Incompleteness: A Personal Perspective

Cristian S. Calude

University of Auckland

Google, November 2008

What this talk is not about...

- **A full picture of incompleteness.**
- **A recently discovered fatal flaw invalidating incompleteness.**
- **A cure for incompleteness.**

1. Incompleteness
2. Are there interesting independent sentences?
3. What is the source of incompleteness?
4. How common is the incompleteness phenomenon?

Can mathematics be done exclusively by computer?

- **Can we write a program to check whether a mathematical proof is correct?**
- **Can we write a program to generate all mathematical theorems?**
- **Can we write a program to check whether a mathematical sentence is a theorem?**

The above questions "make sense" if we adopt a (formal, axiomatic) theory to express mathematical sentences and theorems.

Hilbert's 1930 radio address

We must not believe those, who today with philosophical bearing and deliberative tone prophesy the fall of culture and accept the *ignorabimus*. For us there is no *ignorabimus*, and in my opinion none whatever in natural science. In opposition to the foolish *ignorabimus* I offer our answer:
We must know,
We will know.

1930, days later, the shock: the incompleteness theorem

Every effectively generated formal theory including elementary arithmetic cannot be both consistent and complete.

In any consistent, effectively generated formal theory including elementary arithmetic there exists a sentence of arithmetic which is neither provable nor disprovable.

Two examples and a question

Peano Arithmetic, PA, is incomplete or inconsistent.

Zermelo–Fraenkel set theory with choice, ZFC, a system for the "whole mathematics", is incomplete or inconsistent.

What about automatic theorem provers, like Automath, Isabelle, NuPRL, ProofPower, ProverBox, SPARK?

What does incompleteness imply?

- **Arithmetic is incomplete, but elementary geometry is complete.**
- **Incompleteness is "incurable": each time a new true statement is added as an axiom, there are other true statements that still cannot be proved. Algorithmically or probabilistically adding infinitely many true statements would not solve the problem.**
- **Incompleteness is a serious challenge to Hilbert's program towards a universal mathematical formalism.**

What does incompleteness not imply?

- $1 + 1 = 3$.
- **There are no complete and consistent formal systems for arithmetic (take all true statements about the natural numbers to be axioms).**
- **The Bible is either incomplete or inconsistent.**
- **The Constitution is either incomplete or inconsistent.**

Three questions

- **Are there interesting/natural concrete independent sentences?**
- **What is the source of incompleteness?**
- **How common is the incompleteness phenomenon?**

Examples 1

[Gödel] **Every effectively generated formal theory including elementary arithmetic cannot prove its own consistency.**

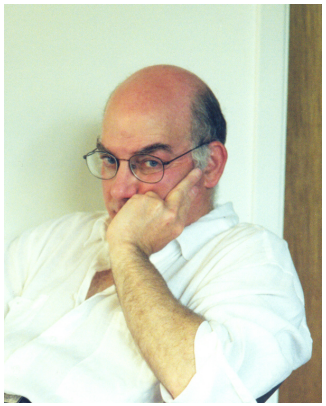
PA cannot prove its own consistency, but ZFC can prove PA consistency.

Examples 2

A universal prefix-free machine is a (Turing) machine with prefix-free domain capable of simulating any other prefix-free machine.

[CC-Hay] **There exists a universal (prefix-free) machine such that PA cannot prove its universality.**

Examples 3



The halting probability of a U is Chaitin's Omega number

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

[Chaitin] **ZFC (if arithmetically sound) can determine at most finitely many bits of Ω_U.**

Examples 4

[CC] **Consider a prefix-free machine U which PA proves universal. There is a universal prefix-free machine V such that**

- **PA proves universal,**
- $\Omega_U = \Omega_V$,
- **ZFC (if arithmetically sound) can determine at most the initial bits equal to 1 of Ω_V.**

Examples 5

[Solovay] **There exists a prefix-free universal machine U such that ZFC (if arithmetically sound) cannot determine any bit of Ω_U.**

All sentences about the values of Ω_U digits are unprovable in ZFC.

Proving complexity is hard

Define the prefix-complexity by $H(x) = \min\{|p| : U(p) = x\}$.

[Chaitin] **For every finitely specified consistent axiomatic theory there exists a constant c such that every provable sentence of the form "$H(x) > m$" has $m < c$.**

Chaitin's principle

[Chaitin's principle] ***The theorems of a finitely specified theory cannot be significantly more complex than the theory itself.***

[CC-Jürgensen] **Chaitin's principle is true for the complexity** $\delta(x) = H(x) - |x|$**.**

Independence abounds, theorems are scarce

[CC-Jürgensen-Zimand] **The set of true and unprovable sentences is topologically large.**

The set of true and unprovable sentences has positive probability.

Is incompleteness bad?

Mathematics needs creativity!

Selected references

1. **C. S. Calude. Incompleteness, complexity, randomness and beyond,** *Minds and Machines* **12, 4 (2002), 503–517.**
2. **C. S. Calude. Chaitin Ω numbers, Solovay machines and incompleteness,** *Theoret. Comput. Sci.* **284 (2002), 269–277.**
3. **C. S. Calude, N. J. Hay. Every Computably Enumerable Random Real Is Provably Computably Enumerable Random,** *CDMTCS Research Report* **328, 2008, 29 pp.**
4. **C. S. Calude, H. Jürgensen. Is complexity a source of incompleteness?** *Advances in Applied Mathematics* **35 (2005), 1–15.**
5. **C. Calude, H. Jürgensen, M. Zimand. Is independence an exception?** *Appl. Math. Comput.* **66 (1994), 63-76.**
6. **G. J. Chaitin. A theory of program size formally identical to information theory,** *J. Assoc. Comput. Mach.* **22 (1975), 329–340.**
7. **R. M. Solovay. A version of Ω for which** *ZFC* **can not predict a single bit, in C.S. Calude, G. Păun (eds.).** *Finite Versus Infinite. Contributions to an Eternal Dilemma*, **Springer-Verlag, London, 2000, 323-334.**