Extending Chaitin's Incompleteness Theorem

Samuel Epstein*

June 4, 2023

Abstract

Chaitin's incompleteness theorem states that sufficiently rich formal systems cannot prove lower bounds on Kolmogorov complexity. In this paper we extend this theorem by showing theories that prove the Kolmogorov complexity of a large (but finite) number of strings are inaccessible. This is done by first showing such theories have large information with the halting sequence. Then, by applying the independence postulate, such theories are shown to be inaccessible in the physical world.

1 Introduction

Gödel's famous incompleteness theorem states that any theory $\mathcal{F}$ that is consistent, recursively axiomatizable, and "sufficiently rich" (contains Robinson-arithmetic $\mathcal{Q}$, or $\mathcal{Q}$ can be interpreted in it) is incomplete, in that there exists true statements that cannot be proven in it.

It is well known that there is no recursive method to determine a non constant lower bound on Kolmogorov complexity, $\mathbf{K}$. Chaitin's incompleteness theorem proves there exist no logical means to prove lower bounds on $\mathbf{K}$. Let $\mathcal{F}$ be as above, and significantly strong to make assertions about the Kolmogorov complexity of strings. Furthermore, let $\mathcal{F}$ be sound. Then we get the celebrated theorem.

Theorem. (Chaitin's Incompleteness Theorem) *For theory $\mathcal{F}$, there is a constant c such that $\mathcal{F}$ does not prove $c < \mathbf{K}(x)$ for any x.*

The proof is straightforward. Assume otherwise. Take any c and enumerate proofs of $\mathcal{F}$ until it proves the statement $c < \mathbf{K}(x)$ for some x. Then return x. This implies that $\mathbf{K}(x) < O(\log c)$, causing a contradiction for large enough c.

However this theorem doesn't prohibit the existence of formal systems that prove $c < \mathbf{K}(x)$ for a finite but very large number of strings. Or for our purposes, the above theorem doesn't prohibit theories which prove $\mathbf{K}(x) = c$ for a large (but finite) number of strings. Such theories are not to be expected to be accessible by logicians. In this paper, we prove such systems are exotic, and cannot exist in the physical world. To do so we use two steps. The first step proves the following.

Theorem. *A relation $X \subset \{0,1\}^* \times \mathbb{N}$ of 2^n unique pairs $(b, \mathbf{K}(b))$ has $n <^{\log} \mathbf{I}(X; \mathcal{H})$.*

The term $\mathcal{H}$ is the halting sequence. The information term $\mathbf{I}$ is defined in Section 2. The second part involves invoking the Indepedence Postulate (**IP**), introduced in [Lev84, Lev13]. **IP** is an unprovable statement that physical sequences are independent from mathematical ones. Among other applications, **IP** can be interpreted as a finitary Church-Turing thesis. The statement is as follows.

*JP Theory Group. samepst@jptheorygroup.org

IP: *Let α be a sequence defined with an n-bit mathematical statement (e.g., in Peano Arithmetic), and a sequence β can be located in the physical world with a k-bit instruction set (e.g., ip-address). Then $\mathbf{I}(\alpha : \beta) < k + n + c$, for some small absolute constant c.*

We rework **IP** so that $x = \alpha \in \{0,1\}^*$, β is equal to the halting sequence $\mathcal{H}$, and the information term $\mathbf{I}$ is equal to $\mathbf{I}(\cdot;\mathcal{H})$, defined in Section 2. Since $\mathcal{H}$ can be described by an $O(1)$ bit mathematical sequence, we get

$$\mathbf{I}(x;\mathcal{H}) <^+ \mathbf{Address}(x).$$

Let $\mathcal{F}$ be a formal system defined in Chaitin's Incompleteness Theorem. Assume that $\mathcal{F}$ can be used to prove $\mathbf{K}(x_i) = c_i$ for 2^n unique strings x_i. Then by Theorem 1, Lemma 2, and **IP**,

$$n <^{\log} \mathbf{I}(\{(x_i, c_i)\};\mathcal{H}) <^{\log} \mathbf{I}(\mathcal{F};\mathcal{H}) <^{\log} \mathbf{Address}(\mathcal{F}).$$

Thus as the number strings with proved Kolmogorov complexities grows, the formal system $\mathcal{F}$ becomes exotic and by **IP**, inaccessible in the physical world. For related work, in [Lev13], it was shown that consistent completions of PA have infinite mutual information with $\mathcal{H}$ and thus have infinite addresses. This paper extends this result by proving the existence of theories with finite mutual information with the halting sequence. Note that Theorem 1 can be generalized to binary relations that approximate Kolmogorov complexity.

