# Incompleteness, Complexity, Randomness and Beyond

CRISTIAN S. CALUDE
*Department of Computer Science, University of Auckland, Auckland, New Zealand; E-mail: cristian@cs.auckland.ac.nz*

> The Library is composed of an ... infinite number of hexagonal galleries ... [it] includes all verbal structures, all variations permitted by the twenty-five orthographical symbols, but not a single example of absolute nonsense. ... These phrases, at first glance incoherent, can no doubt be justified in a cryptographical or allegorical manner; such a justification is verbal and, ex hypothesi, already figures in the Library. ... The certitude that some shelf in some hexagon held precious books and that these precious books were inaccessible seemed almost intolerable. A blasphemous sect suggested that ... all men should juggle letters and symbols until they constructed, by an improbable gift of chance, these canonical books ... but the Library is ... useless, incorruptible, secret.
>
> *Jorge Luis Borges, "The Library of Babel"*

**Abstract.** Gödel's Incompleteness Theorems have the same scientific status as Einstein's principle of relativity, Heisenberg's uncertainty principle, and Watson and Crick's double helix model of DNA. Our aim is to discuss some new faces of the incompleteness phenomenon unveiled by an information-theoretic approach to randomness and recent developments in quantum computing.

**Key words:** complexity, incompleteness, Omega Number, quantum computing, randomness, Turing barrier

## 1. Incompleteness and Uncomputability

Interest in *incompleteness* dates from early times. Incompleteness was an important issue for Aristotle, Kant, Gauss, Kronecker, but it didn't have a fully explicit, precise meaning before the works of Hilbert and Ackermann, Whitehead and Russell, Gödel and Turing.

In a famous lecture before the *International Congress of Mathematicians* (Paris, 1900), David Hilbert expressed his conviction of the solvability of every mathematical problem: "Wir müssen wissen. Wir werden wissen." (We must know. We will know.). Hilbert highlighted the need to clarify the methods of mathematical reasoning, using a formal system of explicit assumptions, or axioms. Hilbert's vision was the culmination of 2,000 years of mathematics going back to Euclidean geometry. He stipulated that such a formal axiomatic system should be both 'consistent' (free of contradictions) and 'complete' (in that it represents all the truth).

In their monumental *Principia Mathematica* (1925–1927), Whitehead and Russell developed the first coherent and precise formal system aimed at describing the

*Minds and Machines* **12:** 503–517, 2002.

whole of mathematics. Although *Principia Mathematica* held great promise for Hilbert's demand, it fell short of actually proving its completeness.

After proving the completeness of the system of predicate logic in his doctoral dissertation (1929), Gödel continued the investigation of the completeness problem for more comprehensive formal systems, especially systems encompassing all known methods of mathematical proof. In 1931 (see Feferman et al., 1990) Gödel proved his famous *First Incompleteness Theorem*, which in modern terms reads:

> *any computably enumerable, consistent formal axiomatic system containing elementary arithmetic is* incomplete, *that is, there exist true, but unprovable (within the system) statements*.

The system is computably enumerable if its 'theorems' can be listed by a Turing machine. Informally, the set of axioms and deduction rules generates all 'theorems'; for example, we cannot take as axioms all true statements about natural numbers as this set is not computably enumerable. The condition that the system contains elementary arithmetic is also essential. For example, Euclidean geometry, which makes statements only about points, circles and lines in general, does not satisfy this condition, hence it might be complete; and, indeed, it is complete as Tarski has proved. The flat nature of Euclidean geometry plays no role here, non-Euclidean geometries are also complete.

This result together with the Second Incompleteness Theorem (which states that the consistency of the axioms cannot be proved within the system) ended a hundred years of attempts to establish axioms that would put mathematics on an axiomatic basis. Gödel's Incompleteness Theorem does not destroy the fundamental idea of formalism, but suggests that (a) mathematics will be described by many formal systems as opposed to a universal one, and (b) a more sophisticated and comprehensive form of formal system than that envisaged by Hilbert is required (see also Post, 1965).

Anticipating resistance to his conclusions Gödel wrote his papers very carefully. Speculating on his extreme caution, Feferman et al. (1984) stated that Gödel "could have been more centrally involved in the development of the fundamental concepts of modern logic – *truth* and *computability* – than he was". Gödel took pains to convince various people of the validity of his assertions and results, but he avoided any public debate and considered his results to have been accepted by those whose opinion mattered to him. P. Finsler, E. Post and E. Zermelo were concerned with priority issues, while C. Perelman, M. Barzin, J. Kuczyński asserted that Gödel had in fact discovered another *antinomy*; see Dawson (1997). Unlike the others, Post expressed "the greatest admiration" for Gödel's work, conceding that "after all it is not ideas but the execution of ideas that constitute[s] ... greatness". Gödel's result provoked Hilbert's anger, but he apparently accepted its correctness (cf. Dawson, 1997). Hilbert never cited Gödel's work.

The reactions of two great philosophers are also of interest. Wittgenstein's negative comments (dated 1938 and posthumously published in "Remarks on the foundations of mathematics" in Wittgenstein (1964)) are now generally considered an

embarrassment in the work of a great philosopher. Russell realized the importance of Gödel's work, but expressed his ongoing puzzlement in a rather ambiguous way in a letter dated 1 April 1963 (addressed to L. Henkin; see Dawson, 1997): *Are we to think that* $2+2$ *is not 4, but* $4.001$*?* Following the same source, Gödel remarked (in a letter addressed to A. Robinson) that "Russell evidently misinterprets my result; however he does so in a very interesting manner ... ".

