Algorithmic Randomness, Quantum Physics, and Incompleteness

Cristian S. Calude
University of Auckland

Figure 1: New Zealand

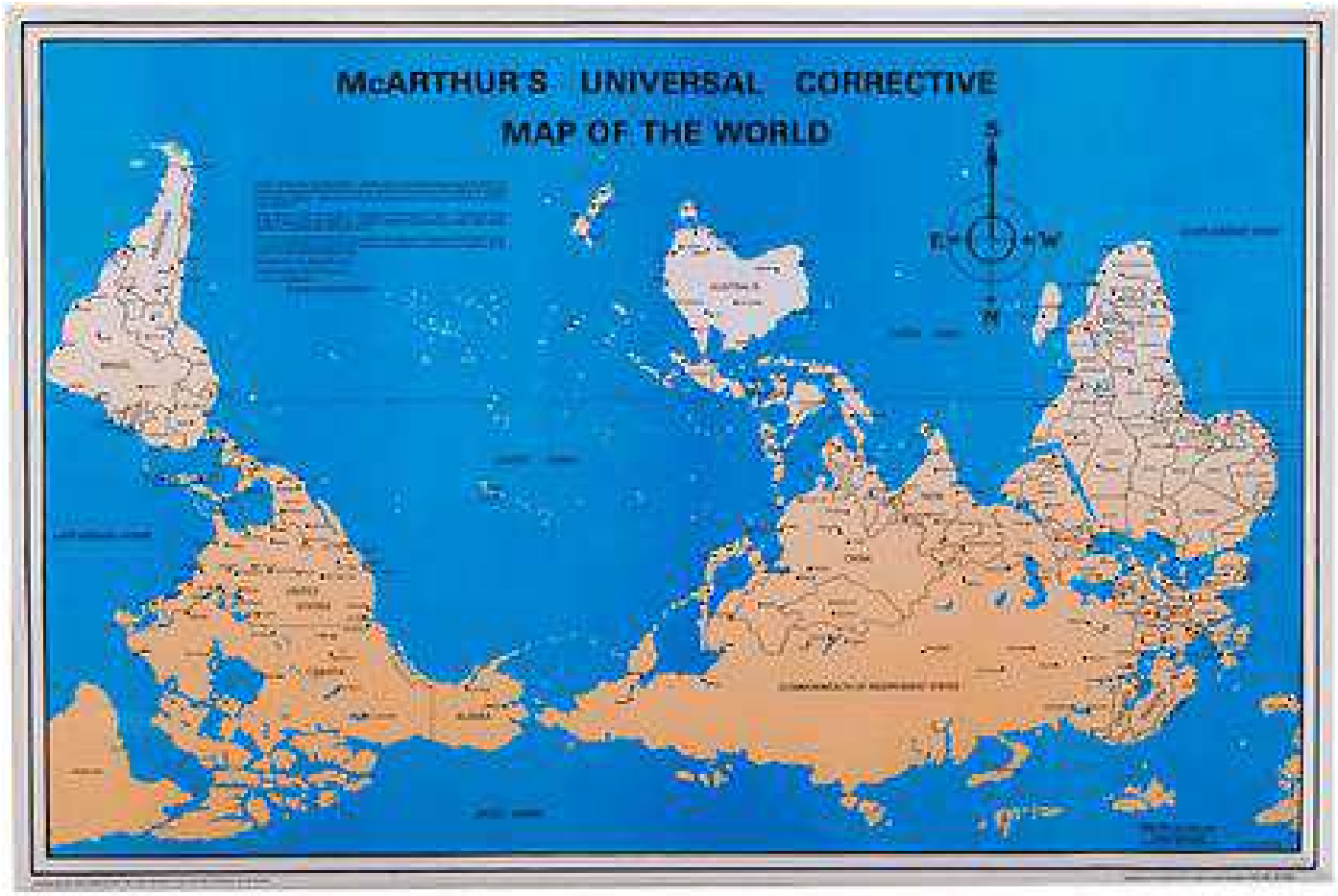

Figure 2: Corrective World Map

Figure 3: Heisenberg

In 1927 Heisenberg discovered that the "more precisely the position is determined, the less precisely the momentum is known in this instant, and vice versa".

Figure 4: Gödel

Four years later Gödel showed that a finitely specified, consistent formal system which is large enough to include arithmetic is incomplete.

Questions

We will adress the following main question:

Does uncertainty imply incompleteness?

and some related questions:

- Can complexity shed more light on incompleteness?
- Is randomness in quantum mechanics "algorithmically random"?
- Can quantum randomness be used to trespass the Turing's barrier?

