Available online at www.sciencedirect.com
SCIENCE DIRECT®
ADVANCES IN
Applied

www.elsevier.com/locate/yaama

Is complexity a source of incompleteness?

Cristian S. Calude [a,*], Helmut Jürgensen [b,c]

[a] *Department of Computer Science, The University of Auckland, Private Bag 92019, Auckland, New Zealand*
[b] *Department of Computer Science, The University of Western Ontario, London, Ontario, Canada N6A 5B7*
[c] *Institut für Informatik, Universität Potsdam, August-Babel-Str. 89, D-14469 Potsdam, Germany*

Received 11 November 2004; accepted 28 November 2004

Available online 21 January 2005

Abstract

In this paper we prove Chaitin's "heuristic principle," *the theorems of a finitely-specified theory cannot be significantly more complex than the theory itself*, for an appropriate measure of complexity. We show that the measure is invariant under the change of the Gödel numbering. For this measure, the theorems of a finitely-specified, sound, consistent theory strong enough to formalize arithmetic which is arithmetically sound (like Zermelo–Fraenkel set theory with choice or Peano Arithmetic) have bounded complexity, hence every sentence of the theory which is significantly more complex than the theory is unprovable. Previous results showing that incompleteness is not accidental, but ubiquitous are here reinforced in probabilistic terms: the probability that a true sentence of length n is provable in the theory tends to zero when n tends to infinity, while the probability that a sentence of length n is true is strictly positive.

1. Introduction

Gödel's Incompleteness Theorem states that every finitely-specified, sound, theory which is strong enough to include arithmetic cannot be both consistent and complete. Gödel's original proof as well as most subsequent proofs are based on the following idea: a theory which is finitely-specified, sound, consistent and strong enough can express sen-

* Corresponding author.
E-mail address: cristian@cs.auckland.ac.nz (C.S. Calude).

0196-8858/$ – see front matter
doi:10.1016/j.aam.2004.10.003

tences about provability within the theory, which, themselves, are not provable by the theory, but can be shown to be true using a proof by contradiction. A true and unprovable sentence is called independent. This type of proof of incompleteness does not answer the questions of whether independence is a widespread phenomenon nor which kinds of sentences can be expected to be independent.

Chaitin [14] presented a complexity-theoretic proof of Gödel's Incompleteness Theorem which shows that high complexity is a reason of the unprovability of infinitely many (true) sentences. This result suggested to him the following "heuristic principle," a kind of information-preservation principle: *the theorems of a finitely specified theory cannot be significantly more complex than the theory itself*. This approach would address the second of the questions above, that is, highly complex sentences are independent, and, as a consequence, would indicate that independence is pervasive. A formal confirmation of the pervasiveness of independence has been obtained in [9] via a topological analysis; a quantitative result is still missing.

In this paper we prove that a formal version of the "heuristic principle" is indeed correct for an appropriate measure of complexity; the measure is invariant under the change of the Gödel numbering. For this measure, δ, the theorems of a finitely-specified, sound, consistent theory which is strong enough to include arithmetic have bounded complexity, hence every sentence of the theory which is significantly more complex than the theory is unprovable. Previous results showing that incompleteness is not accidental, but ubiquitous are here reinforced in probabilistic terms: the probability that a true sentence of length n is provable in the theory tends to zero when n tends to infinity, while the probability that a sentence of length n is true is strictly positive.

The paper is organized as follows. In Sections 2 and 3 we present the background, the notation and main results needed for our proofs. In Section 4 we discuss some general complexity-theoretic results which will be used to prove the main result (Theorem 4.6). In Section 5 we prove that incompleteness is widespread in probabilistic terms. In Section 6 we use the new complexity measure to prove Chaitin's information-theoretic incompleteness result for the Omega Number. We finish with a few general comments in Section 7. The bibliography includes a selection of relevant papers and books, but is by no means complete.

2. Background

Gödel's Incompleteness Theorem, announced on 7 October 1930 in Königsberg at the First International Conference on the Philosophy of Mathematics[1] is a landmark of the twentieth century mathematics see ([31,32,34] for the original paper, [10,35,43,48] for other proofs and more related mathematical facts, [5,7,13,27,28,35,36,38,46,47,51] for more mathematical, historical and philosophical details). It says that *in a finitely-specified, sound, consistent theory strong enough to formalize arithmetic, there are true, but unprovable sentences;* so such a theory is *incomplete*. A true and unprovable sentence is called

[1] Hilbert, von Neumann, Carnap, Heyting presented reports; the conference was a part of the German Mathematical Congress.

independent. The first condition states that axioms can be algorithmically listed; consistency means free of contradictions; soundness means that any proved sentence is true.

According to Hintikka [35, p. 4], with the exception of von Neumann, who immediately grasped Gödel's line of thought and its importance, incompleteness passed un-noticed in Königsberg: even the speaker who summarized the discussion omitted Gödel's result. In spite of being praised, discussed, used or abused by many authors, the Incompleteness Theorem seems, even after so many years since its discovery, stranger than most mathematical theorems.[2] For example, according to Solovay [37, p. 399]: "The feeling was that Gödel's theorem was of interest only to logicians;" in Smoryński's words [37, p. 399], "It is fashionable to deride Gödel's theorem as artificial, as dependent on a linguistic trick."

In 1974 Chaitin [14] presented a complexity-theoretic proof of Gödel's Incompleteness Theorem which shows that high complexity is a reason of the unprovability of infinitely many (true) sentences. This complexity-theoretic approach was discussed by Chaitin [16–18,20,21,23] and various authors including Davis [24], Tymoczko [50], Boolos and Jeffrey [3, pp. 288–291], Svozil [49], Li and Vitányi [40], Barrow [1,2], Calude [4,6], Calude and Salomaa [11], Casti [12], Delahaye [25]; it was criticized by van Lambalgen [39], Fallis [30], Raatikainen [45], Hintikka [35].

Chaitin's proof in [14] is based on program-size complexity (Chaitin complexity) H: the complexity $H(s)$ of a binary string s is the size, in bits, of the shortest program for a universal self-delimiting Turing machine to calculate s. The complexity $H(s)$ is unbounded. The proof shows that *for every finitely-specified, sound, consistent theory strong enough to formalize arithmetic, there exists a positive constant M such that no sentence of the form "$H(x) > m$" is provable in the theory unless m is less than M*. There are infinitely many true sentences of the form "$H(x) > m$" with $m > M$, and each of them is unprovable in the theory.

