Axiom Bits and Proof Length: Short Review

C. S. Calude

December 23, 2025

Long proofs are an anathema to mathematicians.

1 Definitions

Definition 1 (Axiom bits)**.** *Let T be a recursively axiomatizable theory. An* axiom extension *of T is a theory*

$$T' = T + \alpha,$$

where α is a finite set of sentences, encoded as a finite binary string. The length of α is called the number of axiom bits.

Definition 2 (Proof length)**.** *For a fixed proof system P, let*

$$\ell_P(\varphi \mid T)$$

denote the length of the shortest P-proof of φ from axioms T.

2 Formal Speed-Up Theorems

Theorem 1 (Finite axiom extension yields non-recursive speed-up)**.** *Let T be a consistent, recursively axiomatizable theory extending Robinson arithmetic. Then there exists a* finite *axiom extension*

$$T' = T + \alpha$$

such that for infinitely many sentences φ_n:

1. *$\ell(\varphi_n \mid T)$ grows faster than any recursive function;*
2. *$\ell(\varphi_n \mid T') = O(n)$.*

In particular, the proof-length speed-up of T' over T is not recursively bounded.

Theorem 2 (Information-theoretic lower bound on proofs)**.** *For any proof system P and any theory T,*

$$\ell_P(\varphi \mid T) \;\geq\; K(\varphi \mid T) - O(1),$$

where $K(\cdot)$ denotes conditional Kolmogorov complexity.

Corollary 1. *Let $T' = T + \alpha$. A significant shortening of proofs of φ is possible only if*

$$K(\varphi \mid T + \alpha) \ll K(\varphi \mid T),$$

that is, only if the added axioms encode non-redundant information relevant to φ.

3 A Concrete Arithmetic Example

Proposition 1 (Consistency as axiom-bit compression)**.** *Let $T = \mathsf{PA}$ and let φ_n express the consistency of* PA *for proofs of length $\leq n$. Then:*

1. PA *proves each φ_n, but the shortest proofs grow faster than any primitive recursive function;*
2. *In the theory*
$$T' = \mathsf{PA} + \mathrm{Con}(\mathsf{PA}),$$
each φ_n has a proof of constant length.

4 Conclusion

Proofs are compressed representations of information. If a theory lacks the information encoding the obstruction to a theorem, proofs must reconstruct it, resulting in a large length. Adding axiom bits shortens proofs precisely when those bits encode the missing obstruction. The article [9] studies the "gap" between the length of a theorem and the smallest length of its proof in a given formal system.

References

[1] K. Gödel, "On the length of proofs," in *Collected Works, Vol. I*, Oxford University Press, 1986.

[2] G. Kreisel, "On the interpretation of non-finitist proofs," *Journal of Symbolic Logic*, vol. 16, pp. 241–267, 1951.

[3] S. Cook and R. Reckhow, "The relative efficiency of propositional proof systems," *Journal of Symbolic Logic*, vol. 44, no. 1, pp. 36–50, 1979.

[4] S. R. Buss, "On Gödel's theorems on lengths of proofs I: Number of lines and speedup for arithmetics," *Journal of Symbolic Logic*, vol. 59, no. 3, pp. 737–756, 1994.

[5] J. S. Royer, "Two recursion-theoretic characterizations of proof speed-ups," *Journal of Symbolic Logic*, vol. 54, no. 3, pp. 867–883, 1989.

[6] G. J. Chaitin, "A theory of program size formally identical to information theory," *Journal of the ACM*, vol. 22, no. 3, pp. 329–340, 1975.

[7] L. Bienvenu, A. Shen, and N. Vereshchagin, "The axiomatic power of Kolmogorov complexity," *Theory of Computing Systems*, vol. 52, pp. 1–38, 2013. (Explicitly studies proof compression via complexity axioms.)

[8] K. Gödel, "Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I," *Monatshefte für Mathematik und Physik*, vol. 38, pp. 173–198, 1931.

[9] C. S. Calude, L. Staiger, "Long and short proofs," "*Bull. Math. Soc. Sci. Math. Roumanie*," Tome 65 (113), No. 2, (2022), 203–211.