How (not) to Compute the Halting Probability or Validate the Heuristic Principle

Saeed Salehi

April 2024

Gregory John Chaitin

Born: 1947$_{77}$ (Jewish)

Argentine-American

Algorithmic Information Theory

A. Kolmogorov & R. Solomonoff

0. Incompleteness (1971)$_{24}$

1. Heuristic Principle (1974)$_{27}$

2. Halting Probability (1975)$_{28}$

Chaitin's Constant: $\mathbf{\Omega}$

← March 2001$_{54}$

IBM's Thomas John Watson Research Center in New York

A Genius

Many honors (& writings)

Many critics (and many fans)

0. Chaitin's Incompleteness Theorem

2018: (S. S. & P. Seraji), On Constructivity and the Rosser Property: a closer look at some Gödelean proofs, *APAL* 169(10):971–80.

2020: (Saeed Salehi) Gödel's Second Incompleteness Theorem: how it is derived and what it delivers, *BSL* 26(3-4):241–56.

Chaitin's (alternative proof for the 1st) Incompleteness Theorem:

For each sufficiently strong, consistent, and RE theory T,

there exists a (Characteristic/Chaitin) constant $\mathfrak{c}_T$ such that

for no string σ can T prove that

"σ cannot be generated by an input-free program with length $\leqslant \mathfrak{c}_T$".

true for co-finitely many σ's

2018: CIT is non-constructive, though can be extended to Rosserian.

2020: CIT cannot be constructive, and **not** infers or inferred from $\mathbb{G}_2$.

Exaggerations and Criticisms

1978: M. Davis: "Chaitin…showed how…to obtain a dramatic extension of Gödel's incompleteness theorem" (*What is a Computation?*, p. 265)

1986: G. Chaitin: "This [the CIT] is a dramatic extension of Gödel's theorem" (*Randomness and Gödel's theorem*, p. 68[Inf.Rand.Inc.$_{1987}$])

1988: I. Stewart: "Chaitin…has proved the ultimate in undecidability theorems…that the logical structures of arithmetic can be random" (*The Ultimate in Undecidability*, **Nature**$_{332}$, p. 115)

1989: G. Chaitin: "I have shown that God…plays dice…in pure math… My work is a fundamental extension of the work of Gödel and Turing on undecid. in pure math" (*Undecidability & Randomness in Pure Math*)

1989: M. van Lambalgen, *Algorithmic Information Theory*, **JSL** 54_4:1389–400.

1996: D. Fallis, *The Source of Chaitin's Incorrectness*, **Phil.Math.III** 4_3:261–96.

1998: P. Raatikainen, *On Interpreting Chaitin's Incom. Thm.*, **JPL** 27_6:569–86.

2000: P. Raatikainen, *Algor. Info. Theory & Undecid.*, **Synthese** 123_2:217–25.

A Fanfare

Lecture — Undecidability & Randomness in Pure Mathematics

Gregory J. Chaitin

Chapter

Abstract

I have shown that God not only plays dice in physics, but even in pure mathematics, in elementary number theory, in arithmetic! My work is a fundamental extension of the work of Gödel and Turing on undecidability in pure mathematics. I show that not only does undecidability occur, but in fact sometimes there is complete randomness, and mathematical truth becomes a perfect coin toss.

Book | © 2002

Conversations with a Mathematician

Math, Art, Science and the Limits of Reason

Home › Book

Authors: Gregory J. Chaitin

Written by the author of the best-selling trilogy "The Limits of Mathematics" "The Unknowable" and "Exploring Randomness"

A collection of interviews with Greg Chaitin, the creator of Algorithmic Information Theory

https://doi.org/10.1007/978-1-4471-0185-7_8

HP: Heuristic Principle / Halting Probability

- On Chaitin's Heuristic Principle and Halting Probability.
  arXiv:2310.14807v3 [math.LO].
  `https://arxiv.org/abs/2310.14807`

1. **H**euristic **P**rinciple

2. **H**alting **P**robability

1. CHAITIN'S HEURISTIC PRINCIPLE

- Greater Complexity Implies Unprovability

If a sentence is more complex (heavier) than the theory,
then that sentence is *unprovable* from that theory.

(Un-)Provability:

Example (Arithmetic & Geometry)

$\mathfrak{Arithmetic} \vdash \neg\exists x,y,z\,(xyz\neq 0 \wedge x^4+y^4=z^2)$. PIERRE DE FERMAT

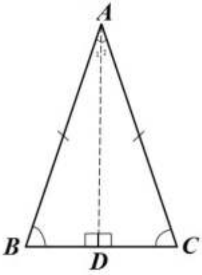
$\mathfrak{Arithmetic} \vdash \exists x,y,z>1\,(x^4+y^4=z^2+1)$. $x=5,\ y=7,\ z=55$

$\mathfrak{Arithmetic} \vdash \exists x,y,z\,(xyz\neq 0 \wedge x^4+y^4+1=z^2)$?

