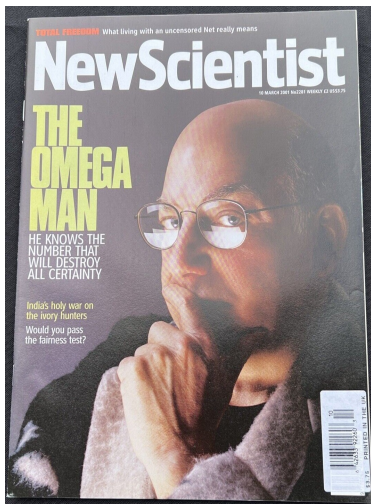


ON CHAITIN'S TWO HP'S:
(1) HEURISTIC PRINCIPLE
(2) HALTING PROBABILITY

SAEED SALEHI

February 2024

GREGORY JOHN CHAITIN



Born: 1947⁷⁷ (Jewish)

Argentine-American

Algorithmic Information Theory

A. KOLMOGOROV & R. SOLOMONOFF

◊. Incompleteness (1971)²⁴

1. Heuristic Principle (1974)²⁷

2. Halting Probability (1975)²⁸

CHAITIN'S Constant: Ω

← March 2001⁵⁴

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 c_T such that

for no string σ can T prove that

“ σ cannot be generated by an input-free program with length $\leq c_T$ ”.
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** 54₄:1389–400.
- 1996 D. Fallis, *The Source of Chaitin's Incorrectness*, **Phil.Math.III** 4₃:261–96.
- 1998 P. Raatikainen, *On Interpreting Chaitin's Incom. Thm.*, **JPL** 27₆:569–86.
- 2000 P. Raatikainen, *Algor. Info. Theory & Undecid.*, **Synthese** 123₂:217–25.

A FANFARE

Lecture — Undecidability & Randomness in Pure Mathematics

[Gregory J. Chaitin](#)

Chapter

236 Accesses | 1 [Altmetric](#)

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. Heuristic Principle
2. Halting Probability

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)

Arithmetic $\vdash \neg \exists x, y, z (xyz \neq 0 \wedge x^4 + y^4 = z^2)$.

Arithmetic $\vdash \exists x, y, z > 1 (x^4 + y^4 = z^2 + 1)$.

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

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

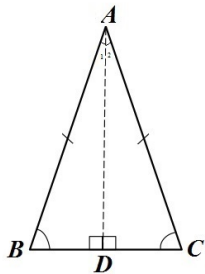
Arithmetic $\not\vdash 1 = 2$

Geometry $\not\vdash \forall \triangle ABC (\overline{AB} = \overline{AC})$

PIERRE DE FERMAT

$x = 5, y = 7, z = 55$

Arithmetic $\not\vdash 1=2$



$$a = b$$

$$a^2 = ab$$

$$a^2 - b^2 = ab - b^2$$

$$(a + b)(a - b) = b(a - b)$$

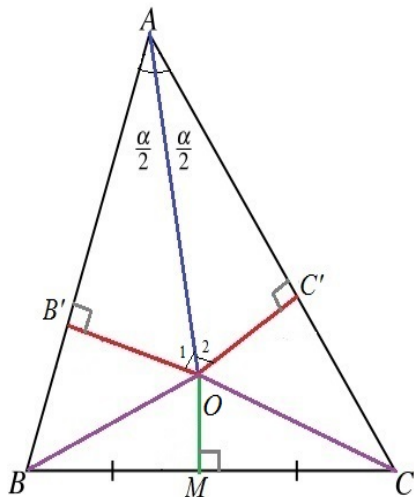
$$(a + b) = b$$

$$a + a = a$$

$$2a = a$$

$$2 = 1$$

Geometry $\not\equiv \forall \triangle ABC (\overline{AB} = \overline{AC})$



$$\bullet \angle BAO = \angle CAO \implies$$

$$\triangle OB'A \cong \triangle OC'A \implies$$

$$\overline{AB'} = \overline{AC'} \quad \& \quad \overline{OB'} = \overline{OC'}$$

$$\bullet \overline{BM} = \overline{MC} \implies$$

$$\triangle OMB \cong \triangle OMC \implies$$

$$\overline{OB} = \overline{OC} \implies$$

$$\triangle OBB' \cong \triangle OCC' \implies$$

$$\overline{B'B} = \overline{C'C} \implies$$

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

$$\implies \overline{AB} = \overline{AC}$$

SOLOMONOFF-KOLMOGOROV-CHAITIN COMPLEXITY

Definition (Program Size Complexity)

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

Example

$$(10)^n = 1010 \cdots 10 \quad \Bigg| \quad \{10^n\}_{n=1}^{\infty} = 10100100010000 \cdots 10^n 10^{n+1} \cdots$$

```
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
```


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:

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

HEURISTIC PRINCIPLE, HP

Definition (HP-satisfying weighing)

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

$$\mathcal{W}(\psi) > \mathcal{W}(\mathcal{T}) \implies \mathcal{T} \not\vdash \psi.$$

Equivalently, $\mathcal{T} \vdash \psi \implies \mathcal{W}(\mathcal{T}) \geq \mathcal{W}(\psi)$

- ▶ 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 δ -complexity: $\mathcal{C}(x) - |x|$.

