Can Randomness Be Certified by Proof?

Cristian S. Calude   Nicholas J. Hay

University of Auckland

NKS 2008 Midwest Conference 2008

- Peano Arithmetic

Introduction

- Peano Arithmetic
- PA provability

- Peano Arithmetic
- PA provability
- Can finite random strings be certified by PA proofs?

Introduction

- Peano Arithmetic
- PA provability
- Can finite random strings be certified by PA proofs?
- Can random c.e. reals be certified by PA proofs?

- Peano Arithmetic
- PA provability
- Can finite random strings be certified by PA proofs?
- Can random c.e. reals be certified by PA proofs?
- Final remarks

- Peano Arithmetic
- PA provability
- Can finite random strings be certified by PA proofs?
- Can random c.e. reals be certified by PA proofs?
- Final remarks
- Selected references

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).

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 $\varphi(x, \overline{y})$:

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

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 $\varphi(x, \overline{y})$:

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

In what follows we will assume that PA is sound.

A partial function from $\mathbb{N}$ to $\mathbb{N}$ is partially computable iff its graph is equivalent to a Σ_1 formula of PA.

A partial function from $\mathbb{N}$ to $\mathbb{N}$ is partially computable iff its graph is equivalent to a Σ_1 formula of PA.

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

A partial function from $\mathbb{N}$ to $\mathbb{N}$ is partially computable iff its graph is equivalent to a Σ_1 formula of PA.

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

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

A partial function from $\mathbb{N}$ to $\mathbb{N}$ is partially computable iff its graph is equivalent to a Σ_1 formula of PA.

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. $\{(n, m) \mid f(n) = m\} = \{(n, m) \mid \mathbf{N} \models \varphi(n, m)\}$,
2. 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 $|s'| \leq |s| + c$.

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"?

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.*

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.

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 $H_U(x) \geq |x|$.

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* $m > c$.

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. *For every universal prefix-free machine* U *and* $m \geq 0$*, there is a constant* $c = c_{\mathrm{PA},U,m} > 0$ *such that PA cannot prove that a string of length larger than* $m + c$ *is* m*-random for* U*.*

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. *For every universal prefix-free machine U and $m \geq 0$, there is a constant $c = c_{\mathrm{PA},U,m} > 0$ such that PA cannot prove that a string of length larger than $m + c$ is m-random for U.*

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 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.

In contrast with strings, randomness for reals does not depend on U.

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.

In contrast with strings, randomness for reals does not depend on U.

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.?*

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.?*

The key concept is **representation**.

For every a universal prefix-free machine U let

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

For every a 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 prefix-free universal machine.*

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

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

Problem: No every prefix-free universal machine is provably prefix-free universal machine!

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

Problem: No every prefix-free universal machine is provably prefix-free universal machine!

Still there is 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*

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

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*

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

Theorem. *Let* V *be provably universal prefix-free,* c *be a positive integer,* γ *a positive c.e. real. Then* $\alpha = 2^{-c}\Omega_V + \gamma$ *is provably random and c.e.*

The **representation** adopted is:

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

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

The **representation** adopted is:

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

where V is a fixed provably prefix-free universal 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 prefix-free universal machine, work too?

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

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

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

Theorem. *For every universal prefix-free machine U there exits 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.*

If PA receives an algorithm for a machine V, a proof that V is universal and prefix-free, a positive integer c, and a computable increasing sequence of rationals converging to a real $\gamma > 0$, then PA can prove that $\alpha = 2^{-c}\Omega_V + \gamma$ is random and c.e.

If PA receives an algorithm for a machine V, a proof that V is universal and prefix-free, a positive integer c, and a computable increasing sequence of rationals converging to a real $\gamma > 0$, then PA can prove that $\alpha = 2^{-c}\Omega_V + \gamma$ is random and c.e.

Similarly, if PA receives an algorithm for a machine U, a proof that U is universal and prefix-free, then it can prove that Ω_U is random and c.e.

We have chosen Isabelle to obtain an automatic proof of our version of the Kraft-Chaitin Theorem, one of the key results used in the proof. This includes a description of the formalisation (for Isabelle) of the Kraft-Chaitin Theorem and the description of the main steps of the automatic proof.

We have chosen Isabelle to obtain an automatic proof of our version of the Kraft-Chaitin Theorem, one of the key results used in the proof. This includes a description of the formalisation (for Isabelle) of the Kraft-Chaitin Theorem and the description of the main steps of the automatic 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 have chosen Isabelle to obtain an automatic proof of our version of the Kraft-Chaitin Theorem, one of the key results used in the proof. This includes a description of the formalisation (for Isabelle) of the Kraft-Chaitin Theorem and the description of the main steps of the automatic 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.

1. C. S. Calude, N. J. Hay. Every Computably Enumerable Random Real Is Provably Computably Enumerable Random, *CDMTCS Research Report* 328, 2008, 29 pp.
2. 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.
3. G. J. Chaitin. A theory of program size formally identical to information theory, *J. Assoc. Comput. Mach.* 22 (1975), 329–340.
4. A. Kučera, T. A. Slaman. Randomness and recursive enumerability, *SIAM J. Comput.* 31, 1 (2001), 199-211.