$\mathfrak{Geometry} \vdash \forall\triangle ABC\,(\overline{AB}=\overline{AC} \longleftrightarrow \angle B=\angle C)$

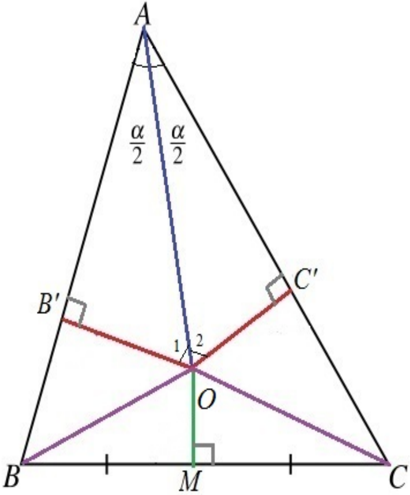
$\mathfrak{Arithmetic} \nvdash 1=2$ $\mathfrak{Geometry} \nvdash \forall\triangle ABC\,(\overline{AB}=\overline{AC})$

Arithmetic $\nvdash 1 = 2$



$$a = b$$
$$a^2 = ab$$
$$a^2 - b^2 = ab - b^2$$
$$(a + b)(a - b) = b(a - b)$$
$$(a + b) = b$$
$$a + a = a$$
$$2a = a$$
$$2 = 1$$

$\mathfrak{Geometry} \nvdash \forall\triangle ABC\,(\overline{AB}=\overline{AC})$



- $\angle BAO = \angle CAO \implies$
$\triangle OB'A \cong \triangle OC'A \implies$
$\overline{AB'} = \overline{AC'}$ & $\overline{OB'} = \overline{OC'}$

- $\overline{BM} = \overline{MC} \implies$
$\triangle OMB \cong \triangle OMC \implies$

$\overline{OB} = \overline{OC} \implies$
$\triangle OBB' \cong \triangle OCC' \implies$
$\overline{B'B} = \overline{C'C} \implies$

$\overline{AB'} + \overline{B'B} = \overline{AC'} + \overline{C'C}$
$\implies \overline{AB} = \overline{AC}$

https://jdh.hamkins.org/all-triangles-are-isosceles/

Solomonoff-Kolmogorov-Chaitin Complexity

Definition (Program Size Complexity)

$\mathcal{C}(x) =$ the length of
the shortest input-free program that outputs only x (and halts).

Example

$(10)^n = 1010\cdots10$	$\{10^n\}_{n=1}^{\infty} = 10100100010000\cdots10^n10^{n+1}\cdots$

BEGIN
  input n
  for $i=1$ to n
    print **1**
    print **0**
END
	BEGIN
	  let $n=1$
	  while $n>0$ do
	    begin
	      print **1**
	      for $i=1$ to n
	        print **0**
	      let $n=n+1$
	    end
	END

Descriptive Complexity & Randomness

- $111111111111111111111111111111111111 \cdots$ 1^*
- $100100100100100100100100100100100 \cdots$ $(100)^*$
- $0101101110111101111101111110111 \cdots$ $\{01^n\}_{n>0}$
- $0101111010111110111111111011 \cdots$ $\{01^{(\pi-3)_n}\}_{n=1}^{\infty}$
- $11000110000111111000010010100001101010 \cdots$

Definition (Random)

A random number or a string is one whose program-size complexity is almost its length.

COMPLEXITY OF SENTENCES AND THEORIES

Arithmetic:

- $\exists x,y,z\,(xyz\neq 0 \;\wedge\; x^2+y^2=z^2)$ $x=3,y=4,z=5$
- $\neg\exists x,y,z\,(xyz\neq 0 \;\wedge\; x^3+y^3=z^3)$
- $\neg\exists x,y,z\,(xyz\neq 0 \;\wedge\; x^4+y^4=z^4)$
- $\forall n>2\neg\exists x,y,z\,(xyz\neq 0 \;\wedge\; x^n+y^n=z^n)$

Geometry:

- $\forall\triangle ABC\,(M_a,M_b,M_c\text{midpoints}\longrightarrow\exists\mathbb{G}[AM_a\cap BM_b\cap CM_c=\{\mathbb{G}\}])$
- $\forall\triangle ABC\,(AA',BB',CC'\text{altitudes}\longrightarrow\exists\mathbb{H}[AA'\cap BB'\cap CC'=\{\mathbb{H}\}])$
- $\forall\triangle ABC\,\exists!\mathbb{O}\,(\overline{\mathbb{O}A}=\overline{\mathbb{O}B}=\overline{\mathbb{O}C})$
- $\forall\triangle ABC\,(\mathbb{G},\mathbb{H},\mathbb{O}\text{ are identical or on a line})$

Heuristic Principle, HP

Definition (HP-satisfying weighing)

A mapping $\mathscr{W}$ from theories and sentences to $\mathbb{R}$ satisfies HP when, for every theory $\mathcal{T}$ and every sentence ψ we have

$$\mathscr{W}(\psi) > \mathscr{W}(\mathcal{T}) \Longrightarrow \mathcal{T} \nvdash \psi.$$

Equivalently, $\mathcal{T} \vdash \psi \Longrightarrow \mathscr{W}(\mathcal{T}) \geqslant \mathscr{W}(\psi)$

- Chaitin's Idea: program-size complexity
- Lots of Criticisms ...
- Some built their own *partial* weighting
- Fans come to rescue ...

HP, A LOST PARADISE

- **CRITICISMS:**

  For complex sentences $\mathfrak{S}, \mathfrak{S}'$, or complex numbers $\mathcal{N}, \mathcal{N}'$, the following *complicated* sentences are all provable:

  - $\mathfrak{S} \rightarrow \mathfrak{S}$, $\mathfrak{S} \wedge \mathfrak{S}' \rightarrow \mathfrak{S}' \wedge \mathfrak{S}$, $(\neg \mathfrak{S}' \rightarrow \neg \mathfrak{S}) \Rightarrow (\mathfrak{S} \rightarrow \mathfrak{S}')$.
  - $1 + \mathcal{N} = \mathcal{N} + 1$, $\mathcal{N} \times \mathcal{N}' = \mathcal{N}' \times \mathcal{N}$, $n(\mathcal{N} + \mathcal{N}') = n\mathcal{N} + n\mathcal{N}'$.

- **A SALVAGE?**

  △ δ-complexity: $\mathcal{C}(x) - |x|$.
  XXX $\mathcal{T} \vdash \psi \Longrightarrow \delta(\mathcal{T}) \geqslant \delta(\psi)$ XXX

- **NO HOPE:**

  ▷ $\bot \rightarrow \mathfrak{S}$, $\mathfrak{S} \rightarrow \top$, $p \rightarrow (\mathfrak{S} \rightarrow p)$, $\neg p \rightarrow (p \rightarrow \mathfrak{S})$.
  ▷ $\mathcal{N} > 0$, $\mathcal{N} \times 0 = 0$, $1 + \mathcal{N} \neq 1$, $2 \leqslant 2 \times \mathcal{N}$.

HP^{-1}, the converse of HP

$$\text{HP}: \quad \mathcal{T} \vdash \psi \Longrightarrow \mathscr{W}(\mathcal{T}) \geqslant \mathscr{W}(\psi)$$

can be satisfied by any constant weighing.

$$\text{HP}^{-1}: \quad \mathscr{W}(\mathcal{T}) \geqslant \mathscr{W}(\psi) \Longrightarrow \mathcal{T} \vdash \psi$$

cannot hold for real-valued weights since every two real numbers are comparable ($a \geqslant b \vee b \geqslant a$), while some theories and sentences are incomparable, such as ψ and $\neg\psi$ for a non-provable and non-refutable ψ (like any atom in PL or $\forall x \forall y (x = y)$ in FOL).

Both HP and HP^{-1} hold for some non-real-valued weightings.

EP, The Equivalence Principle

$$\text{EP}: \quad \mathscr{W}(\mathcal{T}) = \mathscr{W}(\mathcal{U}) \Longrightarrow \mathcal{T} \equiv \mathcal{U}$$

is a (weak) consequence of HP^{-1}.

This is compatible with HP, even for real-valued weighings.

Theorem (Existence)

There exist some real-valued weightings that satisfy both HP and EP.

Theorem (Computability)

No computable HP+EP-satisfying weighing exists for undecidable logics.
For decidable logics, there are computable HP+EP-satisfying weightings.

The Proof

Definition (Sequence of Sentences)

Let $\psi_1, \psi_2, \psi_3, \cdots$ be an effective list of all the sentences.
For a theory T and $n > 0$, let

$$\chi_n(T) = \begin{cases} 0, & \text{if } T \nvdash \psi_n; \\ 1, & \text{if } T \vdash \psi_n. \end{cases}$$

Finally, let $\mathcal{V}(T) = \sum_{n>0} 2^{-n}\chi_n(T)$.