The high H-complexity of the sentences "$H(x) > m$" with $m > M$ is a source of their unprovability.[3] Is every true sentence s with $H(s) > M$ unprovable by the theory? Unfortunately, the answer is *negative* because only finitely many sentences s have complexity $H(s) < M$ in contrast with the fact that the set of all theorems of the theory is infinite. For example, ZFC (Zermelo–Fraenkel set theory with choice) or Peano Arithmetic trivially prove all sentences of the form "$n + 1 = 1 + n$." The H-complexity of the sentences "$n + 1 = 1 + n$" grows unbounded with n. This fact, noticed and discussed by Chaitin in [22, Section 6] (reprinted in [21, pp. 55–81]) as well as by Svozil [49, pp. 123–125], is essential for the critique in [30,45] (cited in [35]); the works [21,22,49] seem to be unknown to the authors of [30,35,45].

Chaitin's proof based on H cannot be directly extended to all unprovable sentences, hence the problem of whether complexity is a source of incompleteness remained open. In this note we prove that the "heuristic principle" proposed by Chaitin [21, p. 69], namely that *the theorems of a finitely-specified theory cannot be significantly more complex than*

[2] This is quite impressive, as mathematics abounds with baffling results.

[3] Fallis [30, p. 264], argued that Gödel's true but unprovable sentence G is likely to have excessive H-complexity. Similarly, if the theory is capable of expressing its own consistency, then the corresponding sentence is likely to have excessive H-complexity. It would be interesting to have a mathematical confirmation of these facts.

the theory itself [4] is correct if we measure the complexity of a string by the difference between the program-size complexity and the length of the string, our δ-complexity (Theorem 4.6). The H-complexity of the sentences "$n+1=1+n$" grows unbounded with n, but the "intuitive complexity" of the sentences "$n+1=1+n$" remains bounded; this intuition is confirmed by δ-complexity. Note that a sentence with a large δ-complexity has also a large H-complexity, but the converse is not true. There are only *finitely* many strings with bounded H-complexity, but *infinitely* many strings with bounded δ-complexity.

As a consequence of Theorem 4.6, we prove that the incompleteness phenomenon is more widespread than previously shown in [14,20,21,31,32] and by the topological analysis of [9]: the probability that a true sentence of length n is provable in the theory tends to zero when n tends to infinity, while the probability that a sentence of length n is true is strictly positive.

3. Prerequisites

We follow the notation in [6]. By $\mathbb{N}=\{0,1,2,\ldots\}$ we denote the set of non-negative integers. Further on, $\log_Q$ denotes the base $Q \geqslant 2$ logarithm and $\log n = \lfloor \log_2(n+1)\rfloor$; $\lfloor\alpha\rfloor$ is the "floor" of the real α and $\lceil\alpha\rceil$ is the "ceiling" of α. The cardinality of the set A is denoted by $\mathrm{card}(A)$. An alphabet with Q elements will be denoted by X_Q; by X_Q^* we denote the set of finite strings (words) on X_Q, including the *empty* string λ. The length of the string $w \in X_Q^*$ is denoted by $|w|_Q$.

For $Q=2$, we use the special set $B=\{0,1\}$ instead of X_2. We consider the following bijection between non-negative integers and strings on B: $0\mapsto\lambda$, $1\mapsto 0$, $2\mapsto 1$, $3\mapsto 00$, $4\mapsto 01$, $5\mapsto 10$, $6\mapsto 11,\ldots$ The image of n, denoted $bin(n)$, is the binary representation of the number $n+1$ without the leading 1. Its length is $|bin(n)|_2=\log n$. In general, we denote by $string_Q(n)$ the nth string on X_Q according to the quasi-lexicographical order. In particular, $bin(n)=string_2(n)$. In this way we get a bijective function $string_Q:\mathbb{N}\to X_Q^*$; $|string_Q(n)|_Q=\lfloor\log_Q(n(Q-1)+1)\rfloor$.

We assume that the reader is familiar with Turing machines processing strings, computability and program-size complexity (see, for example, [3,4,6,26]). The program set (domain) of the Turing machine T is the set $PROG_T=\{x\in X_Q^*\colon T \text{ halts on } x\}$; when T halts on x, $T(x)$ is the result of the computation of T on x. A partial function φ from strings to strings is called partial computable (abbreviated p.c.) if there is a Turing machine T such that: (a) $PROG_T=\mathrm{dom}(\varphi)$, and (b) $T(x)=\varphi(x)$, for each $x\in PROG_T$. A computable function is a p.c. function φ with $\mathrm{dom}(\varphi)=X_Q^*$. A set of strings is computable if its characteristic function is computable. A set of strings is computably enumerable (abbreviated c.e.) if it is the program set of a Turing machine.

A *self-delimiting Turing machine* is a Turing machine T such that its program set is a prefix-free set of strings. Recall that a *prefix-free set* of strings S is a set such that no

[4] An "approximation" of this principle supported by Chaitin's proof is that "one cannot prove, from a set of axioms, a theorem that is of greater H-complexity than the axioms *and know* that one has done it;" see [21, p. 69], also Theorem 4.7 in Section 4.

string in S is a proper extension of any other string in S. In what follows the term *machine* will refer to either a p.c. function with prefix-free domain or a self-delimiting Turing machine.

Each prefix-free set $S \subset X_Q^*$ satisfies Kraft's inequality: $\sum_{i=1}^{\infty} r_i \cdot Q^{-i} \leqslant 1$, where $r_i = \mathrm{card}\{x \in S\colon\ |x|_Q = i\}$. A stronger result, the Kraft–Chaitin Theorem (see [6, p. 53]), is essential in algorithmic information theory: Let $n_1, n_2, \ldots$ be a computable sequence of non-negative integers such that

$$\sum_{i=1}^{\infty} Q^{-n_i} \leqslant 1. \tag{1}$$

Then, we can effectively construct a prefix-free sequence of strings $w_1, w_2, \ldots$ such that for each $i \geqslant 1$, $|w_i|_Q = n_i$.