In the long run Gödel's interpretations of incompleteness prevailed: the Incompleteness Theorems neither rejected the notion of formal system (quite the opposite) nor caused despair over the imposed limitations; they just re-affirmed the creative power of human reason. In Post's celebrated words: "mathematical proof is [an] essentially creative [activity]."

In 1936 Turing (1936/1937) showed the undecidability of the *Halting Problem*, the question of whether a given computer program will eventually halt:

> *no mechanical procedure (therefore no formal axiomatic theory) can solve the Halting Problem.*

These two results have very deep connections. To understand them we need to examine a very delicate notion: randomness.

## 2. Randomness

What is randomness? Are there random events in nature? Are there laws of randomness? Even today, these questions stir controversy.

> *I am convinced that the vast majority of my readers, and in fact the vast majority of scientists and even nonscientists, are convinced that they know what 'random' is. A toss of a coin is random; so is a mutation, and so is the emission of an alpha particle. ... Simple, isn't it?* said Kac (1983).

Well, no! Kac knew very well that randomness, the very stuff of life, could be called many things, but not simple. The fact that maintaining perfect order is difficult surprises no one, but it may come as something of a "revelation" that perfect disorder is beyond reach. People, even experts, perform poorly when dealing with randomness. The "gambler fallacy" is a classical example: the common belief that after a sequence of losses in a game of chance there will probably follow a sequence of gains is false. Various explanations have been suggested: according to one of them, the human cognitive and psychological constitution, trained over the years to look for patterns and trends (even where there are none) is "blind" when it comes to randomness.

Randomness is a most troubling concept — it is hard not only to attain but also to define or even to imagine in spite of the fact that there *have been heroic efforts to understand randomness* (cf. Efron cited in Kolata, 1986).

Most books on probability theory do not even attempt to define randomness: It's like the concept of a point in geometry books. According to Beltrami (1999):

*The subject of probability begins by assuming that some mechanism of uncertainty is at work giving rise to what is called randomness, but it is not necessary to distinguish between chance that occurs because of some hidden order that may exist and chance that is the result of blind lawlessness. This mechanism, figuratively speaking, churns out a succession of events, each individually unpredictable, or it conspires to produce an unforeseeable outcome each time a large ensemble of possibilities is sampled.*

Randomness means the absence of order or pattern. In an extreme sense there is no such notion as "true randomness". As an illustration note that any sequence (the simplest mathematical infinite object) has some kind of order, regularity. For example, van der Waerden (1927) proved that *in all binary sequences at least one of the two symbols must occur in arithmetical progressions of every length*. Many other patterns common to all sequences have been subsequently discovered.

Randomness as pattern-breaking (within a given context) can be viewed in (at least) four ways:

- Randomness as the output of a "chance" process: patterns are specified by a set of very small probability.
- Randomness as the result of "mixing": far-from-equilibrium-states specify the patterns.
- Randomness as "mimicking chance": statistical tests specify the patterns.
- Randomness as a measure of incompressibility: low complexity (short) programs specify the patterns.

In what follows, we will focus on the *information-theoretic approach to randomness* proposed by *algorithmic information theory*. To this aim we will work with a fixed alphabet $\Sigma$ and a universal self-delimiting Turing machine (for short, universal Chaitin machine) $U$ processing strings (over $\Sigma$) into strings. Self-delimiting means that no halting program is a prefix of another. In this context universality is a stronger property than classical (Turing) universality: not only can the universal machine simulate every other machine, but the simulation is done in the most economical way. This means that the program-size complexity induced by $U$, $H_U(x)$, defined as the length of the shortest program which on $U$ produces $x$ (formally, $H_U(x) = \min\{|w| \mid U(w) = x\}$) is asymptotical optimal. That is, for every Chaitin machine $C$, there is a constant const such that for every string $x$ we have $H_U(x) \leq H_C(x) + \text{const}$.

There are various equivalent ways to define the notion of (algorithmic) random sequence: measure-theoretic definitions (Martin-Löf, 1966a, b; Solovay, 1975), information-theoretical definitions (Chaitin, 1975; Schnorr), topological definitions (Hertling and Weihrauch, 1998). For example, an infinite sequence $\mathbf{x} = x_1x_2 \ldots x_n \ldots$ is *Chaitin-random* if the difference between the complexity of a prefix of length $n$ and the length itself tends to infinity (formally, $\lim_{n\to\infty} H_U(x_1x_2 \ldots x_n) - n = \infty$).

A real $\alpha$ is *random* if its binary expansion is a random (infinite) sequence (Chaitin, 1975); the choice of base is irrelevant (Calude and Jürgensen, 1994; Hert-

ling and Weihrauch, 1998; Staiger, 1999). Random reals share many properties naturally associated with randomness:

- a random real has maximum entropy,
- no random real is computable,
- the digits of a random real are 'generated' in an unpredictable way,
- global disorder contrasts with local total order (any pattern appears).

## 3. Information-Theoretic Incompleteness

*Is there any relation between randomness and incompleteness*? The answer is *affirmative* and one possibility for revealing such relations is to look at a special class of reals – the *computable enumerable reals* (see Soare, 1969).

Turing's argument was based on computable real numbers. A real is *computable* if there is a computable function for calculating its digits one by one (see Rice, 1954). There are programs for calculating $\pi$, $e$, $\sqrt{3}$, $\log_2 3$, all rationals, all algebraic reals, and in fact all "natural" constants, but it is a bit surprising that *nearly all real numbers are not computable*.

