PANU RAATIKAINEN

ALGORITHMIC INFORMATION THEORY AND UNDECIDABILITY

1. INTRODUCTION

Algorithmic information theory, or the theory of Kolmogorov complexity, has become an extraordinarily popular theory, and this is no doubt due, in some part, to the fame of Chaitin's incompleteness results arising from this field. Actually, there are two rather different results by Chaitin: the earlier one concerns the finite limit of the provability of complexity (see Chaitin, 1974a, 1974b, 1975a); and the later is related to random reals and the halting probability Ω (see Chaitin, 1986, 1987a, 1987b, 1988, 1989, 1990, 1992, 1993).

These results have indeed received wide attention, and they have been a source of lots of philosophical speculation. I have given a detailed critical examination of the interpretations of the earlier result of Chaitin elsewhere (Raatikainen, 1998); and it is my aim in this paper to discuss critically the received interpretation of the later result (for earlier critical discussion of both these results, see also the important paper by van Lambalgen (1989)).

My main target here is the purported strength of these results. The interpretation that I shall question becomes clear from the following representative quotations from Chaitin:

"This is a dramatic extension of Gödel's theorem. Number theory, the queen of mathematics, is infected with uncertainty and randomness" (Chaitin, 1986).

"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" (Chaitin, 1989).

Chaitin says that he constructs "a much more uncomputable real than Turing does" (viz. Ω); and he continues: "This is an impenetrable stone wall, it's a worst case. From Gödel we knew that we could not get a formal axiomatic system to be complete. We knew we were in trouble, and Turing showed us how basic it was, but Ω is an extreme case where reasoning fails

Synthese **123:** 217–225, 2000.

completely. ... I'm claiming I have a much stronger incompleteness result" (Chaitin, 1993). Sometimes Chaitin even claims that he is presenting "the strongest possible version of Gödel's incompleteness theorem" (Chaitin, 1987b, ix).

And Chaitin is certainly not alone in giving such strong conclusions. Stewart (1988), for example, writes that Chaitin "has proved the ultimate in undecidability theorems ... that the logical structure of arithmetic can be random"; and the title of Gardner (1979) preaches that "the random number omega bids fair to hold the mysteries of the universe" – not even to mention the fantastic interpretations that one can find in numerous popular science books.

Such strong claims, especially when they are published in respectable scientific forums, are certainly worthy of careful examination. It is my aim in this paper to question such claims and show that Chaitin's results are in fact rather non-dramatic and simple consequences of Turing's classical result concerning the undecidability of the halting problem, and that they are certainly not the most extreme possible undecidability or incompleteness results.

2. TECHNICAL REQUISITES

Let us first review shortly the basic notions on which the discussion below is based. (For all unexplained notation and terminology from recursive function theory, the reader can consult e.g. Rogers (1967) or Odifreddi (1989), and for futher details of algorithmic information theory, e.g., Chaitin (1987b) or Li & Vitanyi (1993).)

By a *prefix-free* coding (of Turing machines, programs etc.) one means any such coding that no code is an initial segment of another code. Let a standard prefix-free coding of Turing machines be fixed. Let us denote a Turing machine with the code e by T_e, the corresponding partial recursive function by φ_e, and, the recursively enumerable (or, in short, r.e.) set that is the domain of φ_e by W_e. The standard halting set is denoted by $\mathcal{K}_0$, i.e., $\langle x, e\rangle \in \mathcal{K}_0 \Leftrightarrow x \in W_e$. By an *acceptable* coding system one means any coding system such that it is possible to go effectively from the standard coding to the system, and *vice versa*.

Let U be a universal Turing machine which accepts only binary prefix-free programs. The length of a binary program p is denoted by $|p|$. We are now ready to define our key subject of study, viz. Chaitin's famous random real Ω. Formally,

$$\Omega = \sum_{U(p)\ halts} 2^{-|p|}\ .$$

Intuitively, Ω may be considered as the halting probability of the universal Turing machine U, i.e. the probability that U halts when its binary prefix-free input is chosen randomly, e.g., by flipping a coin. It is worth emphasizing that Ω is Δ_2^0 (see e.g., van Lambalgen (1989), or Li & Vitanyi (1993), 185), for I shall use this fact repeatedly in what follows. Note also that Ω is in fact relative to the chosen universal machine U, and thus to a particular coding of Turing machines that is used.