The Main Observation

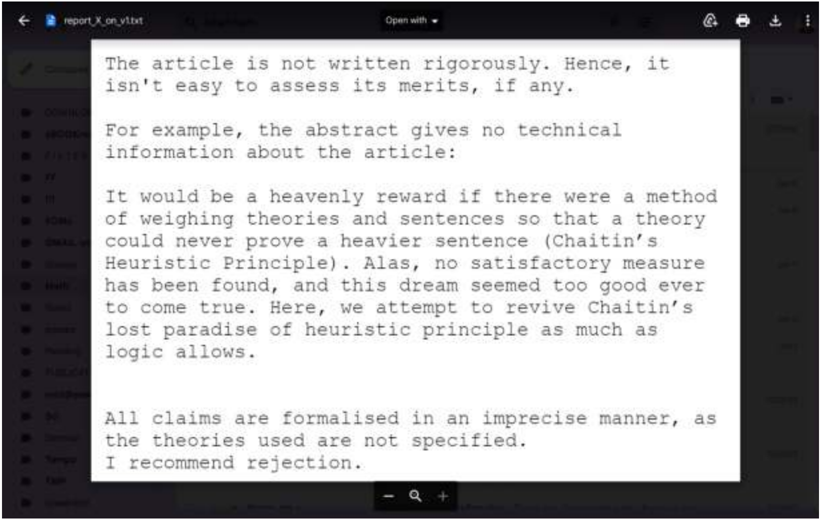
For all theories T and U, we have $T \vdash U \iff \forall n > 0\colon \chi_n(T) \geqslant \chi_n(U)$.

$\mathrm{HP} + \mathrm{HP}^{-1}$

So, we have both

$$\mathrm{HP} : T \vdash U \Longrightarrow \mathcal{V}(T) \geqslant \mathcal{V}(U)$$
$$\mathrm{EP} : \mathcal{V}(T) = \mathcal{V}(U) \Longrightarrow T \equiv U$$

A REFEREE REPORT (for 1.)



The article is not written rigorously. Hence, it isn't easy to assess its merits, if any.

For example, the abstract gives no technical information about the article:

It would be a heavenly reward if there were a method of weighing theories and sentences so that a theory could never prove a heavier sentence (Chaitin's Heuristic Principle). Alas, no satisfactory measure has been found, and this dream seemed too good ever to come true. Here, we attempt to revive Chaitin's lost paradise of heuristic principle as much as logic allows.

All claims are formalised in an imprecise manner, as the theories used are not specified.
I recommend rejection.

2. Chaitin's Halting Probability

- Halting Probability (of a randomly given input-free program)

$$\Omega = \sum_{p \text{ halts}} 2^{-|p|}.$$

Halting or Looping forever:

A random $\{0, 1\}$-string may not be (the ASCII code of) a program.
Even if it is, then it may not be input-free.
If a binary string is (the code of) an input-free program, then
it may halt after running or may loop forever.

$$\Omega = \sum_{p \in \{0,1\}^* \text{ halts}}^{p\text{: input-free}} 2^{-|p|}.$$

A Partial Agreement

The probability of getting a fixed binary string of length n by tossing a fair coin (whose one side is '0' and the other '1') is 2^{-n}, and the halting probability of programs with size n is

$$\frac{\text{the number of \textit{halting programs} with size } n}{\text{the number of \textit{all binary strings} with size } n} = \frac{\#\{p \in \mathbb{P} : p\downarrow \ \& \ |p| = n\}}{2^n}$$

since there are 2^n binary strings of size n. Thus, the halting probability of programs with size n can be written as $\sum_{p\downarrow}^{|p|=n} 2^{-|p|}$.

Denote this number by Ω_n; so, the number of halting programs with size n is $2^n\Omega_n$.

And a Disagreement

According to Chaitin (and almost everybody else), the halting probability of programs with size $\leqslant N$ is $\sum_{n=1}^{N}\Omega_n = \sum_{p\downarrow}^{|p|\leqslant N} 2^{-|p|}$; and so, the halting probability is $\sum_{n=1}^{\infty}\Omega_n = \sum_{p\downarrow} 2^{-|p|} (= \boldsymbol{\Omega})$!