A real $\alpha$ is *computably enumerable* (*c.e.*) if it is the limit of a computable, increasing, converging sequence of rationals. In contrast with the case of a computable real, whose digits are given by a computable function, during the process of approximation of a c.e. real one may never know how close one is to the final value. Specker (1949) gave the first example of a *convergent, computable sequence of rationals which does not converge computably*, hence its limit is a *c.e. real which is not computable*.

In 1975 a more modern version of the Halting Problem emerged. Chaitin (1975) introduced the probability that an arbitrary universal Chaitin machine will eventually halt:

$$\Omega_U = \sum_{U(x)\ \text{stops}} 2^{-|x|}.$$

The number $\Omega_U$ is a probability because of Kraft's inequality (which applies to the set of halting programs of the self-delimiting machine $U$). Chaitin's Omega reals share two apparently irreconcilable properties: 'algorithmic randomness' and 'computable enumerability'. Note also that c.e. and random reals have many other interesting properties; for example, they are weak truth-table-complete, but not truth-table-complete (Calude and Nies, 1997).

Each $\Omega_U$ depends on the choice of $U$, so there is not just one Omega (as there is only one $\pi$), but a class of Omegas. This observation leads to Solovay's question (Solovay, 1975): Are there random and computably enumerable real numbers other than Omegas? The answer is *negative*, and the proof is constructive, (cf. Calude et al., 2001; Slaman, personal communication, 14 December 1998; Kučera and Slaman, 2001):

*Let $\alpha \in (0, 1)$. The following conditions are equivalent:*

1. *The real $\alpha$ is c.e. and random.*
2. *The real $\alpha$ is the halting probability of some universal Chaitin machine $U$, $\alpha = \Omega_U$.*

To make the discussion more concrete we will formulate all results relative to $ZFC$, Zermelo–Fraenkel set theory with choice; all theorems hold true under more general conditions. *The First Information-theoretic Incompleteness Theorem* (Chaitin, 1975) is:

*Let $U$ be a universal Chaitin machine. Then $ZFC$, if arithmetically sound, can prove only finitely many statements of the form "$H_U(x) > m$".*

In fact, *there is a constant $c > 0$ such that $ZFC$ cannot prove the statement "$H_U(x) > m$" if $m > H_U(ZFC) + c$.* So, all true statements "$H_U(x) > m$" (an infinite set) are unprovable in $ZFC$. Recognizing high complexity is a difficult task even for $ZFC$. The difficulty depends upon the choice of $U$: some $U$'s are worse than others. Raatikainen (1998) has shown that *there exists a universal Chaitin machine $U$ so that $ZFC$, if arithmetically sound, can prove no statement of the form "$H_U(x) > n$".* It follows that $ZFC$, if arithmetically sound, can prove no (obviously, true) statement of the form "$H_U(x) > 0$".

Chaitin's *Second Information-theoretic Incompleteness Theorem* reads:

*Let $U$ be a universal Chaitin machine. If $ZFC$ is arithmetically sound, then $ZFC$ can determine the value of only finitely many bits of $\Omega_U$.*

We can explicitly compute a bound on the number of bits of $\Omega_U$ which $ZFC$ can determine, but the bound *is not computable*. For example, Chaitin (1997) has constructed a universal Chaitin machine $U_{\text{Lisp}}$ and a theory $T$ such that $T$ can determine the value of at most $H_{U_{\text{Lisp}}}(T) + 15,328$ bits of $\Omega_U$.

Can we 'find out' the (finitely many) bits which $ZFC$ can determine?

For every c.e. and random real $\alpha$ we can construct a universal Chaitin machine $U$ such that $\alpha = \Omega_U$ and $ZFC$ is able to determine finitely (but as many as we want) bits of $\Omega_U$. Solovay (2000) went in the opposite direction by showing that:

*We can effectively construct a universal Chaitin machine $U_{Solovay}$ such that $ZFC$, if arithmetically sound, cannot determine any single bit of $\Omega_{U_{Solovay}}$.*

Chaitin's Second Information-theoretic Incompleteness Theorem holds true for any *universal* Chaitin machine while Solovay constructed a *specific* machine. A Chaitin machine for which Peano Arithmetic can prove its universality and $ZFC$ cannot determine more than the initial block of 1's of the binary expansion of its halting probability will be called *Solovay machine*. Which c.e. and random reals are halting probabilities of Solovay machines? Calude (2002) proved the following result:

*Assume that $ZFC$ is arithmetically sound. Then, every c.e. and random real is the halting probability of a Solovay machine.*

For example, if $\alpha \in (3/4, 7/8)$ is c.e. and random, then in the worst case $ZFC$ can determine its first two bits (11), but no more. Assume that $ZFC$ is arithmetically sound. Then, every c.e. and random real $\alpha \in (0, 1/2)$ is the halting probability of a Solovay machine which cannot determine any single bit of $\alpha$. No c.e. and random real $\alpha \in (1/2, 1)$ has the above property.

A direct consequence of Solovay's result is the following constructive form of information-theoretic incompleteness:

*There exists a universal Chaitin machine $U_{Solovay}$ so that $ZFC$, if arithmetically sound, cannot prove the* true statement "The first bit of $\Omega_{U_{Solovay}}$ is 0".