The algorithmic complexity of a finite string s, $K(s)$, is defined as $\min\{|p| : U(p) = s\}$. A finite string s is called *random* if its complexity is (roughly) equal to its length, $|s| \approx K(s)$, i.e., if it cannot be compressed to a shorter program. An infinite sequence s is defined to be random if the algorithmic complexity of the initial segement s_n of length n does not drop arbitrarily far below n, i.e., $(\exists c)(\forall n)[K(s_n) \geq n - c]$. It turns out that Ω is, in this defined sense, random.

Now the incompleteness theorem of Chaitin that concerns these notions is the following:

THEOREM 2.1. (Chaitin, 1987a, 1987b, 1992). *Any recursively axiomatizable formalized theory enables one to determine only finitely many digits of* Ω.

Further, Chaitin has constructed a gigantic exponential Diophantine equation (it has 17 000 variables) with a parameter n such that the equation has, for a given n, infinitely (resp. finitely) many solutions if and only if the n-th digit of (the binary presentation of) Ω is 1 (resp. 0) (see Chaitin, 1987b).

3. ON THE UNCOMPUTABILITY OF Ω

It is often emphasized in the literature that if one could compute Ω, then one could decide the halting problem. What is not always so clearly expressed is that a dependence also holds in the other direction. As this fact plays a rather central role below, let us demonstrate it.

THEOREM 3.1. *Ω is recursive in the halting set $\mathcal{K}_0$.*

Proof. It is a special case of Post's Theorem (Post, 1948) that a set is Δ^0_2 iff it is recursive in a Σ^0_1 or Π^0_1 relation. Recall then that $\mathcal{K}_0$ is Σ^0_1-complete. Hence any Σ^0_1 or Π^0_1 relation is recursive in $\mathcal{K}_0$. Thus being recursive in some Σ^0_1 or Π^0_1 relation is equivalent to being recursive in $\mathcal{K}_0$, and a set is Δ^0_2 if and only if it is recursive in $\mathcal{K}_0$. Thus Ω in particular is recursive in $\mathcal{K}_0$. QED.

Intuitively, in terms of relative decidability, this means that Ω is decidable relative to the halting problem; that is, if one could decide the halting problem – say, one could consult an oracle that would give the correct answer for any particular halting question – one could then decide Ω as well. Thus, from the point of view of computability, or decidability, the difference between the much-advertised Ω and the standard halting problem is less drastic than one might believe after reading the most enthusiastic expositions of Chaitin's work.

4. TRIAL AND ERROR COMPUTABILITY

As it happens, Δ^0_2 sets have also a very interesting and natural computational characterization, which is based on the idea of computability in the limit; this is the notion of "trial and error predicate", due to Putnam (1965). As this interesting liberalized notion of computability is apparently not as widely known as it deserves, I shall give a rather detailed exposition of it, following quite closely Putnam's orginal presentation.

The intuitive motivation of the concept of trial and error predicate is the following (see Putnam, 1965): one modifies the notion of a decision procedure by (i) allowing the procedure to "change its mind" any finite number of times (in terms of Turing machines: one visualizes the machine as being given an integer (or an n-tuple of integers) as input. The machine then prints out a finite sequence of "yesses" and "nos". The *last* "yes" or "no" is always to be the correct answer.); and (ii) one gives up the requirement that it be possible to tell (effectively) if the computation has terminated. That is, if the machine has most recently printed "yes", then one knows that the integer put in as input must be in the set *unless the machine is going to change its mind*; but one has no procedure for telling whether the machine will change its mind or not.

The sets for which there exist decision method in this widened sense are decidable by "empirical" means – for, if one always "posits" that the most recently generated answer is correct, one will make a finite number of mistakes, but one will eventually get the correct answer. (Note, however, that even if one has gotten to the correct answer, one is never sure that one has the correct answer.) More formally:

DEFINITION 4.1. (Putnam, 1965). P is called a *trial and error predicate* iff there is a general recursive function f such that that (for every x)

$$P(x) \iff \lim_{y\to\infty} f(x, y) = 1,$$

$$\bar{P}(x) \iff \lim_{y\to\infty} f(x, y) = 0,$$

where

$$\lim_{y\to\infty} f(x, y) = k \ =_{df} (\exists y)(\forall z)(z \geq y \rightarrow f(x, z) = k).$$

Now the fundamental characterization theorem that makes the relevance of this notion for the present purpose transparent is the following:

THEOREM 4.2. (Putnam, 1965). *P is a trial and error predicate if and only if P is* Δ_2^0.