The *program-size complexity* of the string $x \in X_Q^*$ (relative to T) is $H_{Q,T}(x) = \min\{|y|_Q\colon\ y \in X_Q^*,\ T(y) = x\}$, where $\min \emptyset = \infty$. The Invariance Theorem states that we can effectively construct a machine $U = U_Q$ (called *universal*) such that for every machine T there exists a constant $\varepsilon > 0$ such that for all $x \in X_Q^*$, $H_{Q,U}(x) \leqslant H_{Q,T}(x) + \varepsilon$. In what follows we will fix U and put $H_Q = H_{Q,U}$; in particular, H_2 denotes the program-size complexity induced by a universal (binary) machine. If x is in X_Q^*, then $x^* = \min\{u \in X_Q^*\colon U_Q(u) = x\}$, where the minimum is taken according to the quasi-lexicographical order; it is seen that $H_Q(x) = |x^*|_Q$.

4. Complexity and incompleteness

In this section we introduce the δ-measure and then prove for it Chaitin's "heuristic principle": *the theorems of a finitely-specified theory cannot be significantly more complex than the theory itself.*

First we introduce the δ-measure. Recall that U_Q is a fixed universal machine on X_Q and $H_Q = H_{Q,U_Q}$. In what follows we will work with the function $\delta_Q(x) = H_Q(x) - |x|_Q$ (note that $-\delta_Q$ is a "deficiency of randomness" function in the sense of [6, Definition 5.21, p. 113]). The δ-complexity is "close," but not equal, to the conditional H_Q-complexity, of a string given its length.

The complexity measures H_Q and δ_Q have similarities as δ_Q is defined from H_Q by means of some simple computable functions; for example, they are both uncomputable. But H_Q and δ_Q differ in an *essential* way: given a positive N, the set $\{x \in X_Q^*\colon\ H_Q(x) \leqslant N\}$ is finite while, by Corollary 4.3, the set $\{x \in X_Q^*\colon\ \delta_Q(x) \leqslant N\}$ is infinite. Note that the conditional H_Q-complexity does not have this property. A sentence with a large δ_Q-complexity has also a large H_Q-complexity, but the converse is not true. For example, the H_Q-complexity of a (true) sentence of the form "$1 + n = n + 1$" is about $\lfloor \log_Q n \rfloor$ plus a constant, a function which tends to infinity as $n \to \infty$; however, their δ_Q-complexity is bounded.

In view of in [6, Theorem 5.4, p. 102], there exists a constant $c > 0$ such that

$$\max_{|x|_Q = N} \delta_Q(x) \geqslant H_Q\big(\mathit{string}_Q(N)\big) - c, \tag{2}$$

so there are strings of arbitrarily large δ_Q-complexity.

The following result is taken from [6, Theorem 5.31, p. 117].

Theorem 4.1. *For every $t \geqslant 0$, the set $C_{Q,t} = \{x \in X_Q^*: \delta_Q(x) > -t\}$ is immune, that is, the set is infinite and contains no infinite c.e. subset.*

Corollary 4.2. *For every $t \geqslant 0$, the set* $\text{Complex}_{Q,t} = \{x \in X_Q^*: \delta_Q(x) > t\}$ *is immune.*

Proof. As $\text{Complex}_{Q,t} \subset C_{Q,t}$ and every infinite subset of an immune set is immune itself, we only need to show that $\text{Complex}_{Q,t}$ is infinite. To this aim we use formula (2) and the fact that the function $H_Q(string_Q(N))$ is unbounded. □

Corollary 4.3. *For every $t \geqslant 0$, the set $\{x \in X_Q^*: \delta_Q(x) \leqslant t\}$ is infinite.*

Proof. The set in the statement is not even c.e. because, by Corollary 4.2, its complement is immune. □

The above result suggests that any "reasonable" theory cannot include more than finitely many theorems with high δ-complexity. And, indeed, a simple analysis confirms this fact. A formal language used by a theory capable of speaking about natural numbers includes variables (a fixed variable x and the sign $'$ may be used to generate all variables, x, x', x'', etc.), the constant 0, function symbols for successor, addition and multiplication, $s, +, \cdot$, the sign for equality, $=$, logical connectives, $\neg, \wedge, \vee, \Rightarrow$, quantifiers, $\forall, \exists$, and parentheses, $(,)$. They form an alphabet X_{15}.[5] The formal language consists of well-formed formulae which respect strict syntactical rules; for example, each left parenthesis has to be matched with exactly one right parenthesis. Theorems are then defined by specifying the axioms and the inference rules. For instance, the system **Q** introduced by R.M. Robinson (see, for example, [29]) contains the logical axioms (propositional, substitution, $\forall$-distribution, equality axioms) and the following seven axioms:

Q1 $(s(x) = s(x')) \Rightarrow (x = x')$,
Q2 $\neg(0 = s(x))$,
Q3 $(\neg(x = 0)) \Rightarrow \exists x'(x = s(x'))$,
Q4 $x + 0 = x$,
Q5 $x + s(x') = s(x + x')$,
Q6 $x \cdot 0 = 0$,
Q7 $x \cdot s(x') = (x \cdot x') + x$,

and the inference rules of modus ponens and generalization. A proof in the system **Q** is a sequence of well-formed formulae such that each formula is either an axiom, or is derived from two earlier formulae in the sequence by an inference rule. *Theorems* are well-formed formulae which have proofs in **Q**. As theorems are special well-formed formulae,

[5] Of course, we can work with smaller or larger alphabets, depending on specific needs.

it is clear that each theorem x in the system $\mathbf{Q}$ has rather small H_{15}-complexity, more precisely, $H_{15}(x)$ is not larger than its length plus a fixed constant. Such a remark suggests that Chaitin's "heuristic principle" may be true for δ_{15}. However, this property could be a consequence of some particular way of writing/coding the theorems! To be able to measure somehow the "intrinsic" complexity of a theorem we need to prove that the property is *invariant with respect to a system of acceptable names*, in our case, *Gödel numberings*.

To make the discussion precise, let us fix a formal language $L \subset X_Q^*$. A *Gödel numbering* for L is a computable, one-to-one function $g : L \to B^*$, i.e. a system of unique binary names for the well-formed formulae of L. For example, a Gödel numbering for the well-formed formulae of the system $\mathbf{Q}$ can be obtained by coding the elements of the alphabet X_{15} with the first 15 binary strings of length four, and then extend this coding according to the syntax of the language. Various other possibilities can be imagined; see, for example, [3,29].

