Book Review

Exploring Randomness and *The Unknowable*

Reviewed by Panu Raatikainen

Exploring Randomness
Gregory Chaitin
Springer-Verlag, 2000
ISBN 1-85233-417-7
176 pages, $34.95

The Unknowable
Gregory Chaitin
Springer-Verlag, 1999
ISBN 9-814-02172-5
122 pages, $29.00

In the early twentieth century two extremely influential research programs aimed to establish solid foundations for mathematics with the help of new formal logic. The logicism of Gottlob Frege and Bertrand Russell claimed that all mathematics can be shown to be reducible to logic. David Hilbert and his school in turn intended to demonstrate, using logical formalization, that the use of infinistic, set-theoretical methods in mathematics—viewed with suspicion by many—can never lead to finitistically meaningful but false statements and is thus safe. This came to be known as Hilbert's program.

These grand aims were shown to be impossible by applying the exact methods of logic to itself: the limitative results of Kurt Gödel, Alonzo Church, and Alan Turing in the 1930s revolutionized the whole understanding of logic and mathematics (the key papers are reprinted in [5]).

Panu Raatikainen is a fellow in the Helsinki Collegium for Advanced Study and a docent of theoretical philosophy at the University of Helsinki. His e-mail address is panu.raatikainen@helsinki.fi.

What Gödel proved in 1931 is that in any finitely presented system of mathematical axioms there are sentences that are true but that cannot be proved to be true in the system. Church showed in 1936 that there is no general mechanical method for deciding whether a given sentence is logically valid or not and, similarly, that there is no method for deciding whether a given sentence is a theorem of a given axiomatized mathematical theory. Such an impossibility proof required an exact mathematical substitute for the informal, intuitive notion of a mechanical procedure; Church used his own λ-definable functions. Turing arrived independently at the same results at the same time. Moreover, he gave a superior philosophical explication of the concept of mechanical procedure in terms of abstract imaginary machines, known today as Turing machines; this advance made it possible to prove absolute unsolvability results and to develop Gödel's incompleteness theorem in its full generality. This identification of the intuitive notion of mechanical method and an exact mathematical notion is usually called Church's thesis or, more properly, the Church-Turing thesis. It is the fundamental basis of all proofs of absolute unsolvability.

One of the greatest achievements of modern mathematical logic was certainly the proof by Yuri Matiyasevich in 1970, based on earlier work by Julia Robinson, Martin Davis, and Hilary Putnam, that the tenth problem of Hilbert's famous list of open mathematical problems from 1900 is in fact unsolvable; i.e., there is no general method for deciding whether a given Diophantine equation has a solution or not [11]. This result implies that in any axiomatized theory there exist Diophantine

equations that have no solution but cannot be proved in the theory to have no solution.

However, it is now a widespread view, especially in computer science circles, that certain variants of incompleteness and unsolvability results by the American computer scientist Gregory Chaitin are the last word in this field. These variants are claimed to both explain the true reason for Gödel's incompleteness theorem and to be the ultimate, or the strongest possible, incompleteness results. Chaitin's results emerge from the theory of algorithmic complexity or program-size complexity (also known as "Kolmogorov complexity"); Chaitin himself was, in fact, one of the founders of the theory.

The classical work on unsolvability dealt solely with solvability in principle: one abstracted from the practical limits of space and time and required only finiteness. From the late 1950s onward, however, more and more attention has been paid to different kinds of complexity questions—at least in part because of the emergence of computing machines and the practical resource problems that accompanied them. In logic and computer science various different notions of complexity have been studied intensively. First, *computational complexity* measures the complexity of a problem in terms of resources, such as space and time, required to solve the problem relative to a given machine model of computation. Second, *descriptive complexity* analyzes the complexity of a problem in terms of logical resources, such as the number of variables, the kinds of quantifiers, or the length of a formula required to define the problem. And finally, by the *algorithmic complexity*, or the *program-size complexity* (or Kolmogorov complexity), of a number or a string, one means the size of the shortest program that computes as output that number or string.