It follows immediately that Ω can be represented by a trial and error predicate; or, in other words, that Ω can be generated by a trial and error procedure.

Although apparently ignorant of the above notions, it is interesting to note that Chaitin is aware of the fact that Ω is computable in the limit: "However, with computations in the limit, which is equivalent to having an oracle for the halting problem, Ω seems quite understandable: it becomes a computable sequence" (Chaitin, 1987b, 161). Nevertheless, Chaitin draws no critical conclusions from this fact.

The important aspect that matters here is that a trial and error procedure is still completely deterministic; the machine described above proceeds in a perfectly determinate manner. This means in particular that Ω, although not recursively enumerable, can still be generated by a completely deterministic procedure. And this, in turn, should raise some doubts about the genuine randomness of Ω, and more generally, about the plausibility of a definition of randomness that counts such sequences as random.

That is, this observation does not only put the wildest claims on the extreme uncomputability of Ω in the right perspective. It also raises the question of whether the algorithmic theory of randomness is, after all, the most perfect possible theory of randomness. For it classifies as random sequences those which, although not recursively enumerable, can be generated by a completely deterministic process. This is, at least in my mind, a rather serious weakness of this theory.

5. Ω AND OTHER UNDECIDABLE PROBLEMS

Let us next evaluate the strength of the undecidability of Ω and the related incompleteness results. It is highly illuminating to compare them to certain other well-known logical undecidability and incompleteness results.

Let us begin with an example from computability theory. Namely, one should compare Ω to the infinity problem and the finity problem: the set $\{x : W_x$ is infinite$\}$ is Π^0_2-complete, and the set $\{x : W_x$ is finite$\}$ is Σ^0_2-complete (see e.g., Rogers, 1967, 326). Thus these strikingly simply definable and natural sets are properly harder to compute than Ω; in particular, neither of them can be generated by a trial and error procedure.

Next, turning our attention to incompleteness theorems, consider the semi-formal theory PA^+ obtained from Peano Arithmetic by adding to it all the true Π^0_1 sentences; PA^+ can decide the halting problem, and it follows, by Theorem 3.1., that PA^+ can decide Ω completely. On the other hand, it is known that even PA^+ cannot prove the well-known undecidable proposition of Paris and Harrington (1977). (As Kreisel (1980, 175) has pointed out; cf. Kleene (1986)). This Π^0_2 sentence is a natural finitary version of Ramsey's theorem, a simple sentence of combinatorics – in contradistinction to the huge and completely artificial arithmetical equation of Chaitin (which has 17 000 varibles and fills some 200 pages!). Later Friedman has provided other finitary combinatorial truths that are unprovable even in much stronger theories (see Harrington et al., 1985). There are thus well-known, natural and simple mathematical truths that are, in a definite sense, more unprovable than the facts concerning the digits of Ω.

Further, it is straightworward to generalize Gödel's original trick to PA^+, and to other non-effictively axiomatizable theories, to obtain true unprovable sentences – this was noted by Rosser (1937) (cf. Mostowski 1952, Kreisel and Levy, 1968). In general, it is well known that, for any n, the set of true Π^0_n sentences have a Π^0_n truth definition (and similarly for Σ^0_n); let us denote such a definition by $\mathrm{Tr}_{\Pi^0_n}(x)$. Let $\mathrm{Prov}(x)$ be a standard provability predicate. By applying Gödel's diagonalization lemma – also known as fixed-point lemma and self-referential lemma – (for some n) to the formula $(\forall x)[\mathrm{Tr}_{\Pi^0_n}(x) \rightarrow \neg\mathrm{Prov}(x \dot{\rightarrow} y)]$ one obtains a true sentence that says that it is not provable from the (non-effective) theory that contains all the true Π^0_n sentences (see Kreisel and Levy, 1968). Clearly one can thus obtain incompleteness results that go far beyond anything that Chaitin has reached.

