Can Peano Arithmetic Prove Randomness?

Cristian S. Calude

Joint work with Nicholas J. Hay (first part) and

Nicholas J. Hay & Frank C. Stephan (second part)

TCS: From Foundation to Application, Niš, November 2009

Introduction

- Peano Arithmetic
- PA provability
- Can finite random strings be certified by PA proofs?
- Can random c.e. reals be certified by PA proofs?
- Formal proof with Isabelle
- Provability of ε–randomness

Peano Arithmetic

Peano Arithmetic (PA) is the first-order theory for arithmetic whose non-logical symbols consist of the constant symbols 0 and 1, the binary relation symbol $<$ and the two binary function symbols $+$ (addition) and $\cdot$ (multiplication).

PA has 15 axioms (defining discretely ordered rings) together with induction axioms for each formula $\varphi(x, \overline{y})$:

$$\forall \overline{y}(\varphi(0, \overline{y}) \wedge \forall x(\varphi(x, \overline{y}) \rightarrow \varphi(x+1, \overline{y})) \rightarrow \forall x(\varphi(x, \overline{y})).$$

In what follows we will assume that PA is sound.

A function $f : \mathbb{N} \to \mathbb{N}$ is *provably computable* if there exists a Σ_1-formula of PA $\varphi(x, y)$ such that:

1. $\{(n, m) \mid f(n) = m\} = \{(n, m) \mid \mathbf{N} \vDash \varphi(n, m)\}$,
2. $\mathrm{PA} \vdash \forall x \exists! y \varphi(x, y)$.

Theorem. *Every primitive recursive function is provably computable, but the converse is not true*.

Theorem. *There exist computable functions which are not provably computable.*

A prefix-free machine U is *universal* if for every prefix-free machine V there is a constant $c = c_{U,V}$ such that for all strings s, t, if $V(s) = t$, then $U(s') = t$ for some string s' of length $|s'| \leq |s| + c$.

The prefix-free machines can be canonically enumerated (V_i). Given an index i for a universal prefix-free machine, can PA prove that "U_i is universal"?

Theorem. *There exists a universal prefix-free machine that is provably universal.*

Theorem. *There exists a universal prefix-free machine that is not provably universal.*

If U is a universal prefix-free machine then

$$H_U(x) = \min\{|y| \mid U(y) = x\}$$

is the prefix-complexity of the string x.

A string x is m-*random for* U if $H_U(x) \geq |x| - m$; x is *random for* U if $H_U(x) \geq |x|$.

A simple combinatorial argument shows the existence of random strings of any length.

Theorem [Chaitin 1975]. *For every universal prefix-free machine U there is a constant $c = c_{\mathrm{PA},U} > 0$ such that PA cannot prove any statement "$H_U(x) > m$" with $m > c$.*

Corollary. *There exists a universal prefix-free machine U_0 such that PA cannot prove that a string of positive length is random for U_0.*

A real $\alpha \in (0,1)$ is *random for* U if there exists a constant c such that for all $n \geq 1$, $H_U(\alpha_1 \cdots \alpha_n) \geq n - c$, where $\alpha_1 \cdots \alpha_n \cdots$ is the unending binary expansion of α.

A computable enumerable (c.e.) real is a limit of a computable increasing sequence of rationals.

Solovay's question

Is there some representation *of a random and c.e. real* α *for which* PA *can* prove *that* α *is random and c.e.?*

For every universal prefix-free machine U let

$$\Omega_U = \sum_{U(x)<\infty} 2^{-|x|}.$$

Theorem [Chaitin 1975; Calude, Hertling, Khoussainov, Wang 1998; Kučera, Slaman 2001]. *The set of all random and c.e. reals coincides with the set of all Ω_U when U is a universal prefix-free machine.*

Candidate: Can we represent a random and c.e. real by Ω_U, where U is a provably universal prefix-free machine?

Problem: Not every universal prefix-free machine is provably universal prefix-free!

Any hope?

Theorem. *Let V be a universal prefix-free machine. If α is random and c.e. then there exists an integer $c > 0$ and a c.e. real $\gamma > 0$ such that*

$$\alpha = 2^{-c} \cdot \Omega_V + \gamma.$$

The **representation** is:

$$2^{-c} \cdot \Omega_V + \gamma,$$

where V is a fixed provably universal prefix-free machine, $c > 0$ is a natural number and $\gamma > 0$ is a c.e. real.

Theorem. *Every c.e. and random real is provably random and c.e.*

Does the representation Ω_U, where U is a provably universal prefix-free machine, work too?

Theorem. *For every universal prefix-free machine U there exists a provably universal prefix-free machine U' such that $\Omega_U = \Omega_{U'}$.*

Corollary. *Every c.e. and random real can be written as the halting probability of a provably universal prefix-free machine.*

A negative result

Does there exist a universal machine whose halting probability is not provable random?

Theorem. *There exists a universal prefix-free machine U such that PA cannot prove the randomness of Ω_U solely based on U.*

Formal proof with Isabelle

We used Isabelle to obtain an automatic proof of a version of the Kraft-Chaitin Theorem, one of the key results used in the proof.

During the work to automate the proof of the Kraft-Chaitin Theorem a mistake in our human-made argument was unearthed and corrected.

We also used the experience with Isabelle to test the adequacy of the representation of a c.e. random real to obtain the PA proof of randomness.

We are completing the full formal proof...

Let $\varepsilon \in (0, 1]$ be computable and let U be a universal prefix-free machine. Following Tadaki, a real $\alpha \in (0, 1)$ is ε–*random* if there exists a constant c such that for all $n \geq 1$,

$$H_U(\alpha_1 \cdots \alpha_n) \geq \varepsilon \cdot n - c.$$

A prefix-free machine U is ε–*universal* if for every prefix-free machine T there exists a constant $c_{U,T}$ such that for each program σ there exists a program p such that

$$U(p) = T(\sigma) \text{ and } \varepsilon \cdot |p| \leq |\sigma| + c_{U,T}.$$

Provability of ε–randomness 2

Theorem. *A c.e. real α is ε–random* iff $\alpha = \Omega_U$, for some ε–universal prefix-free machine U.

Theorem. *Every c.e. and ε–random real is provably ε–random and c.e.*

Thank you!

Selected references

1. C. S. Calude, N. J. Hay. Every computably enumerable random real is provably computably enumerable random, *Logic Journal of the IGPL* June, 2009, 24 pp, doi:10.1093/jigpal/jzp015.
2. C. S. Calude, N. J. Hay, F. C. Stephan. Representation of Left-Computable ε–Random Reals, *CDMTCS Research Report* 365, 2009, 11 pp.
3. C. S. Calude, P. Hertling, B. Khoussainov, and Y. Wang. Recursively enumerable reals and Chaitin Ω numbers, in: M. Morvan, C. Meinel, D. Krob (eds.), *Proc. 15th STACS (Paris)*, Springer–Verlag, Berlin, 1998, 596–606.
4. G. J. Chaitin. A theory of program size formally identical to information theory, *J. Assoc. Comput. Mach.* 22 (1975), 329–340.
5. A. Kučera, T. A. Slaman. Randomness and recursive enumerability, *SIAM J. Comput.* 31, 1 (2001), 199-211.