_\xi}(\beta) & \text{if } \alpha = \sup \alpha_\xi \ (\xi \in \Omega_{<k}) \end{cases}$$

Denote $\varphi^{(0)}_\alpha$ as B_α, so $B_\alpha = H_{2^\alpha}$.

Define $\tau = \sup \tau_i$ where $\tau_0 = \omega$ and

$$\tau_1 = \varphi^{(1)}_\omega(\omega) \ , \ \tau_2 = \varphi^{(1)}_{\varphi^{(2)}_\omega(\omega_1)}(\omega) \ , \ \tau_3 = \varphi^{(1)}_{\varphi^{(2)}_{\varphi^{(3)}_\omega(\omega_2)}(\omega_1)}(\omega) \ , \ \ldots$$

Theorem

The proof-theoretic ordinal of ID_i is τ_{i+2}. The provably computable functions of Π^1_1-CA_0 are those computably-bounded by $\{B_\alpha\}_{\alpha \prec \tau}$.

Links to Independence Results

Theorem (Friedman's Miniaturized Kruskal Theorem for Labelled Trees)

For each constant c there is a number $K(c)$ so large that in every sequence $\{T_j\}_{j<K(c)}$ of finite trees with labels from a given finite set, and such that $|T_j| \leq c \cdot 2^j$, there are $j_1 < j_2$ such that $T_{j_1} \hookrightarrow T_{j_2}$. The embedding must preserve infs, labels, and satisfy a certain "gap condition".

Lemma

The (natural) computation sequence for $B_{\tau_i}(n)$ satisfies the size-bound above, and is a "bad" sequence, i.e. no embeddings.

Corollary

For a simple c_n we therefore have $B_\tau(n) = B_{\tau_n}(n) < K(c_n)$ for all n. Therefore K is not provably recursive in $ID_{<\omega}$, nor in Π^1_1-CA_0.

The Computation Sequence for τ_n

By reducing/rewriting τ_n according to the defining equations of the φ-functions, we pass through all the ordinals $\prec_n \tau_n$. Each term is a binary tree with labels $\leq n$, and each one-step-reduction at most doubles the size of the tree. E.g. with $n = 2$ the sequence begins:

$$\tau_2 \to \varphi^{(1)}_{\varphi^{(2)}_2(\omega_1)}(\omega) \to \varphi^{(1)}_{\varphi^{(2)}_1\varphi^{(2)}_1(\omega_1)}(\omega) \to \varphi^{(1)}_{\varphi^{(2)}_0\varphi^{(2)}_0\varphi^{(2)}_1(\omega_1)}(\omega) \to$$

$$\varphi^{(1)}_{\varphi^{(2)}_0\varphi^{(2)}_1(\omega_1)}(\varphi^{(1)}_{\varphi^{(2)}_0\varphi^{(2)}_1(\omega_1)}(\omega)) \to \varphi^{(1)}_{\varphi^{(2)}_1(\omega_1)}(\varphi^{(1)}_{\varphi^{(2)}_1(\omega_1)}(\varphi^{(1)}_{\varphi^{(2)}_0\varphi^{(2)}_1(\omega_1)}(\omega)))$$

$$\to \varphi^{(1)}_{\omega_1}\varphi^{(1)}_{\omega_1}\varphi^{(1)}_{\varphi^{(2)}_0(\omega_1)}\varphi^{(1)}_{\varphi^{(2)}_1(\omega_1)}\varphi^{(1)}_{\varphi^{(2)}_0\varphi^{(2)}_1(\omega_1)}(\omega) \to \varphi^{(1)}_{\varphi^{(1)}_{\omega_1}(-)}(\varphi^{(1)}_{\omega_1}(-))\ldots$$

The length of the entire sequence (down to zero) is therefore $\geq B_{\tau_{n-1}}(n)$. Furthermore, the sequence is bad - no term is gap-embeddable in any follower. Therefore for all n, $B_{\tau_{n-1}}(n) < K(c_n)$ and so K is not provably recursive in Π^1_1-CA$_0$.

References

R.L. Goodstein: "On the restricted ordinal theorem", Journal of Symbolic Logic 9 (1944) pp. 33–41.

L.A. Kirby and J.B. Paris: "Accessible independence results for Peano arithmetic", Bulletin of the London Mathematical Society 14 (1982) pp. 285–293.

E.A. Cichon: "A short proof of two recently discovered independence results using recursion theoretic methods", Proceedings of the American Mathematical Society 87 (1983) pp. 704–706.

W. Buchholz and S.S. Wainer: "Provably computable functions and the fast growing hierarchy", in S.G. Simpson (Ed) Logic and Combinatorics, AMS Contemporary Mathematics vol. 65 (1987) pp. 179–198.

H. Schwichtenberg and S.S. Wainer: "Proofs and Computations", ASL Perspectives in Logic, CUP (2012).