In fact, a more general theorem is true:

*For every binary string $s = s_1 s_2 \ldots s_n$ we can effectively construct a Solovay machine $U_{Solovay}$ such that the binary expansion of $\Omega_{U_{Solovay}}$ has the string $0 s_1 s_2 \ldots s_n$ as prefix. Hence, the following statements*

"The $0^{th}$ binary digit of the expansion of $\Omega_{U_{Solovay}}$ is 0",
"The $1^{st}$ binary digit of the expansion of $\Omega_{U_{Solovay}}$ is $s_1$",
"The $2^{nd}$ binary digit of the expansion of $\Omega_{U_{Solovay}}$ is $s_2$",
$\vdots$
"The $n^{th}$ binary digit of the expansion of $\Omega_{U_{Solovay}}$ is $s_n$",

*are true but unprovable in $ZFC$.*

The information-theoretic version of incompleteness produces, in a constructive way, natural examples in which the axiomatic method is completely powerless. It also shows that incompleteness is pervasive, not accidental (for a different approach, see Calude et al., 1994). This may change the general view on the axiomatic method, one of the most powerful tools in mathematics. In Gödel's own words (see Gödel, 1964):

*... besides mathematical intuition there exists another (though only probable) criterion of truth of mathematical axioms, namely their fruitfulness in mathematics, and one may add, possibly also in physics ... The simplest case of an application of the criterion under discussion arises when some ... axiom has number-theoretical consequences verifiable by computation up to any given integer.*

Do these results have any impact on mathematics and/or the philosophy of mathematics? Opinions vary dramatically. H. Weyl described incompleteness in a pessimistic way, as a *constant drain on the enthusiasm* of pursuing scientific research; F. Dyson sees it in an optimistic way, as an insurance policy that science will go on forever. And, of course, some would argue that the work of the overwhelming majority of mathematicians and philosophers has been quite unaffected by the incompleteness results. One thing is certain: incompleteness has captured the interest of many. Many books and thousands of technical papers discuss it and its implications and the March 29, 1999 issue of *TIME* magazine has included

Gödel and Turing in its list of the twenty greatest twenty scientists and thinkers of the twentieth century.

## 4. Beyond

In this section we will discuss some recent results which in a way or another "challenge" the limits discussed above.

### 4.1. Computing a glimpse of an omega

Any attempt to compute the uncomputable or to decide the undecidable is without doubt challenging, but hardly new (see, for example, Marxen and Buntrock, 1990; Stewart, 1991; Casti, 1997). What about computing pieces of a concrete Omega number? First, note that any Omega number is not only uncomputable, but random, making the computing task even more demanding.

Computing lower bounds for Omega is not difficult: we just generate more and more halting programs. Are the bits produced by such a procedure exact? *Hardly*. If the first bit of the approximation happens to be 1, then sure, it is exact. However, if the provisional bit given by an approximation is 0, then, due to possible overflows, nothing prevents the first bit of Omega from being either 0 or 1. This situation extends to other bits as well. As we have already discussed, only an initial run of 1's may give exact values for some bits of Omega.

Another (more serious) difficulty preventing the computation of a fragment of an Omega is the following. *Globally*, if we can compute all bits of $\Omega_U$, then we can solve the Halting Problem for every program for $U$, and conversely, knowing all halting programs one can compute all bits of $\Omega_U$. *Locally*, given the first $N$ bits of Omega one can decide the halting status of all programs of length at most $N$. However, if we can solve for $U$ the Halting Problem for all programs up to $N$ bits long we might not get an exact value for any bit of $\Omega_U$ (less all values for the first $N$ bits). Reason: longer halting programs can contribute to the value of a "very early" bit of the expansion of $\Omega_U$. Using a "hybrid approach", programming combined with mathematical proofs, all halting programs of up to 84 bits for a concrete $U$ have been calculated (Calude et al., 2001). This information has been used to compute (only) the first 64 *exact* bits of $\Omega_U$:

0000001000000100000110001000011010001111110010111011101000010000.

### 4.2. Turing's barrier revisited

Classically, there are two equivalent ways to look at the mathematical notion of proof: (a) as a finite sequence of sentences strictly obeying some axioms and inference rules, (b) as a specific type of computation. Indeed, from a proof given

as a sequence of sentences one can easily construct a machine producing that sequence as the result of some finite computation and, conversely, given a machine computing a proof we can just print all sentences produced during the computation and arrange them in a sequence. A proof is an explicit sequence of reasoning steps that can be inspected at *leisure*; *in theory*, if followed with care, such a sequence either reveals a gap or mistake, or can convince a skeptic of its conclusion, in which case the theorem *is considered proven*.

This equivalence has stimulated the construction of programs which perform like *artificial mathematicians*.[1] From proving simple theorems of Euclidean geometry to the proof of the four-color theorem, these "theorem provers" have been very successful. Of course, this has sparked lots of controversies. *Artificial mathematicians* are far less ingenious and subtle than human mathematicians, but they surpass their human counterparts by being infinitely more patient and diligent. What about making errors? Are human mathematicians less prone to errors? This is a difficult question which requires more attention.

If a conventional proof is replaced by a "quantum computational proof" (or a proof produced as a result of a molecular experiment), then the conversion from a computation to a sequence of sentences may be impossible, e.g., due to the size of the computation. For example, a quantum machine could be used to create some proof that relied on quantum interference among all the computations going on in superposition. The quantum machine would say "your conjecture is true", but there will be no way to exhibit all trajectories followed by the quantum machine in reaching that conclusion. In other words, the quantum machine has the ability to check a proof, but it may fail to reveal any "trace" of how it did it. Even worse, any attempt to *watch* the inner working of the quantum machine (e.g. by "looking" at any information concerning the state of the on-going proof) may compromise forever the proof itself!