Theory of Algorithmic Complexity

The basic idea of the theory of algorithmic complexity was suggested in the 1960s independently by Ray J. Solomonoff, Andrei N. Kolmogorov, and Gregory Chaitin. Solomonoff used it in his computational approach to scientific inference, Kolmogorov aimed initially to give a satisfactory definition for the problematic notion of a random sequence in probability theory, and Chaitin first studied the program-size complexity of Turing machines for its own sake. Kolmogorov went on to suggest that this notion also provides a good explication of the concept of the information content of a string of symbols. Later Chaitin followed him in this interpretation. Consequently, the name "algorithmic information content" has frequently been used for program-size complexity, and the whole field of study is very often called "algorithmic information theory" ([10] is a comprehensive survey of the theory and its applications).

Chaitin was active in developing this approach into a systematic theory (although one should not ignore the important contributions by many others). From the 1970s onwards Chaitin's interest has focused more and more on incompleteness and unsolvability phenomena related to the notion of program-size complexity. Indeed, he now says that "the most fundamental application" of the theory is in "the new light that it sheds on the incompleteness phenomenon" (*The Unknowable*, pp. 86–7).

It was known from the beginning that program-size complexity is unsolvable. Chaitin, however, made in the early 1970s an interesting observation: Although there are strings with arbitrarily large program-size complexity, for any mathematical axiom system there is a finite limit c such that in that system one cannot prove that any particular string has a program-size complexity larger than c [1]. Later Chaitin attempted to extend his "information-theoretic" approach to incompleteness theorems in order to obtain "the strongest possible version of Gödel's incompleteness theorem" ([3], p. v). For this purpose he has defined a specific infinite "random" sequence Ω.

As was noted, one of the major sources that originally motivated the development of the theory of program-size complexity, especially in Kolmogorov's case, was a problem in the theory of probability, viz. that of giving a precise and plausible definition for the notion of a random string. The problem is related to the paradox of randomness, which may be explained as follows: Assume we are given two binary strings of 20 digits each, and we are informed that they were both obtained by flipping a coin. Let these two strings be:

$$x = 00000000000000000000$$

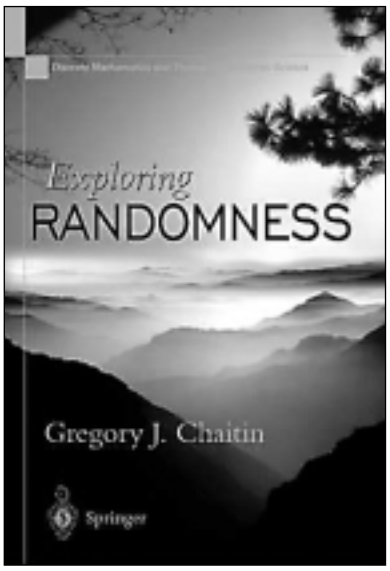
and

$$y = 01001110100111101000.$$

Now according to the standard theory of probability, these strings are equally probable. And yet intuitively one tends to think that x cannot possibly be a randomly generated string—there is too much regularity in it—whereas y appears to be genuinely irregular and random and may well be the result of a toss of a coin. The algorithmic theory of randomness explicates this idea of regularity with the help of Turing machine programs. One considers a finite string as regular, or nonrandom, if it can be generated by a simple program, i.e., if its program-size complexity is considerably smaller than its length. Accordingly, a finite string is defined to be random if its program-size complexity is roughly equal to its

length, i.e., if it cannot be compressed to a shorter program. (Note that this notion is relative to a chosen programming language or coding system; a finite string may be random in one but nonrandom in another.)

Extending this approach to infinite strings turned out to be, however, more difficult than was thought. Kolmogorov's first idea was that an infinite string be considered random if all of its finite initial segments are random. But Per Martin-Löf showed that this definition does not work and then gave a more satisfactory definition in measure-theoretic terms. In 1975 Chaitin presented a definition (which is equivalent to Martin-Löf's definition) in terms of program-size complexity: An infinite string is defined to be random if the program-size complexity of an initial segment of length n does not drop arbitrarily far below n [2]. One should add that it is not indisputable that this really provides in all respects an unproblematic explication of the notion of randomness.