As the set of theorems is a c.e. subset of the set of well-formed formulae, we will work only with computable, one-to-one functions $g : \mathcal{T} \to B^*$ defined on the set of theorems.

The δ-complexity of a theorem $u \in \mathcal{T}$ induced by the Gödel numbering g is defined by

$$\delta_g(u) = H_2\bigl(g(u)\bigr) - \lceil \log_2 Q \rceil \cdot |u|_Q. \tag{3}$$

The formula for δ_f is essentially the formula defining δ_Q relativized to the Gödel numbering g: the factor $\lceil \log_2 Q \rceil$ has the role of "adjusting" the sizes of the alphabets X_Q and B.

The first result confirms the intuition: we prove that δ_g is, up to an additive constant, equal to $\lceil \log_2 Q \rceil \cdot \delta_Q$.

Theorem 4.4. *Let $\mathcal{T} \subset X_Q^*$ be c.e. and $g : \mathcal{T} \to B^*$ be a Gödel numbering. Then, there effectively exists a constant c (depending upon U_Q, U_2, and g) such that for all $u \in \mathcal{T}$ we have*

$$\bigl|\delta_g(u) - \lceil \log_2 Q \rceil \cdot \delta_Q(u)\bigr| \leqslant c. \tag{4}$$

Proof. First we prove the existence of a constant c_1 such that

$$\delta_g(u) \leqslant \lceil \log_2 Q \rceil \cdot \delta_Q(u) + c_1. \tag{5}$$

For each string $w \in PROG_{U_Q}$ we define $n_w = \lceil \log_2 Q \rceil \cdot |w|_Q$, and we note that

$$\sum_{w \in PROG_{U_Q}} 2^{-n_w} = \sum_{w \in PROG_{U_Q}} 2^{-\lceil \log_2 Q \rceil \cdot |w|_Q} \leqslant \sum_{w \in PROG_{U_Q}} Q^{-|w|_Q} \leqslant 1,$$

because $PROG_{U_Q}$ is prefix-free. Using now the Kraft–Chaitin Theorem, we can effectively construct, for every $w \in PROG_{U_Q}$ a binary string s_w such that $|s_w|_2 = n_w$ and the set $\{s_w\colon\ w \in PROG_{U_Q}\}$ is c.e. and prefix-free. This allows us to construct the machine C defined by

$$C(s_w) = g\bigl(U_Q(w)\bigr), \quad \text{for } w \in PROG_{U_Q}.$$

As $C(s_{w^*}) = g(U_Q(w^*)) = g(w)$ we have

$$H_C(g(w)) \leqslant |s_{w^*}|_2 = \lceil \log_2 Q \rceil \cdot |w^*|_Q = \lceil \log_2 Q \rceil \cdot H_Q(w).$$

Applying the Invariance Theorem, we get a constant $c_1 > 0$ such that

$$\begin{aligned}\delta_g(w) = H_2(g(w)) - \lceil \log_2 Q \rceil \cdot |w|_Q &\leqslant \lceil \log_2 Q \rceil \cdot (H_Q(w) - |w|_Q) + c_1 \\ &= \lceil \log_2 Q \rceil \cdot \delta_Q(w) + c_1,\end{aligned}$$

which proves (5).

Secondly, we prove the existence of a constant c_2 such that

$$\lceil \log_2 Q \rceil \cdot \delta_Q(u) \leqslant \delta_g(u) + c_2. \tag{6}$$

For each $w \in PROG_{U_2}$ such that $|w|_2 \geqslant \log_2 Q$, we put $m_w = \lceil |w|_2 \cdot \log_Q 2 \rceil \geqslant 1$ and note that

$$\sum_{\substack{w \in PROG_{U_2}, \\ |w|_2 \geqslant \log_2 Q}} Q^{-m_w} \leqslant \sum_{\substack{w \in PROG_{U_2}, \\ |w|_2 \geqslant \log_2 Q}} 2^{-|w|_2} \leqslant 1,$$

hence, in view of the Kraft–Chaitin Theorem, we can effectively construct, for every $w \in PROG_{U_2}$ with $|w|_2 \geqslant \log_2 Q$, a string $t_w \in X_Q^*$ of length $|t_w|_Q = m_w$ such that the set $\{t_w\colon w \in PROG_{U_2}\}$ is c.e. and prefix-free. In this way we construct the machine D defined by $D(t_w) = u$ if $U_2(w) = g(u)$. This construction is well-defined because g is a Gödel numbering. It is seen that if $U_2(w) = u$ and $|w|_2 \geqslant \log_2 Q$, then $H_D(u) \leqslant \lceil |w|_2 \cdot \log_Q 2 \rceil$, so applying the Invariance Theorem we get a constant d such that

$$\lceil \log_2 Q \rceil \cdot H_Q(u) \leqslant \lceil \log_2 Q \rceil \cdot H_D(u) + d \leqslant H_2(g(u)) + d,$$

hence there is a constant c_2 such that (6) becomes true. We have used the fact that $\lceil \log_2 Q \rceil \cdot \lceil m \cdot \log_Q 2 \rceil \leqslant m$, for all integers $m > 0$.

Finally, (4) follows from (5) and (6). $\square$

As a consequence, asymptotically, the δ-measure is independent of the Gödel numbering.