Let us see why we believe this to be an error. The halting probability of programs with size $\leqslant N$ is in fact

$$\frac{\text{the number of halting programs with size} \leqslant N}{\text{the number of all binary strings with size} \leqslant N} = \frac{\sum_{n=1}^{N} 2^n\Omega_n}{\sum_{n=1}^{N} 2^n}.$$

Now, it is a calculus exercise to notice that, for sufficiently large Ns,

$$\frac{\sum_{n=1}^{N} 2^n\Omega_n}{\sum_{n=1}^{N} 2^n} \neq \sum_{n=1}^{N}\Omega_n, \text{ and } \lim_{N\to\infty}\frac{\sum_{n=1}^{N} 2^n\Omega_n}{\sum_{n=1}^{N} 2^n} \neq \lim_{N\to\infty}\sum_{n=1}^{N}\Omega_n.$$

Possible Errors / Mistakes

The number Ω was meant to be "the probability that a computer program whose bits are generated one by one by independent tosses of a fair coin will eventually halt".

As also pointed out by Chaitin, the series $\sum_{p\downarrow} 2^{-|p|}$ could be > 1, or may even diverge, if the set of programs is not taken to be *prefix-free* (that "no extension of a valid program is a valid program"—what "took ten years until [he] got it right").

So, the fact that, for *prefix-free* programs, the real number $\sum_{p\downarrow} 2^{-|p|}$ lies between 0 and 1 (by Kraft's inequality, that $\sum_{s\in S} 2^{-|s|} \leqslant 1$ for every prefix-free set S) does not make it the probability of anything!

POSSIBLE SOURCE OF ERROR / MISTAKE

$S \mapsto \Omega_S = \sum_{\sigma \in S} 2^{-|\sigma|}$ is a measure; but not a *probability* measure! (e.g. $\Omega_{\{0,1\}\cup\{00\}} > 1$). (Prefix-free sets are not closed under union).

If S is *prefix-free* (KRAFT) or *decipherable* (MCMILLAN) then $\Omega_S \leqslant 1$. ($\mathcal{C}$ is decipherable, when if $x_1 \cdots x_m = y_1 \cdots y_n$ for $x_i, y_j \in \mathcal{C}$, then $m = n$ and $x_i = y_i$ for all $i \leqslant m$). (The Guilty!)

► *Revisiting the Inequalities of KRAFT and MCMILLAN with New Proofs.*

But a real number cannot be called a probability, if it is just between 0 and 1; there should be a measure and a space for a probability that satisfies Kolmogorov axioms: $\mu(\emptyset) = 0$, $\mu(\mathbb{S}) = 1$, and $\forall \langle S_i \cap S_j = \emptyset \rangle_{i \neq j}$ family $\{S_i \subseteq \mathbb{S}\}$, we should have $\mu(\bigcup_i S_i) = \sum_i \mu(S_i)$.

For all the (input-free) programs $\mathbb{P}$, *we have* $\Omega_{\mathbb{P}} \neq 1$.

Any Solutions?

1. Conditional Probability

   Let $\Omega_S = \sum_{s\in S} 2^{-|s|}$ and $\mho_S = \Omega_S/\Omega_{\mathbb{P}}$ for a set $S \subseteq \mathbb{P}$ of programs. This is a probability measure: $\mho_\emptyset = 0$, $\mho_{\mathbb{P}} = 1$, and for any family $\{S_i \subseteq \mathbb{P}\}_i$ of pairwise disjoint sets of programs, $\mho_{\bigcup_i S_i} = \sum_i \mho_{S_i}$.
   If $\mathcal{H}$ is the set of all the binary codes of the halting programs, then the (conditional) halting probability is $\mho_{\mathcal{H}}$, or $\boldsymbol{\Omega}/\Omega_{\mathbb{P}}$.
   We then have $\mho_{\mathcal{H}} > \boldsymbol{\Omega}$ since it can be shown that $\Omega_{\mathbb{P}} < 1$.

2. Asymptotic Probability

   Count $\hbar_n$ the number of halting programs (the strings that code some input-free programs that eventually halt after running) that have integer codes‡ less than or equal to n. Then define the halting probability to be $\lim_{n\to\infty} \hbar_n/n$, of course, if it exists.
   Or take $\lim_{N\to\infty} \left(\sum_{n=1}^{N} 2^n\Omega_n\right)/\left(\sum_{n=1}^{N} 2^n\right)$ if the limit exists.

   Note that this number can be shown to be $\leqslant \dfrac{\boldsymbol{\Omega}}{2}$.

‡ integer code: $0_1, 1_2, 00_3, 01_4, 10_5, 11_6, 000_7, 001_8, 010_9, \cdots$

Thank You!

Thanks to

The Participants .... For Listening · · ·

and

The Organizer, For Taking Care of Everything · · ·