These facts may not affect the essence of mathematical objects and constructions (which have an autonomous reality quite independent of the physical reality), but they seem to have an impact on how we learn/understand mathematics (which is through the physical world). Indeed, our glimpses of mathematics seem to be "revealed" through physical objects, i.e. human brains, silicon computers, quantum Turing machines, etc., hence, according to Deutsch (1985), they have to obey not only the axioms and the inference rules of the theory, but the *laws of physics* as well.

The question of trespassing Turing's barrier, i.e. the possibility of solving a Turing undecidable problem, to compute an uncomputable function has been considered by various authors, (for example, Siegelmann, 1995; Copeland, 1999, 2000). Is there any hope for quantum (or DNA) computing to challenge the Turing barrier? According to Feynman's argument (see Feynman, 1985; a paper reproduced also in Hey, 1999) any quantum system can be simulated with arbitrary precision by a (probabilistic) Turing machine, so the answer seems to be *negative*. However, some recent tentative approaches promise a positive answer: for quantum approaches [2]

(see Calude et al., 1999, 2000; Etesi and Németi, 2002; Calude and Pavlov, 2002; Kieu 2001a, b; and for DNA methods, see Calude and Păun, 2001).

Is incompleteness affected? We need more understanding of the quantum world to be able to answer this question. One step toward a possible answer is to look at the quantum version of $\Omega$, the number $\Omega_q$ invented in 1995 by G. Chaitin, K. Svozil and A. Zeilinger (see Svozil, 1995; Williams and Clearwater, 2000; see also Kieu, 2001a; Vitányi, 2001). The number $\Omega_q$ is the probability amplitude with which a random quantum program halts on a self-delimiting universal quantum machine (hence, the halting probability of a self-delimiting universal quantum machine[3] is $|\Omega_q|^2$). For computing $\Omega_q$ only the quantum versions of classical bits in the domain of the quantum machine are allowed as inputs, so from the computability point of view $\Omega_q$ is an $\Omega$, hence all information-theoretic results remain unchanged. The halting probability of any quantum device capable of solving the Halting Problem (for classical Turing machines) will be an $\alpha$ number (as introduced in Becher et al., 2001), a random, but not c.e. real; the "incompleteness" derived from such a number has not (yet) been studied.

As is pointed out in Calude et al. (2000), all these theoretical proposals for trespassing Turing's barrier by a quantum machine may have a fairly low impact on current computer technology because for all practical purposes the halting computation has a non-zero, but very small chance of detection. So, when reality seems so far way from theory, why are we concerned with the latter? According to Landauer (1987) the answer is:

> *Because it is at the very core of science. . . . Information, numerical or otherwise, is not an abstraction, but it is inevitably tied to a physical representation. . . . the handling of information is inevitably tied to the physical universe, its contents and its laws.*

## 5. Digression: Is the Universe Lawless?

The hypothesis that the "Universe is lawful" is supported by our daily observations: the rhythm of day and night, the pattern of planetary motion, the regular ticking of clocks. It is a simple matter of reflection to point out some limits to this type of argument: the vagaries of weather, the devastation of earthquakes, or the fall of meteorites – all seem to be fortuitous. How can the same physical process, for example the spin of a roulette wheel, obey both the laws of chance and the laws of physics?

Perhaps a different hypothesis can better explain this type of behaviour. As our direct information refers to *finite* experiments, it is not out of the question to discover *local rules*, functioning on large, but finite scales, even if the global behaviour of the process is, or appears to be, random. The fact that the first billion digits of a random sequence are perfectly lawful, by being for instance exactly the first digits of the decimal expansion of $\pi$, does not change in any way the global property

of randomness. But, to "see" this *global randomness* we have to go beyond the finite; we have to access the *infinite*! The hypothesis stating that the "Universe is lawless", motivated by a crude model of the Universe based on the Omega number developed in Calude and Salomaa (1994) , was discussed in Calude and Meyerstein (1999): it tries to explain our *partial, incomplete and provisional* understanding of the Universe in a different way. But, of course, the adjectives "partial, incomplete and provisional" apply to the model itself!

**Acknowledgements**

We thank Greg Chaitin, Jack Copeland, Fred Kroon, Sergiu Rudeanu, Jerry Seligman and Karl Svozil for useful comments and criticism.

## Notes

[1]Other types of "reasoning" such as medical diagnosis or legal inference have been successfully modeled and implemented; see, for example, the British National Act which has been encoded in first-order logic and a machine has been used to uncover its potential logical inconsistencies.

[2]The solution proposed in Calude and Pavlov (2002) (see also Chown, 2002) is based on the "continuity" of quantum programs. Because of continuity, in deciding the halting/non-halting status of a non-halting machine, the quantum program "announces" (with a non-empty probability) the non-halting decision well before reaching it; hence, the challenge is to design a procedure that detects and measures this tiny, but non-empty signal. This was indeed achieved by exploiting some properties of the Brownian motion.

[3]Things are more complicated as the halt bit of the quantum machine might enter a superposition state and remain there while other parts of the output state describing the quantum machine continue to change. To settle the matter one has to perform a measurement.