Corollary 4.5. *Let $\mathcal{T} \subset X_Q^*$ be c.e. and $g, g' : \mathcal{T} \to B^*$ be two Gödel numberings. Then, there effectively exists a constant c (depending upon U_2, g and g') such that for all $u \in \mathcal{T}$ we have*

$$|\delta_g(u) - \delta_{g'}(u)| \leqslant c. \tag{7}$$

Proof. The relation (7) follows from Theorem 4.4. However, it is instructive to give a short, direct proof. To this aim consider the machine C defined for $w \in B^*$ by $C(w) = g(u)$ if $U_2(w) = g'(u)$. The definition is correct because $PROG_C \subset PROG_{U_2}$ and g is computable and one-to-one. If $U_2(s) = g'(u)$, then $C(s) = g(u)$, so by the Invariance Theorem there exists a constant c_1 such that for all $u \in L$, $\delta_g(u) \leqslant \delta_{g'}(u) + c_1$. Finally, (7) follows by symmetry. □

Theorem 4.6. *Consider a finitely-specified, arithmetically sound* (*i.e. each arithmetical proven sentence is true*), *consistent theory strong enough to formalize arithmetic, and denote by $\mathcal{T}$ its set of theorems written in the alphabet X_Q. Let g be a Gödel numbering for $\mathcal{T}$. Then, there exists a constant N, which depends upon U_Q, U_2 and $\mathcal{T}$, such that $\mathcal{T}$ contains no x with $\delta_g(x) > N$.*

Proof. Because of syntactical constraints, there exists a positive constant d such that for every $x \in \mathcal{T}$, $H_Q(x) \leqslant |x|_Q + d$, i.e. $\delta_Q(x) \leqslant d$ (see also the discussion of the system **Q** following Corollary 4.3). Hence in view of Theorem 4.4, there is a constant $N \geqslant d$ such that for every $x \in \mathcal{T}$, $\delta_g(x) \leqslant N$. □

Every sentence x in the language of $\mathcal{T}$ with $\delta_g(x) > N$ is unprovable in the theory; every such "true" sentence is thus independent of the theory.

Do we have examples of such sentences? First, Chaitin's sentences of the form "$H_2(x) > n$," for large n are such examples.

Here is another way to construct true sentences of high δ-complexity. A formula $\varphi(x)$ in the language of arithmetic is called Σ_1 if it is of the form $(\exists y)\theta(x, y)$, where θ contains only two free variables x and y. We write $\mathbb{N} \models \varphi(n)$ to mean that $\varphi(n)$ is true when n is interpreted as a non-negative integer. The Representation Theorem (see [48]) states that a set $R \subset \mathbb{N}$ is c.e. iff there (effectively) exists a Σ_1 formula $\varphi(x)$ such that for all $n \in \mathbb{N}$ we have: $n \in R \Leftrightarrow \mathbb{N} \models \varphi(n)$.

For every $a \in \mathbb{N}$, the set $\{n \in \mathbb{N}\colon\ \delta_Q(\mathit{string}_Q(n)) \leqslant a\}$ is c.e., so in view of the Representation Theorem there exists a Σ_1 formula φ (depending on U_Q, a) such that for every $n \in \mathbb{N}$ we have: $\delta_Q(\mathit{string}_Q(n)) \leqslant a \Leftrightarrow \mathbb{N} \models \varphi(n)$. Consequently, the formula $\psi = \neg\varphi$ represents the predicate "$\delta_Q(\mathit{string}_Q(n)) > a$." Because of consistency and soundness, by enumerating the theorems in $\mathcal{T}$ of the form $\psi(m)$ (corresponding to true formulae $\psi(m)$) we get an enumeration of the set $\{x \in \mathcal{T}\colon\ \psi(\mathit{string}_Q^{-1}(x)) \in \mathcal{T}\} \subset \{x \in \mathcal{T}\colon\ \delta_Q(x) > a\}$.

Now let a be a non-negative integer. As $\{x \in \mathcal{T}\colon\ \psi(\mathit{string}_Q^{-1}(x)) \in \mathcal{T}\}$ is a c.e. subset of the immune set $\{x \in X_Q^*\colon\ \delta_Q(x) > a\}$, it has to be finite, that is, there exists an $M \in \mathbb{N}$ such that for every $x \in \mathcal{T}$ with $\psi(\mathit{string}_Q^{-1}(x)) \in \mathcal{T}$ we have: $|x|_Q \leqslant M$. We have got Chaitin's statement [21, p. 69]:

Theorem 4.7. *Every finitely-specified, arithmetically sound, consistent theory strong enough to formalize arithmetic can prove only, for finitely many of its theorems, that they have high δ-complexity.*

The theory can formalize all sentences of the form $\psi(m)$ in a very economical way, i.e. with small δ-complexity, but is incapable of proving more than finitely many instances: almost all true formulae of the form $\psi(m)$ are unprovable.

Comments. (a) Theorem 4.6 establishes a limit on the δ_g-complexity of provable sentences in $\mathcal{T}$; the bound depends upon the chosen Gödel numbering g. In this approach, it makes no sense to measure the power of the theory by its complexity, i.e. through the minimal N such that the theory proves no sentence x with $\delta_g(x) > N$ (see also the discussion in [39]).

(b) Theorem 4.6 does not hold true for an arbitrary finitely-specified theory as there are c.e. sets containing strings of arbitrary large δ-complexity.

(c) It is possible to have incomplete theories without high δ-complexity sentences; for example, an incomplete theory for propositional tautologies.

5. Is incompleteness widespread?

The first application complements the result of [9] stating that the set of unprovable sentences is topologically large. We probabilistically show that only a few true sentences can be proven in a given theory, but the set of true sentences is "large."

We begin with the following result.

Proposition 5.1. *Let $N > 0$ be a fixed integer, $T \subset X_Q^*$ be c.e. and $g : T \to B^*$ be a Gödel numbering. Then,*

$$\lim_{n\to\infty} Q^{-n} \cdot \operatorname{card}\bigl\{x \in X_Q^*\colon\ |x|_Q = n,\ \delta_g(x) \leqslant N\bigr\} = 0. \tag{8}$$

Proof. We present here a direct proof.[6] In view of Theorem 4.4, there exists a constant $c > 0$ such that

$$\bigl\{x \in X_Q^*\colon\ |x|_Q = n,\ \delta_g(x) \leqslant N\bigr\} \subseteq \bigl\{x \in X_Q^*\colon\ |x|_Q = n,\ \lceil \log_2 Q\rceil \cdot \delta_Q(x) \leqslant N + c\bigr\}.$$

So, we only need to evaluate the limit

$$\lim_{n\to\infty} Q^{-n} \cdot \operatorname{card}\bigl\{x \in X_Q^*\colon\ |x|_Q = n,\ \delta_Q(x) \leqslant M\bigr\} = 0, \tag{9}$$

where $M = \lceil (N + c)/\lceil \log_2 Q\rceil\rceil$.