Also in 1975 Chaitin presented for the first time his (since then much-advertised) number Ω: it is the halting probability of the universal Turing machine U, i.e., the probability that U halts when its binary input is chosen randomly bit by bit, such as by flipping a coin. The infinite string Ω is, according to the above definition, random [2]. Somewhat analogously to his earlier incompleteness result, Chaitin has demonstrated that no axiomatic mathematical theory enables one to determine infinitely many digits of Ω ([3], [4]; cf. [6], [8]).

Chaitin's New Approach via LISP Programs

This is the general theoretical background of the books under review. How do these two new books by Chaitin relate to these older works? In terms of results there is hardly anything new compared to the older work by Chaitin and others reviewed above. Rather, these books aim to popularize that work. In *The Unknowable* the emphasis is on the incompleteness phenomena related to program-size complexity. *Exploring Randomness* aims to explain the program-size complexity approach to randomness.

What is new is Chaitin's approach via LISP-programming; he has "translated" his own earlier work, which was in terms of abstract, idealized Turing machines, into actual programs in the LISP computer language. Well, not exactly: according to Chaitin, no existing programming language provides exactly what is needed, so he invented a new version of LISP. Chaitin begins *The Unknowable* by saying that what is new in the book is the following: "I compare and contrast Gödel's, Turing's and my work in a very simple and straightforward manner using LISP" (p. v). According to Chaitin this book is a "prequel" to his previous book, *The Limits of Mathematics* (Springer-Verlag, 1998), and is an easier introduction to his work on incompleteness. In *Exploring Randomness* Chaitin in turn writes that "[t]he purpose of this book is to show how to program the proofs of the main theorems about program-size complexity, so that we can see the algorithms in these proofs running on the computer" (p. 29).

Such an approach may be attractive for programming enthusiasts and engineers, but for the rest of us its value is less clear. It is quite doubtful whether it manages to increase the understanding of the basic notions and results and whether it really makes the fundamental issues, which are rather theoretical and conceptual, more accessible. All these can be, and have been, explained quite easily and elegantly in terms of simply describable Turing machines, and it is questionable that it is really easier to understand them by first learning Chaitin's specially modified LISP and then programming them. And after all, the key point here is that there is no program for deciding the basic properties—that they are not programmable. In *The Unknowable* (p. 27) Chaitin says that "[r]eaders who hate computer programming should skip directly to Chapter VI"—that is, should skip half of the book (and similarly with *Exploring Randomness*). What is left is two popular surveys of the field.

What is totally missing from Chaitin's accounts is the link between his particular programming language and the intuitive notion of mechanical procedure, that is, an analogue of the Church-Turing thesis. Turing's conceptual analysis of what a mechanical procedure is and the resulting Church-Turing thesis are indispensable for the proper understanding of the fundamental unsolvability results: only the thesis gives them their absolute character (in contradistinction to unsolvability by some fixed, restricted methods). Consequently, without some extra knowledge, the theoretical relevance of the limitations of the LISP programs that Chaitin demonstrates may remain unclear to the reader: one may wonder whether perhaps some other programming language would do better. This is a serious weakness of these presentations as first introductions to the unsolvability phenomena.

Problematic Philosophical Conclusions

The most controversial parts of Chaitin's work are certainly the highly ambitious philosophical conclusions he has drawn from his mathematical

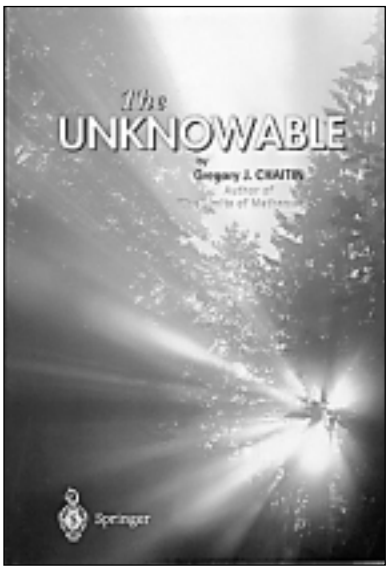
work. Recall that according to Chaitin the most fundamental application of the theory is in the new light that it sheds on the incompleteness phenomenon. He writes: "Gödel and Turing were only the tip of the iceberg. AIT [algorithmic information theory] provides a much deeper analysis of the limits of the formal axiomatic method. It provides a deeper source of incompleteness, a more natural explanation for the reason that no finite set of axioms is complete" (*Exploring Randomness*, p. 163).