## Bibliographical Comments

The list of references is by no means comprehensive and should be used in conjunction with bibliographies appearing in the cited works. One of the best presentations of Gödel's Incompleteness Theorem is Nagel and Newman (1986). The founders of algorithmic information theory are Solomonoff (1964), Kolmogorov (1965) and Chaitin (1966). Chaitin's monographs Chaitin (1992, 1999) deal with information-theoretic incompleteness. More on these issues can be found in Rozenberg and Salomaa (1994), Barrow (1998, 2000, 1995) Beltrami (1999), Zwirn (2000); for critical discussions see van Lambalgen (1989), Raatikainen (1998). Algorithmic information theory is presented in Chaitin (1990, 1997, 1999, 2000), Uspensky et al. (1990), Calude (2002), Li et al. (1997). For other interesting discussions on randomness see Kac (1983), Kolata (1986), Dembski (1998), Beltrami (1999), Hayes (2001), Svozil (1993), Denker et al. (1998). Easy to understand presentations include Bennett et al. (1979), Chaitin (1982, 2001), Casti (2000), Calude

et al. (1999), Calude (2000), Chown (2001, 2002), Rucker (1982). Recent literature inspired by Gödel's incompleteness include Auburn (2001), Doxiadis (2000). Gödel's life is discussed in Kleene (1976), Kreisel (1980), Dawson (1997), Wang (1996), Casti et al. (2000). The literature on quantum computing is growing at full speed: some book references are Gruska (1999), Williams et al. (2000), Calude et al. (2001).

## References


Auburn, D. (2001), *Proof. A Play*, New York: Faber & Faber.

Barrow, J.D. (1998), *Impossibility: The Limits of Science and the Science of Limits*, Oxford: Oxford University Press.

Barrow, J.D. (2000), 'Mathematical Jujitsu: Some Informal Thoughts About Gödel and Physics', *Complexity* 5, pp. 28–34.

Becher, V., Daicz, S. and Chaitin, G.J. (2001), 'A Highly Random Number', in C.S. Calude, M. J. Dinneen and S. Sburlan, eds., *Combinatorics, Computability and Logic, Proceedings of DMTCS'01*, London: Springer, pp. 55–68.

Beltrami, E. (1999), *What is Random? Chance and Order in Mathematics and Life*, New York: Springer.

Bennett, C.H. and Gardner, M. (1979), 'The Random Number Omega Bids Fair to Hold the Mysteries of the Universe', *Scientific American* 241, pp. 20–34.

Brisson, L. and Meyerstein, L.F. (1995), *Puissance et Limites de la Raison*, Paris: Les Belles Lettres.

Calude, C. S. (2002), *Information and Randomness. An Algorithmic Perspective*, Berlin: Springer.

Calude, C.S. (2000), 'A Glimpse into Algorithmic Information Theory', in P. Blackburn, N. Braisby, L. Cavedon and A. Shimojima, eds., *Logic, Language and Computation*, Volume 3, CSLI Series, Cambridge: Cambridge University Press, pp. 65–81.

Calude, C.S. (2002), 'Chaitin Ω Numbers, Solovay Machines and Incompleteness', *Theoret. Comput. Sci.* 28, pp. 269–277.

Calude, C.S. and Chaitin, G.J. (1999), 'Randomness Everywhere', *Nature* 400, pp. 319–320.

Calude, C.S., Dinneen, M.J. and C.-K. Shu, C.-K. (2002), 'Computing a Glimpse of Randomness', *Experimental Mathematics*; see also *CDMTCS Research Report* 167, 2001, 12 pp.

Calude, C.S., Dinneen, M.J. and Svozil, K. (1999), 'Counterfactual Effect, the Halting Problem, and the Busy Beaver Function' (Preliminary Version), *CDMTCS Research Report* 107, 8 pp.

Calude, C.S., Dinneen, M.J. and Svozil, K. (2000), 'Reflections on Quantum Computing', *Complexity* 6, pp. 35–37.

Calude, C.S., Hertling, P., Khoussainov, B. and Wang, Y. (2001), 'Recursively Enumerable Reals and Chaitin Ω Numbers', *Theoret. Comput. Sci.* 255 pp. 125–149.

Calude, C. and Jürgensen, H. (1994), 'Randomness as an Invariant for Number Representations', in H. Maurer, J. Karhumäki and G. Rozenberg, eds. *Results and Trends in Theoretical Computer Science*, Berlin: Springer, pp. 44–66.

Calude, C., Jürgensen, H. and Zimand, M. (1994), 'Is Independence an Exception ?', *Appl. Math. Comput.* 66, pp. 63–76.

Calude, C.S. and Meyerstein, F.W. (1999), 'Is the Universe Lawful ?', *Chaos, Solitons & Fractals* 10, pp. 1075–1084.

Calude, C. and Nies, A. (1997), 'Chaitin Ω Numbers and Strong Reducibilities', *J. Univ. Comput. Sci.* 3, pp. 1161–1166.

Calude, C.S. and Pavlov, B. (2002), 'Coins, Quantum Measurements, and Turing's Barrier', *Quantum Information Processing* 1(1-2), pp. 107–127.

Calude, C.S. and Păun, G. (2001), *Computing with Cells and Atoms*, London: Taylor & Francis Publishers.

Calude, C. and Salomaa, A. (1994), 'Algorithmically Coding the Universe', in G. Rozenberg and A. Salomaa, eds. *Developments in Language Theory*, Singapore: World Scientific, pp. 472–492.

Casti, J. (1997), 'Computing the Uncomputable', *The New Scientist*, 154/2082, p. 34.