First, we note that for every n we have: $\{x \in X_Q^*\colon\ |x|_Q = n,\ \delta_Q(x) \leqslant M\} = \{x \in X_Q^*\colon\ |x|_Q = n,\ \exists y \in X_Q^*(|y|_Q \leqslant n + M,\ U_Q(y) = x)\}$, so

$$\begin{aligned}\operatorname{card}\bigl\{x \in X_Q^*\colon\ |x|_Q = n,\ \delta_Q(x) \leqslant M\bigr\} &\leqslant \operatorname{card}\bigl\{y \in X_Q^*\colon\ |y|_Q \leqslant n + M,\ \bigl|U_Q(y)\bigr|_Q = n\bigr\}\\ &\leqslant \operatorname{card}\bigl\{y \in X_Q^*\colon\ |y|_Q \leqslant n + M,\ U_Q(y) \text{ halts}\bigr\}.\end{aligned}$$

[6] Alternatively, one can evaluate the size of the set of strings of a given length having almost maximum δ_Q-complexity.

Consequently,

$$\lim_{n\to\infty} Q^{-n}\cdot \mathrm{card}\bigl\{x\in X_Q^*\colon\ |x|_Q=n,\ \delta_Q(x)\leqslant M\bigr\} = \lim_{n\to\infty}\sum_{i=1}^{n+M} Q^{-n}\cdot r_i, \tag{10}$$

where $r_i = \mathrm{card}\{y\in X_Q^*\colon\ |y|_Q=i,]\ U_Q(y)$ halts$\}$. Using the Stolz–Cesaro Theorem, we get

$$\lim_{n\to\infty}\sum_{i=1}^{n+M} Q^{-n}\cdot r_i = Q^M\cdot \lim_{m\to\infty}\sum_{i=1}^{m} Q^{-i}\cdot r_i = Q^M/(Q-1)\cdot \lim_{m\to\infty} Q^{-m}\cdot r_m = 0, \tag{11}$$

due to Kraft's inequality $\sum_{i=1}^{\infty} r_i\cdot Q^{-i}\leqslant 1$. So, in view of (9)–(11), we get (8).

Theorem 5.2. *Consider a consistent, sound, finitely-specified theory strong enough to formalize arithmetic. The probability that a true sentence of length n is provable in the theory tends to zero when n tends to infinity, while the probability that a sentence of length n is true is strictly positive.*

Proof. We fix a consistent, sound, finitely-specified theory, let $\mathcal{T}$ be its set of theorems and let g be a Gödel numbering of $\mathcal{T}$. For every integer $n\geqslant 1$, let $\mathcal{T}^n=\{x\in\mathcal{T}\colon\ |x|_Q=n\}$. By Theorem 4.6, there exists a positive integer N such that $\mathcal{T}\subseteq\{x\in X_Q^*\colon\ \delta_g(x)\leqslant N\}$. Consequently, for every n: $\mathcal{T}^n\subseteq\{x\in X_Q^*\colon\ |x|_Q=n,\ \delta_g(x)\leqslant N\}$, so in view of Proposition 5.1, the probability that a sentence of length n is provable in the theory tends to zero when n tends to infinity.

Next consider the sentences $h_{x,m}=$ "$H_Q(x)>m$," where x is a string over the alphabet X_Q. For every $m\geqslant 1$ there exists a positive integer N_m such that for every string $x\in X_Q^*$ of length $|x|_Q>N_m$, $h_{x,m}$ is true.

For each fixed m, $|h_{x,m}|_Q=|x|_Q+c$, so for every $m\geqslant 1$ and $n\geqslant N_m+c$ we have:

$$\mathrm{card}\bigl\{w\in X_Q^*\colon\ |w|_Q=n,\ w \text{ is true}\bigr\}\cdot Q^{-n}\geqslant \mathrm{card}\bigl\{x\in X_Q^*\colon\ |x|_Q=n-c\bigr\}\cdot Q^{-n}\geqslant Q^{-c},$$

showing that the probability that a sentence of length n is true is strictly positive. □

6. Incompleteness and Ω_U

The second application is to use δ to prove Chaitin's Incompleteness Theorem for Ω_U [16] (see also the analysis in [6,8,25]). This shows that δ is a "natural" complexity. We start with the following preliminary result.

Lemma 6.1. *Let $x_1x_2\cdots$ be an infinite binary sequence and let F be a strictly increasing function mapping positive integers to positive integers. If the set $\{(F(i),x_{F(i)})\colon\ i\geqslant 1\}$*

is c.e., then there exists a constant $\varepsilon > 0$ (*which depends upon* U *and the characteristic function of the set*) *such that for all* $k \geqslant 1$ *we have*:

$$\delta_2(x_1x_2\cdots x_{F(k)}) \leqslant \varepsilon - k. \tag{12}$$

Proof. To prove (12), for $k \geqslant 1$ we consider the strings:

$$w_1x_{F(1)}w_2x_{F(2)}\cdots w_kx_{F(k)}, \tag{13}$$

where each w_j is a string of length $F(j) - F(j-1) - 1$, $F(0) = 0$. In this way, we effectively generate all binary strings of length $F(k)$ in which the bits on the "marked"positions $F(1), \ldots, F(k)$ are fixed.

It is clear that $\sum_{i=1}^{k} |w_i| = F(k) - k$ and the mapping $(w_1, w_2, \ldots, w_k) \mapsto w_1w_2\cdots w_k$ is bijective, hence to generate all strings of the form (13) we only need to generate all strings of length $F(k) - k$. Hence, we consider the enumeration of all strings of the form (13) for $k = 1, 2, \ldots$. The lengths of these strings form the sequence

$$\underbrace{F(1), F(1), \ldots, F(1)}_{2^{F(1)-1}\text{times}}, \ldots, \underbrace{F(k), F(k), \ldots, F(k)}_{2^{F(k)-k}\text{times}}, \ldots$$

which is computable and satisfies the inequality (1) as $\sum_{k=1}^{\infty} 2^{F(k)-k} \cdot 2^{-F(k)} = 1$. Hence, by the Kraft–Chaitin Theorem, for every string w of length $F(k) - k$ there effectively exists a string z_w having the same length as w such that the set $\{z_w \in B^*\colon |w|_2 = F(k) - k, k \geqslant 1\}$ is prefix-free. Indeed, from a string w of length $F(k) - k$, we get a unique decomposition $w = w_1\cdots w_k$, and z_w as above, so we can define $C(z_w) = w_1x_{F(1)}w_2x_{F(2)}\cdots w_kx_{F(k)}$; C is a machine. Clearly, $\delta_C(w_1x_{F(1)}w_2x_{F(2)}\cdots w_kx_{F(k)}) \leqslant |z_w|_2 - F(k) = -k$, for all $k \geqslant 1$. So by the Invariance Theorem, we get the inequality (12).