Finally, speaking about “extreme undecidability”, one can hardly find a more basic and more extremely undecidable set than the set of sentences that are *true* in the standard model of arithmetic; this set is not Σ^0_n or Π^0_n for any n, but only Δ^1_1; this classical result was proved by Tarski (1933) (and in fact also by Gödel in 1930, although he did not publish it but went on to prove his incompleteness theorems). Thus even a complete knowledge of Chaitin’s Ω would not at all enable one to decide this fundamental set – the set of arithmetical truths.

One may thus conclude that the undecidablity and incompleteness results arising from Chaitin’s Ω are in no way “ultimate”, “extreme”, or the “strongest”. There are plenty of more undedicable problems and more unprovable truths, which are in addition much more simple and natural.

6. ON THE LIMITS OF FORMAL SYSTEMS

An integral part of the standard interpretation of Chaitin’s incompleteness result on random reals (Theorem 2.1.) is the claim that, in addition to the fact that one can decide in a given formalized theory only finitely many digits of Ω, this finite limit is determined by the complexity of the formalized theory itself (by the complexity of a formalized theory $\mathcal{F}$ one means here the size of the minimal program that enumerates all the theorems of $\mathcal{F}$).

I shall show next (by an argument somewhat similar to the one that I used in (Raatikainen, 1998) that this interpretation is simply false.

Let $\mathcal{F}$ be a formalized theory that contains elementary arithmetic, and let $T_{\mathcal{F}}$ be a Turing machine that (given a coding of the language of $\mathcal{F}$) enumerates the theorems of $\mathcal{F}$. Obviously $\mathcal{F}$ can itself prove that it has infinitely many theorems, and consequently that $T_{\mathcal{F}}$ does not halt.

Fix then an *acceptable coding* of Turing machines as follows: (i) let $T_{\mathcal{F}}$ have the minimal code 0; and (ii) up to some very large n (e.g., $n = 10^{10^{10}}$), choose the first n programs such that they halt, and $\mathcal{F}$ can prove this fact. (After n, one may code the programs in any suitable way.)

Now the complexity of $\mathcal{F}$ (in the chosen coding) is the minimal possible. Yet $\mathcal{F}$ can decide a very large number of digits of Ω (relative to this coding). As one can choose n above to be however large one wishes, the argument shows that there is no real connection between the complexity of a formalized theory and the number of digits of Ω it can decide. In fact, in the above coding, it is relatively easy to check (and prove in any plausible arithmetical theory) that $\Omega = 0.4999\ldots999\ldots$ (in the ordinary decimal notation); i.e. that for a very large m (although a little smaller than n above) the first m (after the initial 0.4) digits of Ω are nines.

The basic problem here is that the whole setting is relative to even two different codings: the coding of Turing machines, and the Gödel numbering of formalized theories. And obviously there is neither priviledged coding of Turing machines (and universal Turing machine), nor priviledged Gödel numbering of formalized theories, and consequently certainly no absolute, non-relative complexity of a formalized theory.

7. CONCLUSIONS

It would be absurd to completely disparage the interest shown in the halting probability Ω; it in admittedly an interesting sequence. But neither should one overstate its relevance or its undecidability. It is just one among various undecidable sets, neither the most natural and simple, nor the most strongly undecidable. Especially, its rather ingenious definition and its close dependence on the halting problem make it, at least from the point of view of logic in general, certainly much less central than one might think considering various ardent expositions.

REFERENCES

Chaitin, Gregory J.: 1974a, ‘Information-Theoretic Computational Complexity’, *IEEE Transactions on Information Theory IT-20*, pp. 10–15.

Chaitin, Gregory J.: 1974b, ‘Information-Theoretic Limitations of Formal Systems’, *Journal of the ACM* **21**, 403–424.

Chaitin, Gregory J.: 1975a, ‘Randomness and Mathematical Proof’, *Scientific American* **232**(5), 47–52.

Chaitin, Gregory J.: 1975b, ‘A Theory of Program Size Formally Identical to Information Theory’, *Journal of the ACM* **22**, 329–340.

Chaitin, Gregory J.: 1986, ‘Randomness and Gödel’s Theorem’, *Mondes en Developpement,* **54–55**, 125–128.

Chaitin, Gregory J.: 1987a, ‘Incompleteness Theorem for Random Reals’, *Advances in Applied Mathematics* **8**, 119–146.