But why does Chaitin think so? It is because he interprets his own variants of incompleteness theorems as follows: "The general flavor of my work is like this. You compare the complexity of the axioms with the complexity of the result you're trying to derive, and if the result is more complex than the axioms, then you can't get it from those axioms" (*The Unknowable*, p. 24). Or, in other words: "my approach makes incompleteness more natural, because you see how what you can do depends on the axioms. The more complex the axioms, the better you can do" (*The Unknowable*, p. 26).

But appearances notwithstanding, this is simply wrong. In fact, there is no direct dependence between the complexity of an axiom system and its power to prove theorems. On the one hand, there are extremely complex systems of axioms that are very weak and enable one to prove only trivial theorems. Consider, for example, an enormously complex finite collection of axioms with the form $n < n+1$; even the simple theory consisting of the single generalization "for all x, $x < x+1$" can prove more. On the other hand, there exist very simple and compact axiom systems that are sufficient for the development of all known mathematics (e.g., the axioms of set theory) and that can in particular decide many more cases of program-size complexity than some extremely complex but weak axiom systems (such as the one above). Moreover, it is possible for two theories to differ considerably in strength or complexity but nevertheless be able to decide exactly the same facts about program-size complexity and have the same Chaitinian finite limit c [12]. Analogously, Chaitin's claim with respect to Ω that "an N-bit formal axiomatic system can determine at most N bits of Ω" (*The Unknowable*, p. 90) is again not true for related reasons [13].

It has been shown conclusively (see [9], [12], [13]) that Chaitin's philosophical interpretations of his work are unfounded and false; they are based on various fatal confusions. And thus we have all the more reason for doubting the claim that his approach can explain the true source of the incompleteness and unsolvability theorems. As his philosophical interpretations fall, so does this claim. Chaitin's findings are not without interest, but their relevance for the foundations of mathematics has been greatly exaggerated.

Further, Chaitin has often stated that he has shown that mathematical truth is random: "But the bits of this number Ω, whether they're 0 or 1, are mathematical truths that are true by accident! …they're true by no reason…there is no reason that individual bits are 0 or 1!" (*Exploring Randomness*, pp. 23–4) This is false too. The individual bits of Ω are 0 or 1 depending on whether certain Turing machines halt or not—that is the reason. It is an objective matter of fact; the truth here is completely determined, and Chaitin's interpretation of the situation is quite misleading.



Chaitin also claims that Ω is "maximally unknowable" and that in his setting one gets incompleteness and unsolvability "in the worst possible way" (*Exploring Randomness*, p. 19). But contrary to what Chaitin's own interpretations suggest, his results can in fact be derived as quite easy corollaries of Turing's classical unsolvability result and are not essentially stronger than it. Moreover, there are many incompleteness and unsolvability results in the literature of mathematical logic that are in various ways stronger than Chaitin's results; many of them also have a much more natural mathematical content [13].

Chaitin, however, seems to be quite indifferent to all such criticism. Instead of trying to seriously answer it in any way, he sweeps all such problems under the carpet with rather cheap rhetoric: "AIT is tremendously revolutionary; it is a major paradigm shift, which is why so many people find the philosophical conclusions that I draw from my theory to be either incomprehensible or unpalatable" (*Exploring Randomness*, p. 161). Or: "AIT is a drastic paradigm shift, and as such, obeys Max Planck's dictum that major new scientific ideas never convince their opponents, but instead are adopted naturally by a new generation that grows up with them and takes them for granted and that have no personal stake nor have built careers on older, obsolete viewpoints" (*Exploring Randomness*, p. 163).

But wouldn't it be conceivable that the true reason for some resistance is not dogmatic prejudice but that his conclusions are untenable because they are very weakly justified and even contradict various logico-mathematical facts? Creative and original as Chaitin has been, it is sometimes quite disturbing that he seems totally ignorant of large parts of mathematical logic relevant to the issues

he is dealing with. It is regrettable that Chaitin does not respond to criticism of his work but simply evades difficult questions and keeps on writing as if they did not exist. Chaitin's own attitude begins to resemble the dogmatism he accuses his opponents of.