Casti, J. (2000), *Five More Golden Rules: Knots, Codes, Chaos, and Other Great Theories of 20th-Century Mathematics*, New York: Wiley.

Casti, J. and DePauli, W. (2000), *Gödel. A Life in Logic*, Cambridge: Perseus.

Chaitin, G.J. (1966), 'On the Length of Programs for Computing Finite Binary Sequences', *J. Assoc. Comput. Mach.* 13, pp. 547–569. (Reprinted in: Chaitin (1990), pp. 219–244.)

Chaitin, G.J. (1975), 'A Theory of Program Size Formally Identical to Information Theory', *J. Assoc. Comput. Mach.* 22, pp. 329–340. (Reprinted in: Chaitin (1990), pp. 113–128)

Chaitin, G.J. (1982), 'Gödel's Theorem & Information', *International Journal of Theoretical Physics* 22, pp. 941–954.

Chaitin, G.J. (1990), *Algorithmic Information Theory*, Cambridge: Cambridge University Press (Third printing).

Chaitin, G.J. (1990), *Information, Randomness and Incompleteness, Papers on Algorithmic Information Theory*, Singapore: World Scientific, Singapore (Second edition).

Chaitin, G.J. (1992), *Information-Theoretic Incompleteness*, Singapore: World Scientific, Singapore.

Chaitin, G.J. (1997), *The Limits of Mathematics*, Singapore: Springer.

Chaitin, G.J. (1999), *The Unknowable*, Singapore: Springer.

Chaitin, G.J. (2000), *Exploring Randomness*, London: Springer.

Chaitin, G.J. (2001), *Conversations with a Mathematician*, London: Springer.

Chown, M. (2001), 'The Omega Man', *New Scientist* 10 March, pp. 29–31.

Chown, M. (2002), 'Smash and Grab', *New Scientist* 6 April, pp. 24–28.

Collins, G. P. (2001), 'Computing with Light', *Scientific American*, Aug. p. 12.

Copeland, J. (1999), 'The Modern History of Computing', in E.N. Zalta, ed. *The Stanford Encyclopedia of Philosophy* `http://plato.stanford.edu/entries/ computing-history/`.

Copeland, J. (2000), 'Narrow Versus Wide Mechanism: Including a Re-examination of Turing's Views on the Mind-machine Issue', *Journal of Philosophy* XCVI 1, pp. 5–32.

Dawson, J.W. Jr. (1984), 'Kurt Gödel in Sharper Focus', *The Mathematical Intelligencer* 6, pp. 9–17.

Dawson, J.W. Jr. (1997), *Logical Dilemmas. The Life and Work of Kurt Gödel*, Massachusetts: A K Peters.

Dembski, W. A. (1998), 'Randomness', in E. Craig, ed., *Routledge Encyclopedia of Philosophy*, Routledge, London, Vol. 8, pp. 56–59.

Denker, M., Woyczyński, M. W. and Ycart, B. (1998), *Introductory Statistics and Random Phenomena: Uncertainty, Complexity, and Chaotic Behavior in Engineering and Science,* Boston: Birkhäuser.

Detlefsen, M. (1998), 'Gödel's Theorems', in E. Craig, ed., *Routledge Encyclopedia of Philosophy*, Routledge, London, Vol. 4, pp. 106–119.

Deutsch, D. (1985), 'Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer', *Proceedings of the Royal Society London* A 400, pp. 97–119.

Doxiadis, A. (2000), *Uncle Petros & Goldback's Conjecture. A Novel about Mathematical Obsession*, New York: Bloomsbury.

Etesi, G. and Németi, I. (2002),. 'Non-Turing Computations via Malament-Hogarth Space-times', *International Journal of Theoretical Physics* 41, pp. 341–370.

Feferman, S. (1984), 'Kurt Gödel: Conviction and Caution', *Philos. Natur.* 21, pp. 546–562.

Feferman, S., Dawson, J., Jr., Kleene S.C., Moore, G.H., Solovay, R.M. and van Heijenoort, J., eds. (1990), *Kurt Gödel Collected Works*, Volume II, Oxford: Oxford University Press.

Feynman, R.P. (1985), 'Simulating Physics with Computers', *International Journal of Theoretical Physics* 11, pp. 11–20.

Hey, J.G., ed. (1999), *Feynman and Computation. Exploring the Limits of Computers*, Reading: Perseus Books.

Gödel, K. (1964), 'Russell's Mathematical Logic', in P. Benacerref and H. Putnam, eds. *Philosophy of Mathematics*, Englewood Cliffs, NJ: Prentice-Hall, pp. 211–232.

Gruska, J. (1999), *Quantum Computing*, London: McGraw-Hill.

Hayes, B. (2001), 'Randomness as a Resource', *American Scientist* 89, 4 July–August, pp. 300-304.

Hertling, P. and Weihrauch, K. (1998), 'Randomness Spaces', in K.G. Larsen, S. Skyum, and G. Winskel, eds. *Automata, Languages and Programming, Proceedings of the 25th International Colloquium, ICALP'98* (Aalborg, Denmark), Berlin: Springer, pp. 796–807.

Kac, M. (1983), 'What is Random ?', *American Scientist* 71, pp. 405–406.

Kieu, T.D. (2001a), 'Hilbert's Incompleteness, Chaitin's Ω Number and Quantum Physics', Los Alamos preprint archive `http://arXiv:quant-ph/0111062`, v1, 10 November.