Chaitin, Gregory J.: 1987b, *Algorithmic Information Theory*, Cambridge University Press, Cambridge.

Chaitin, Gregory J.: 1988, ‘Randomness in Arithmetic’, *Scientific American* **259**(1), 80–85.

Chaitin, Gregory J.: 1989, ‘Undecidability and Randomness in Pure Mathematics’, (a transcript of a lecture delivered 28 September 1989 at SOLVAY conference in Brussels) published in G. J. Chaitin: *Information, Randomness & Incompleteness,* 2nd edn., World Scientific, 1990, pp. 307–313.

Chaitin, Gregory J.: 1990, ‘A Random Walk in Arithmetic’, *New Scientists* **24**, 44–46.

Chaitin, Gregory J.: 1992, 'Information-Theoretic Incompleteness', *Applied Mathematics and Computation* **52**, 83–101.

Chaitin, Gregory J.: 1993, 'Randomness in Arithmetic and the Decline and Fall of Reductionism in Pure Mathematics', *EATCS Bulletin, No. 50 (June 1993)*, pp. 314–328. Reprinted in G. Chaitin: *The Limits of Mathematics*, Springer, Singapore, 1998, pp. 1–27.

Delahaye, Jean-Paul: 1989, 'Chaitin's Equation: an Extension of Gödel's Theorem', *Notices of the A.M.S.* **36**(8), 984–987.

Gardner, Martin: 1979, 'Mathematical Games: the Random Number Omega Bids Fair to Hold the Mysteries of the Universe', *Scientific American* **241**(5), 20–43.

Harrington, L. A., M. D. Morley, A. Scederov and S. G. Simpson (eds): 1985, *Harvey Friedman's Research on the Foundations of Mathematics*, North-Holland, Amsterdam.

Kleene, Stephen C.: 1986, 'Introductory Note to 1930b, 1931 and 1932b', in S. Feferman et al. (eds), Kurt Gödel: *Collected Works, Vol. 1*, Oxford University Press, 1986, pp. 126–141.

Kreisel, Georg: 1980, 'Kurt Gödel', *Biographical Memoirs of Fellows of the Royal Society* **26**, 149–224.

Kreisel, Georg and Azriel Levy: 1968, 'Reflection Principles and their Uses for Establishing the Complexity of Axiomatic Systems', *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik* **14**, 97–142.

Li, Ming and Paul Vitanyi: 1993, *An Introduction to Kolmogorov Complexity and its Applications*, Springer-Verlag, New York.

van Lambalgen, Michiel: 1989, 'Algorithmic Information Theory', *Journal of Symbolic Logic* **54**, 1389–1400.

Mostowski, Andrzej: 1952, *Sentences Undecidable in Formalized Arithmetic – An Exposition of the Theory of Kurt Gödel*, North-Holland, Amsterdam.

Odifreddi, Piergiorio: 1989, *Classical Recursion Theory*, North-Holland, Amsterdam.

Paris, Jeff and Leo Harrington: 1977, 'A Mathematical Incompleteness in Peano Arithmetic', in J. Barwise (ed.), *Handbook of Mathematical Logic*, North-Holland, Amsterdam, pp. 1133–1142.

Post, Emil: 1948, 'Degrees of Recursive Unsolvability', *Bulletin of the A.M.S.* **54**, 641–42.

Putnam, Hilary: 1965, 'Trial and Error Predicates and the Solution to a Problem of Mostowski', *Journal of Symbolic Logic* **30**, 49–57.

Raatikainen, Panu: 1998, 'On Interpreting Chaitin's Incompleteness Theorem', *Journal of Philosophical Logic* **27**, 569–86.

Rogers, Hartley Jr.: 1967, *Theory of Recursive Functions and Effective Computability*, McGraw-Hill, New York.

Rosser, J. Barkley: 1937, 'Gödel's Theorems for Non-Constructive Logics', *Journal of Symbolic Logic* **2**, 129–137.

Stewart, Ian: 1988, 'The Ultimate in Undecidability', *Nature* **332**, 115–16.

Tarski, Alfred:1933/1956, 'The Concept of Truth in Formalized Languages', in *Logic, Semantics, Metamathematics*, edited and translated by J. H. Woodger, Oxford University Press, Oxford.