2 Conventions

For positive real functions f, by $<^+ f$, $>^+ f$, $=^+ f$, and $<^{\log} f$, $>^{\log} f$, $\sim f$ we denote $\leq f + O(1)$, $\geq f - O(1)$, $= f \pm O(1)$ and $\leq f + O(\log(f+1))$, $\geq f - O(\log(f+1))$, $= f \pm O(\log(f+1))$. $\mathbf{K}(x|y)$ is the conditional prefix Kolmogorov complexity. The chain rule states $\mathbf{K}(x,y) =^+ \mathbf{K}(x) + \mathbf{K}(y|\mathbf{K}(x), x)$. Let $[A] = 1$ if the mathematical statement A is true, otherwise $[A] = 0$. Let $\mathbf{K}_t(x|y) = \inf\{\|p\| : U_y(p) = x \text{ in } t \text{ steps}\}$. The information the halting sequence $\mathcal{H}$ has about x is $\mathbf{I}(x;\mathcal{H}|y) = \mathbf{K}(x|y) - \mathbf{K}(x|y,\mathcal{H})$. $\mathbf{I}(x;\mathcal{H}) = \mathbf{I}(x;\mathcal{H}|\emptyset)$. A probability measure is elementary if its support is finite and it has rational values. The deficiency of randomness of $x \in \{0,1\}^*$ with respect to elementary probability measure Q is $\mathbf{d}(X|Q) = \lceil -\log Q(X) - \mathbf{K}(x|\langle Q \rangle) \rceil$. The stochasticity of x is $\mathbf{Ks}(x) = \min_Q \mathbf{K}(Q) + 3\log\max\{\mathbf{d}(X|Q), 1\}$.

Lemma 1 **([Eps21, Lev16])** $\mathbf{Ks}(x) <^{\log} \mathbf{I}(x;\mathcal{H})$.

Lemma 2 **([Eps22])** *For partial computable f, $\mathbf{I}(f(x) : \mathcal{H}) <^+ \mathbf{I}(x;\mathcal{H}) + \mathbf{K}(f)$.*

3 Results

Let $\Omega = \sum\{2^{-\|p\|} : U(p) \text{ halts}\}$ be Chaitin's Omega, $\Omega_n \in \mathbb{Q}_{\geq 0}$ be be the rational formed from the first n bits of Ω, and $\Omega^t = \sum\{2^{-\|p\|} : U(p) \text{ halts in time } t\}$. For $n \in \mathbb{N}$, let $\mathbf{bb}(n) = \min\{t : \Omega_n < \Omega^t\}$. $\mathbf{bb}^{-1}(m) = \arg\min_n\{\mathbf{bb}(n-1) < m \leq \mathbf{bb}(n)\}$. Let $\Omega[n] \in \{0,1\}^*$ be the first n bits of Ω.

Lemma 3 *For $n = \mathbf{bb}^{-1}(m)$, $\mathbf{K}(\Omega[n]|m,n) = O(1)$.*

Proof. For a string x, let $BB(x) = \inf\{t : \Omega^t > 0.x\}$. Enumerate strings of length n, starting with 0^n, and return the first string x such that $BB(x) \geq m$. This string x is equal to $\Omega[n]$, otherwise let y be the largest common prefix of x and $\Omega[n]$. Thus $BB(y) = \mathbf{bb}(\|y\|) \geq BB(x) \geq m$, which means $\mathbf{bb}^{-1}(m) \leq \|y\| < n$, causing a contradiction. □

Theorem 1 *A relation $X \subset \{0,1\}^{*\infty} \times \mathbb{N}$ of 2^n unique pairs $(b, \mathbf{K}(b))$ has $n <^{\log} \mathbf{I}(X;\mathcal{H})$.*

Proof. We relativize the universal Turing machine to n. Let $X = \{x_i, c_i\}_{i=1}^{2^n}$, and $T = \min\{t : \mathbf{K}_t(x_i) = c_i = \mathbf{K}(x_i), \text{ for } i = 1, \ldots, n\}$. Let $N = \mathbf{bb}^{-1}(T)$ and $B = \mathbf{bb}(N)$. We relativize the universal Turing machine to B. Later on, we will make this relativization explicit. We also assume that $c_i > n$. If this is not the case, then one can construct $X' \subset X$ of size 2^{n-1} with $c_i > n-1$ and use X' instead.

Let $m(x) = 2^{-\mathbf{K}_B(x)}$. Let Q be an elementary probability measure that realizes $\mathbf{Ks}(X)$ and $d = \max\{\mathbf{d}(X|Q), 1\}$. Without loss of generality, the support of Q is restricted to finite binary relations $B \subset \{0,1\}^* \times \mathbb{N}$ of size 2^n. Let $B_1 = \bigcup\{y : (y,c) \in B\}$. Let $S = \bigcup\{B_1 : B \in \text{Support}(Q)\}$. We randomly select each string in S to be in a set R independently with probability $d2^{-n}$. Thus $\mathbf{E}[m(R)] \leq d2^{-n}$. For $B \in \text{Support}(Q)$,

$$\begin{aligned}
&\mathbf{E}_R\mathbf{E}_{B\sim Q}[[R \cap B_1 = \emptyset]] \\
=&\mathbf{E}_{B\sim Q} \Pr(R \cap B_1 = \emptyset) \\
=&(1 - d2^{-n})^{2^n} < e^{-d}.
\end{aligned}$$