Kieu, T. D. (2001b), 'Quantum Algorithm for the Hilbert's Tenth Problem', Los Alamos preprint archive `http://arXiv:quant-ph/0110136`, v2, 9 November.

Kleene, S.C. (1976), 'The Work of Kurt Gödel', *J. Symbolic Logic* 41, pp, 761–778; addendum *J. Symbolic Logic* 43, p. 613.

Kolata, G. (1986), 'What Does it Mean to be Random ?', *Science* 7, pp. 1068–1070.

Kolmogorov, A. N. (1965), 'Three Approaches for Defining the Concept of "Information Quantity"', *Problems Inform. Transmission* 1, pp. 3–11.

Kreisel, G. (1980), 'Kurt Gödel', *Biographical Memoirs of Fellows of the Royal Society of London* 26, pp. 149–224; corrigenda 27, p. 697, 28, p. 718.

Kučera, A. and Slaman, T.A. (2001), 'Randomness and Recursive Enumerability', *SIAM J. Comput.* 31, pp. 199–211.

van Lambalgen, M. (1989), 'Algorithmic Information Theory', *J. Symbolic Logic* 54, pp. 1389–1400.

Landauer, R. (1987), 'Computation: A Fundamental Physical View', *Physica Scripta* 35, pp. 88–95.

Li, M. and Vitányi, P. M. (1997), *An Introduction to Kolmogorov Complexity and Its Applications*, Berlin: Springer (Second edition).

Martin-Löf, P. (1966), *Algorithms and Random Sequences*, Nürnberg: Erlangen University.

Martin-Löf, P. (1966), 'The Definition of Random Sequences', *Inform. and Control* 9, pp. 602–619.

Marxen, H. and Buntrock, J. (1990), 'Attaching the Busy Beaver 5', *Bull EATCS* 40, pp. 247–251.

Nagel, E. and Newman, J. R. (1986), *Gödel's Proof*, New York: University Press (Second printing).

Post, E. ( 1965), 'Absolutely Unsolvable Problems and Relatively Undecidable Propositions: Account of an Anticipation', in M. Davis, ed., *The Undecidable*, New York: Raven Press, pp. 340–433.

Raatikainen, P. (1998), 'On Interpreting Chaitin's Incompleteness Theorem', *J. Philos. Logic* 27, pp. 569–586.

Rice, H. (1954), 'Recursive Reals', *Proc. Amer. Math. Soc.* 5, pp. 784–791.

Rozenberg, G. and Salomaa, A. (1994), *Cornerstones of Undecidability*, Englewood Cliffs, NJ: Prentice Hall.

Rucker, R. (1982), *Infinity and the Mind*, New York: Bantam.

Siegelmann, H. (1995), 'Computation Beyond the Turing Limit', *Science* 268, pp. 545–548.

Soare, R. I. (1969), 'Recursion Theory and Dedekind Cuts', *Trans. Amer. Math. Soc.* 140, pp. 271–294.

Solomonoff, R. J. (1964), 'A Formal Theory of Inductive Inference', Part 1 and Part 2, *Inform. and Control* 7, pp. 1–22, 224–254.

Solovay, R. M. (1975), *Draft of a paper (or series of papers) on Chaitin's work ... done for the most part during the period of Sept.–Dec. 1974*, New York: IBM Thomas J. Watson Research Center, 215, pp.

Solovay, R. M. (2000), 'A Version of Ω for Which $ZFC$ Cannot Predict a Single Bit', in C.S. Calude and G. Păun, eds., *Finite Versus Infinite. Contributions to an Eternal Dilemma*, London: Springer, pp. 323–334.

Specker, E. (1949), Nicht konstruktiv beweisbare 'Sätze der Analysis', *J. Symbolic Logic* 14, pp. 145–158.

Svozil, K. (1993), *Randomness & Undecidability in Physics*, Singapore: World Scientific.

Svozil, K. (1995), 'Halting Probability Amplitude of Quantum Computers', *J. UCS* 1, pp. 201–203.

Staiger, L. (1999), 'The Kolmogorov Complexity of Real Numbers', in G. Ciobanu and Gh. Păun, eds. *Proc. Fundamentals of Computation Theory*, Lecture Notes in Comput. Sci. No. 1684, Berlin: Springer, pp. 536-546.

Stewart, I. (1991), 'Deciding the Undecidable', *Nature* 352, pp. 664–665.

Turing, A. M. (1936/7), 'On Computable Numbers with an Application to the Entscheidungsproblem', *Proc. Amer. Math. Soc.* 42, pp. 230–265; a correction, 43, pp. 544–546.

Zwirn, H. (2000), *Les Limites de la Connaissance*, Paris: Odile Jacob.

Uspensky, V.A., Semenov, A. L. and Shen, A. Kh. (1990), 'Can an Individual Sequence of Zeros and Ones be Random ?', *Russian Math. Surveys* 45, pp. 121–189.

Vitányi, P.M. (2001), 'Quantum Kolmogorov Complexity Based on Classical Descriptions', *IEEE Trans. Inform. Theory* 47, pp. 2464–2479.

Wang, H. (1996), *A Logical Journey: From Gödel to Philosophy*, Cambridge: MIT Press.

Williams, C. P. and Clearwater, S. H. (2000), *Ultimate Zero and One*, New York: Copernicus.

Wittgenstein, L. (1964), 'Selections from "Remarks on the Foundations of Mathematics"', in P. Benacerref and H. Putnam (eds). *Philosophy of Mathematics: Selected Readings*, Princeton, NJ: Prentice-Hall, pp. 421–480.