Consider now Chaitin's Omega Number, the halting probability of U: $\Omega_U = 0.\omega_1\omega_2\cdots$, see [15]. The binary sequence $\omega_1\omega_2\cdots$ is (algorithmically) random. There are various ways to characterize randomness (see, for example, [6,18,26]). A particular useful way is the following complexity-theoretic criterion due to Chaitin: there exists a positive constant μ such that for every $n \geqslant 1$,

$$\delta_2(\omega_1\omega_2\cdots\omega_n) \geqslant -\mu. \tag{14}$$

The condition (14) is equivalent to $\sum_{n=0}^{\infty} 2^{-\delta_2(\omega_1\omega_2\cdots\omega_n)} < \infty$, cf. [42].

It is easy to see that the inequality (12) in Lemma 6.1 contradicts (14), so a sequence $x_1x_2\cdots x_n\cdots$ satisfying the hypothesis of Lemma 6.1 cannot be random.

Theorem 6.2. *Consider a consistent, sound, finitely-specified theory strong enough to formalize arithmetic. Then, we can effectively compute a constant* N *such that the theory cannot determine more than* N *scattered digits of* $\Omega_U = 0.\omega_1\omega_2\cdots$.

Proof. Assume that the theory can determine infinitely many digits of $\Omega_U = 0.\omega_1\omega_2\cdots$ Then, we could effectively enumerate an infinite sequence of digits of Ω_U, thus satisfying the hypothesis of Lemma 6.1 which would contradict the randomness of $\omega_1\omega_2\cdots$. □

7. Conclusions

There are various illuminating proofs of Gödel's Incompleteness Theorem and some interesting examples of true but unprovable sentences (see, for example, [21,33,44]). Still, the phenomenon of incompleteness seems, even after almost 75 years since its discovery, strange and to a large extent irrelevant to 'mainstream mathematics,' whatever this expression might mean. Something is *missing* from the picture. Of course, the 'grand examples' are missing; for example, no important open problem except Hilbert's tenth problem, see [41], was proved to be unprovable. Other questions of interest include the source of incompleteness and how common the incompleteness phenomenon is. These two last questions have been investigated in this note.

Chaitin's complexity-theoretic proof of Gödel's Incompleteness Theorem [14] shows that high complexity is a sufficient reason for the unprovability of infinitely many (true) sentences. This approach suggested that excessive complexity may be a source of incompleteness, and, in fact, Chaitin (in [21,22]) stated this as a "heuristic principle:" "the theorems of a finitely-specified theory cannot be significantly more complex than the theory itself." By changing the measure of complexity, from program-size $H(x)$ to $\delta(x) = H(x) - |x|$, we have proved (Theorem 4.6) that for any finitely-specified, sound, consistent theory strong enough to formalize arithmetic (like Zermelo–Fraenkel set theory with choice or Peano Arithmetic) and for any Gödel numbering g of its well-formed formulae, we can compute a bound N such that no sentence x with complexity $\delta_g(x) > N$ can be proved in the theory; this phenomenon is independent on the choice of the Gödel numbering. For a theory satisfying the hypotheses of Theorem 4.6, the probability that a true sentence of length n is provable in the theory tends to zero when n tends to infinity, while the probability that a sentence of length n is true is strictly positive. This result reinforces the analysis in [9] which shows that the set of independent sentences is topologically large.

According to Theorem 4.6, sentences expressed by strings with large δ_g-complexity are unprovable. Is the converse implication true? In other words, given a theory as in the statement of Theorem 4.6, are there independent sentences x with low δ_g-complexity? Even if such sentences do exist, in view of Theorem 5.2, the probability that a true sentence of length n with δ_g-complexity less than or equal to N is unprovable in the theory tends to zero when n tends to infinity.

Other open questions which are interesting to study include:

(a) the complexity of some concrete independent sentences, like the sentence expressing the consistency of the theory itself,
(b) the problem of finding other (more interesting?) measures of complexity satisfying Theorem 4.6,

(c) a stronger version of Theorem 5.2: under the same conditions, the probability that a sentence of length n, expressible in the language of the theory, is provable in the theory tends to zero when n tends to infinity.

Acknowledgments

We thank Henning Bordihn, John Casti, Greg Chaitin, Maia Hoeberechts and André Nies for stimulating discussions and critical comments.