Thus there exists a set $R \subseteq S$ such that $\mathbf{m}(R) \leq 2{\cdot}2^{-n}$ and $\mathbf{E}_{B\sim Q}[[R \cap B_1 = \emptyset]] < 2e^{-d}$. Let $t(B) = .5[R \cap B_1 = \emptyset]2^d$. t is a Q-test, with $\mathbf{E}_{B\sim Q}[t(B)] \leq 1$. It must be that $t(X) \neq 0$, otherwise,

$$1.44d - 1 < \log t(X) <^+ \mathbf{d}(X|Q) + \mathbf{K}(t|Q) <^+ d + \mathbf{K}(d),$$

which is a contradiction for large enough d, which one can assume without loss of generality. Thus $t(X) \neq 0$ and $R \cap X_1 \neq \emptyset$. Furthermore, if $y \in R$, $\mathbf{K}(y) <^+ -\log m(x) - n + \log d + \mathbf{K}(m, R)$. So for $x \in R \cap X_1$, making the relativization of B explicit.

$$\begin{aligned}
\mathbf{K}(x|B) &<^+ -\log m(x) - n + \log d + \mathbf{K}(m, R|B) \\
\mathbf{K}(x) - \mathbf{K}(B) &<^+ \mathbf{K}(x) - n + \log d + \mathbf{K}(S|B) \\
n &<^+ \mathbf{K}(B) + \log d + \mathbf{K}(d, Q|B) \\
n &<^+ \mathbf{K}(B) + \mathbf{Ks}(X|B) \\
n &<^{\log} \mathbf{K}(B) + \mathbf{I}(X;\mathcal{H}|B) \\
n &<^{\log} \mathbf{K}(B) + \mathbf{K}(X|B) - \mathbf{K}(X|\mathcal{H}) + O(\log N) \qquad (1)
\end{aligned}$$

Equation 1 is due to the fact that B is computable from $\Omega[N]$, thus it is computable from $\mathcal{H}$ and N. So we have,

$$\begin{aligned}
&\mathbf{K}(X|B) + \mathbf{K}(B) \\
<^+&\mathbf{K}(X|B, \mathbf{K}(B)) + \mathbf{K}(\mathbf{K}(B)|B) + \mathbf{K}(B) \\
<^+&\mathbf{K}(X, B) + \mathbf{K}(\mathbf{K}(B)|B) \qquad (2) \\
<^+&\mathbf{K}(X, N, B) + O(\log N) \qquad (3) \\
<^+&\mathbf{K}(X, N) + O(\log N). \qquad (4) \\
<^+&\mathbf{K}(X) + O(\log N). \\
n <^{\log}&\mathbf{K}(X) - \mathbf{K}(X|\mathcal{H}) + O(\log N). \qquad (5)
\end{aligned}$$

Equation 2 is from the chain rule. Equation 3 is from the fact that $M = \mathbf{bb}(N)$. Equation 4 comes from $\mathbf{K}(T|X) = O(1)$ and Lemma 3, which implies $\mathbf{K}(B|N,T) <^+ \mathbf{K}(\Omega[N]|N,T) <^+ O(1)$.

From X, one can compute T, where $\mathbf{bb}^{-1}(T) = N$. Therefore by Lemma 3, $\mathbf{K}(\Omega[N]|X) <^{+} \mathbf{K}(N)$, so by Lemma 2,

$$N <^{\log} \mathbf{I}(\Omega[N]; \mathcal{H}) <^{\log} \mathbf{I}(X; \mathcal{H}) + \mathbf{K}(N) <^{\log} \mathbf{I}(X; \mathcal{H}). \tag{6}$$

The above equation used the common fact that the first n bits of Ω had $n - O(\log n)$ bits of mutual information with $\mathcal{H}$. So combining Equations 5 and 6, we get

$$n <^{\log} \mathbf{I}(X; \mathcal{H}).$$

□

References

[Eps21] Samuel Epstein. All sampling methods produce outliers. *IEEE Transactions on Information Theory*, 67(11):7568–7578, 2021.

[Eps22] S. Epstein. 22 Examples of Solution Compression via Derandomization. *CoRR*, abs/2208.11562, 2022.

[Lev84] L. A. Levin. Randomness conservation inequalities; information and independence in mathematical theories. *Information and Control*, 61(1):15–37, 1984.

[Lev13] L. A. Levin. Forbidden information. *J. ACM*, 60(2), 2013.

[Lev16] L. A. Levin. Occam bound on lowest complexity of elements. *Annals of Pure and Applied Logic*, 167(10):897–900, 2016.