XXX $\mathcal{T} \vdash \psi \Rightarrow \delta(\mathcal{T}) \geq \delta(\psi)$ XXX

► No HOPE:

- $\triangleright \perp \rightarrow \mathfrak{S}, \mathfrak{S} \rightarrow \top, p \rightarrow (\mathfrak{S} \rightarrow p), \neg p \rightarrow (p \rightarrow \mathfrak{S})$.
- $\triangleright \mathcal{N} > 0, \mathcal{N} \times 0 = 0, 1 + \mathcal{N} \neq 1, 2 \leq 2 \times \mathcal{N}$.

HP⁻¹, THE CONVERSE OF HP

$$\text{HP} : \mathcal{T} \vdash \psi \implies \mathcal{W}(\mathcal{T}) \geq \mathcal{W}(\psi)$$

can be satisfied by any **constant** weighing.

$$\text{HP}^{-1} : \mathcal{W}(\mathcal{T}) \geq \mathcal{W}(\psi) \implies \mathcal{T} \vdash \psi$$

cannot hold for real-valued weights since every two real numbers are comparable ($a \geq b \vee b \geq a$), 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

$$\text{EP} : \mathcal{W}(\mathcal{T}) = \mathcal{W}(\mathcal{U}) \implies \mathcal{T} \equiv \mathcal{U}$$

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

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

Theorem (Existence)

There exist some real-valued weighings 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 weighings.

THE PROOF

Definition (Sequence of Sentences)

Let $\psi_1, \psi_2, \psi_3, \dots$ be an effective list of all the sentences.

For a theory T and $n > 0$, let

$$\chi_n(T) = \begin{cases} 0, & \text{if } T \not\vdash \psi_n; \\ 1, & \text{if } T \vdash \psi_n. \end{cases}$$

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

The Main Observation

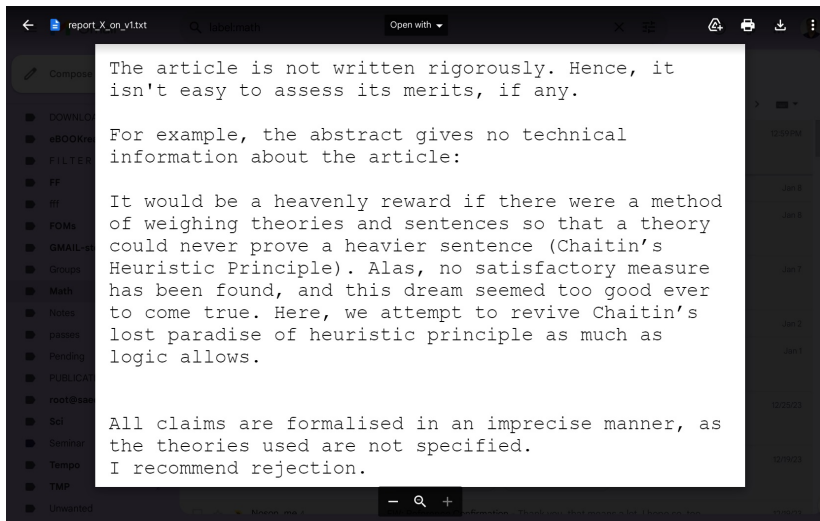
For all theories T and U , we have $T \vdash U \iff \forall n > 0: \chi_n(T) \geq \chi_n(U)$.
HP + HP⁻¹

So, we have both

$$\text{HP} : T \vdash U \implies \mathcal{V}(T) \geq \mathcal{V}(U)$$

$$\text{EP} : \mathcal{V}(T) = \mathcal{V}(U) \implies T \equiv U$$

A REFEREE REPORT (for 1.)



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.

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

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

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

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 $\leq N$ is $\sum_{n=1}^N \Omega_n = \sum_{p \downarrow}^{|\rho| \leq N} 2^{-|p|}$; and so, the halting probability is $\sum_{n=1}^{\infty} \Omega_n = \sum_{p \downarrow} 2^{-|p|} (= \Omega)$!

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

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

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

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

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

ANY SOLUTIONS?

1. CONDITIONAL PROBABILITY

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

2. ASYMPTOTIC PROBABILITY

Count \tilde{h}_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 $\lim_{n \rightarrow \infty} \tilde{h}_n / n$, of course, if it exists. Or take $\lim_{N \rightarrow \infty} (\sum_{n=1}^N 2^n \Omega_n) / (\sum_{n=1}^N 2^n)$ if the limit exists.

Note that this number can be shown to be $\leq \frac{\Omega}{2}$.

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

THANK YOU!

Thanks to

The Participants For Listening ...

and

The Organizer, For Taking Care of Everything ...