At worst, Chaitin's claims are nearly megalomaniacal. What else can one think of statements such as the following?: "AIT will lead to the major breakthrough of 21st century mathematics, which will be information-theoretic and complexity based characterizations and analyses of what is life, what is mind, what is intelligence, what is consciousness, of why life has to appear spontaneously and then to evolve" (*Exploring Randomness*, p. 163).

Problems of Popularization

The historical surveys of the theory of program-size complexity that Chaitin gives are sometimes rather distorted. Some have even complained that Chaitin is "rewriting the history of the field" and "presenting himself as the sole inventor of its main concepts and results" [7]. This complaint also fits to a considerable degree the present books. They are quite idiosyncratic.

The style of these books is very loose and popular. Large parts of the text are directly transcribed from oral lectures and include asides like "Thanks very much, Manuel! It's a great pleasure to be here!" It is perhaps a matter of taste whether one finds this entertaining or annoying. Personally, I don't think that this is a proper style for books in a scientific series. It certainly does not decrease the sloppiness of the text.

The books bring together popular and introductory talks given on different occasions, and some of this material has already appeared elsewhere. There is also a lot of redundancy and overlap between the books. Both books (as well as the earlier *The Limits of Mathematics*) start with a loose and not very reliable historical survey—Chaitin himself calls it "a cartoon summary"—beginning with Cantor's set theory, going through Gödel's and Turing's path-breaking results, and culminating, unsurprisingly, in Chaitin's own work. All three books then present an introduction to LISP and Chaitin's modification of it. Both *The Unknowable* and *Exploring Randomness* contain a more theoretical section on algorithmic information theory and randomness. And finally, both books end with rather speculative remarks on the future of mathematics. Would it have been better to do some editing and publish just one book instead of three?

To a considerable degree, *Exploring Randomness* and *The Unknowable* just recycle the same old ideas. Consequently, for those with some knowledge of this field, these books do not offer anything really new. For those with no previous knowledge of these matters, it is questionable whether these books are really a good place to start.

(There is an errata for *Exploring Randomness* on Chaitin's home page: `http://www.cs.auckland.ac.nz/CDMTCS/chaitin/`).

References

[1] Gregory J. Chaitin, Randomness and mathematical proof, *Sci. Amer.* **232**:5 (1975), 47–52.

[2] ____ , A theory of program size complexity formally identical to information theory, *J. Assoc. Comput. Mach.* **22** (1975), 329–340.

[3] ____ , *Algorithmic Information Theory*, Cambridge University Press, Cambridge, 1987.

[4] ____ , Randomness in arithmetic, *Sci. Amer.* **259**:1 (1988), 80–85.

[5] Martin Davis (ed.), *The Undecidable*, Raven Press, New York, 1965.

[6] Jean-Paul Delahaye, Chaitin's equation: An extension of Gödel's theorem, *Notices Amer. Math. Soc.* **36**:8 (1989), 984–987.

[7] Peter Gacs, Review of Gregory J. Chaitin, Algorithmic Information Theory, *J. Symbolic Logic* **54** (1989), 624–627.

[8] Martin Gardner, Mathematical games: The random number Omega bids fair to hold the mysteries of the universe, *Sci. Amer.* **241**:5 (1979), 20–34.

[9] Michiel Van Lambalgen, Algorithmic information theory, *J. Symbolic Logic* **54** (1989), 1389–1400.

[10] Ming Li and Paul Vitanyi, *An Introduction to Kolmogorov Complexity and Its Applications*, Springer-Verlag, New York, 1993.

[11] Yuri V. Matiyasevich, *Hilbert's Tenth Problem*, MIT Press, Cambridge, MA, 1993.

[12] Panu Raatikainen, On interpreting Chaitin's incompleteness theorem, *J. Philos. Logic* **27** (1998), 269–586.

[13] ____ , Algorithmic information theory and undecidability, *Synthese* **123** (2000), 217–225.