References

[1] J. Barrow, Impossibility. The Limits of Science and the Science of Limits, Oxford University Press, Oxford, 1998.
[2] J. Barrow, Mathematical jujitsu: Some informal thoughts about Gödel and physics, Complexity 5 (5) (2000) 28–34.
[3] G.S. Boolos, R.C. Jeffrey, Computability and Logic, third ed., Cambridge University Press, Cambridge, 1989.
[4] C. Calude, Theories of Computational Compexity, North-Holland, Amsterdam, 1988.
[5] C.S. Calude, A genius's story: two books on Gödel. The life and works of a master logician, Complexity 3 (2) (1997) 1–5.
[6] C.S. Calude, Information and Randomness. An Algorithmic Perspective, Springer-Verlag, Berlin, 1994; second ed., revised and extended, 2002.
[7] C.S. Calude, Incompleteness, complexity, randomness and beyond, Minds Machines 12 (4) (2002) 503–517.
[8] C.S. Calude, Chaitin Ω numbers, Solovay machines and incompleteness, Theoret. Comput. Sci. 284 (2002) 269–277.
[9] C. Calude, H. Jürgensen, M. Zimand, Is independence an exception? Appl. Math. Comput. 66 (1994) 63–76.
[10] C. Calude, G. Păun, Independent instances for some undecidable problems, RAIRO Inform. Théor. 17 (1983) 49–54.
[11] C. Calude, A. Salomaa, Algorithmically coding the universe, in: G. Rozenberg, A. Salomaa (Eds.), Developments in Language Theory, World Scientific, Singapore, 1994, pp. 472–492.
[12] J.L. Casti, Five More Golden Rules. Knots, Codes, Chaos, and Other Great Theories of 20th-century Mathematics, Wiley, New York, 2000.
[13] J.L. Casti, W. DePauli, Gödel. A Life in Logic, Perseus, Cambridge, MA, 2000.
[14] G.J. Chaitin, Information-theoretic limitations of formal systems, J. ACM 21 (1974) 403–424 (reprinted in [19, pp. 113–128]).
[15] G.J. Chaitin, A theory of program size formally identical to information theory, J. ACM 22 (1975) 329–340 (reprinted in [19, pp. 197–223]).
[16] G.J. Chaitin, Randomness and mathematical proof, Sci. Amer. 232 (1975) 47–52 (reprinted in [19, pp. 3–13]).
[17] G.J. Chaitin, Gödel's theorem and information, Int. J. Theoret. Phys. 21 (1982) 941–954 (reprinted in [19, pp. 61–71]).
[18] G.J. Chaitin, Algorithmic Information Theory, Cambridge University Press, Cambridge, 1987; third printing, 1990.
[19] G.J. Chaitin, Information, Randomness and Incompleteness, Papers on Algorithmic Information Theory, World Scientific, Singapore, 1987; second ed., 1990.
[20] G.J. Chaitin, Incompleteness theorems for random reals, Adv. in Appl. Math. 8 (1987) 119–146 (reprinted in [19, pp. 129–152]).
[21] G.J. Chaitin, Information-Theoretic Incompleteness, World Scientific, Singapore, 1992.
[22] G.J. Chaitin, LISP program-size complexity II, Appl. Math. Comput. 52 (1992) 103–126 (reprinted in [21, pp. 55–81]).

[23] G.J. Chaitin, The Limits of Mathematics, Springer-Verlag, Berlin, 1998.
[24] M. Davis, What is a computation? in: L.A. Steen (Ed.), Mathematics Today, Twelve Informal Essays, Springer-Verlag, New York, 1978, pp. 241–267.
[25] J.-P. Delahaye, Information, Compexité et Hasard, Hermes, Paris, 1994.
[26] R. Downey, D. Hirschfeldt, Algorithmic Randomness and Complexity, Springer-Verlag, Heidelberg, 2005, in press.
[27] J.W. Dawson Jr., Logical Dilemmas. The Life and Work of Kurt Gödel, Peters, Wellesley, MA, 1997.
[28] M. Detlefsen, Gödel's theorems, in: E. Craig (Ed.), Routledge Encyclopedia of Philosophy, vol. 4, Routledge, London, 1998, pp. 106–119.
[29] R.L. Epstein, W.A. Carnielli, Computability, Wadsworth & Brooks, Pacific Grove, CA, 1993.
[30] D. Fallis, The source of Chaitin's incorrectness, Philos. Math. 3 (4) (1996) 261–269.
[31] S. Feferman, J. Dawson Jr., S.C. Kleene, G.H. Moore, R.M. Solovay, J. van Heijenoort (Eds.), Kurt Gödel Collected Works, vol. II, Oxford University Press, New York, Oxford, 1990.
[32] K. Gödel, Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, Monatsh. Math. Phys. 38 (1931) 173–198.
[33] J. Hartmanis, J. Hopcroft, Independence results in computer science, ACM SIGACT News 8 (1976) 13–24.
[34] J. van Heijenoort (Ed.), From Frege to Gödel. A Source Book in Mathematical Logic, Harvard University Press, Cambridge, MA, 1967, pp. 1879–1931.
[35] J. Hintikka, On Gödel, Wadsworth, Belmont, 2000.
[36] S.C. Kleene, The work of Kurt Gödel, J. Symbolic Logic 41 (4) (1976) 761–778;
S.C. Kleene, An addendum to "The work of Kurt Gödel", J. Symbolic Logic 43 (3) (1978) 613.
[37] G. Kolata, Does Gödel's theorem matter to mathematics? in: L.A. Harrington, M.D. Morley, A. Sčedrov, S.G. Simpson (Eds.), Harvey Friedman's Research on the Foundations of Mathematics, North-Holland, Amsterdam, 1985, pp. 399–404, reprinted from: Science 218 (1982) 779–780.
[38] G. Kreisel, Kurt Gödel, Biographical Memoirs of Fellows of the Royal Society of London 26 (1980) 149–224; 27, 697; 28, 718.
[39] M. van Lambalgen, Algorithmic information theory, J. Symbolic Logic 54 (1989) 1389–1400.
[40] M. Li, P.M. Vitányi, An Introduction to Kolmogorov Complexity and Its Applications, Springer-Verlag, Berlin, 1993; second ed., 1997.
[41] Yu.V. Matiyasevich, Hilbert's Tenth Problem, MIT Press, Cambridge, MA, 1993.
[42] J. Miller, Private communication to C. Calude, 29 August 2003.
[43] E. Nagel, J.R. Newman, Gödel's Proof, New York University Press, New York, 1958; second printing, 1986.
[44] J. Paris, L. Harrington, A mathematical incompleteness in Peano Arithmetic, in: J. Barwise (Ed.), Handbook of Mathematical Logic, North-Holland, Amsterdam, 1977, pp. 1133–1142.
[45] P. Raatikainen, On interpreting Chaitin's incompleteness theorem, J. Philos. Logic 27 (1998) 569–586.
[46] F.A. Rodriguez-Consuegra (Ed.), Kurt Gödel: Unpublished Philosophical Essays, Birkhäuser, Basel, 1995.
[47] G. Rozenberg, A. Salomaa, Cornerstones of Undecidability, Prentice Hall, 1994.
[48] C. Smoryński, The incompleteness theorems, in: J. Barwise (Ed.), Handbook of Mathematical Logic, North-Holland, Amsterdam, 1977, pp. 821–866.
[49] K. Svozil, Randomness & Undecidability in Physics, World Scientific, Singapore, 1993.
[50] T. Tymoczko, New Directions in the Philosophy of Mathematics, Birkhäuser, Boston, 1986.
[51] H. Wang, A Logical Journey. From Gödel to Philosophy, MIT Press, Cambridge, MA, 1996.