Are there any connections between uncertainty and incompleteness?

Gödel's hostility to any suggestion regarding possible connections between his incompleteness theorem and physics, particularly, Heisenberg's uncertainty relation, is well-known: J. Wheeler was thrown out of Gödel's office for asking the question "Professor Gödel, what connection do you see between your incompleteness theorem and Heisenberg's uncertainty principle?"

Hawking's view (in 2002) is that "a physical theory is self-referencing, like in Gödel's theorem. ... Theories we have so far are both inconsistent and incomplete" .

Short excursion in AIT

Let C be a self-delimiting Turing machine.

- The program-size complexity induced by C, $H_C(x)$, is the length of the smallest input which produces x via C. The "invariance theorem" states that *there exists a self-delimiting universal Turing machine U such that for every self-delimiting Turing machine C there exists a constant $\varepsilon > 0$ (which depends upon U and C) such that for every string x,*

$$H_U(x) \leq \varepsilon + H_C(x).$$

- Let $\nabla_C(x)$ be the smallest integer whose binary representation produces x via C. Clearly,

$$2^{H_C(x)} \leq \nabla_C(x) < 2^{H_C(x)+1}.$$

  Therefore $\Delta_C(x)$, our uncertainty in the value $\nabla_C(x)$, is the difference between the upper and lower bounds given, namely $\Delta_C(x) = 2^{H_C(x)}$.

  The invariance relation becomes:

$$\Delta_U(x) \leq \varepsilon \cdot \Delta_C(x).$$

From uncertainty to randomness

Chaitin's Omega number

$$\Omega_U = 0.\omega_1\omega_2\ldots\omega_n\ldots \tag{1}$$

is the halting probability of U.

Ω_U is more than uncomputable, it is (algorithmically) random. To express this, let $\Delta_s = 2^{-s}$.

For every self-delimiting Turing machine C there is a constant $\varepsilon > 0$ (which depends upon U and C) such that

$$\Delta_s \cdot \Delta_C(\omega_1\ldots\omega_s) \geq \varepsilon. \tag{2}$$

The inequality (2) is an uncertainty relation as it reflects a limit to which we can simultaneously increase both the accuracy with which we can approximate Ω_U and the complexity of the initial sequence of bits we compute. When s grows indefinitely, Δ_s tends to zero in contrast with $\Delta_C(\omega_1\ldots\omega_s)$ which tends to infinity; their product is not only bounded from below, but increases indefinitely. There is a limit ε up to which we can uniformly compress the initial prefixes of the binary expansion of Ω_U.

Is

$$\Delta_s \cdot \Delta_C(\omega_1 \ldots \omega_s) \geq \varepsilon$$

a 'true' uncertainty relation?

Mathematically, the answer is positive: The variables Δ_s and Δ_C are the standard deviations of two measurable observables in suitable probability spaces, $\sigma_X = \Delta_s$ and $\sigma_Y = \Delta_C(\omega_1 \ldots \omega_s)$, hence the relation in the title becomes:

$$\sigma_X \cdot \sigma_Y = \Delta_s \cdot \Delta_C(\omega_1 \omega_2 \ldots \omega_s) \geq \varepsilon.$$

What about the physical point of view?

Consider a quantum algorithm with two parameters, C and s, where C is a self-delimiting Turing machine for which the probability of producing each s-bit string is computable.

We run the algorithm to compute that distribution on a quantum computer with s ouput qubits by putting the output register into a superposition of spin states and applying a suitable Hamiltonian operator. The expectation value for energy is exactly the same as that of Y, but with units of energy, i.e.

$$\Delta_C(\omega_1\omega_2\ldots\omega_s)[J]\cdot\Delta_s \geq \varepsilon[J],$$

where $[J]$ indicates Joules of energy.

Now define

$$\Delta_t \equiv \frac{\sigma_Q}{|d\langle Q\rangle/dt|},$$

where Q is any observable that does not commute with the Hamiltonian. Hence, the following is a form of Heisenberg's uncertainty principle:

$$\Delta_E\cdot\Delta_t \geq \hbar/2.$$

We can replace Δ_E by $\Delta_C(\omega_1\omega_2\ldots\omega_s)$ by the analysis above; but what about Δ_t?

If we choose a time scale such that our two uncertainty relations are equivalent for a single quantum system corresponding to a computer C and *one* value of s, then the relation holds for C and *any* value of s:

$$\Delta_C(\omega_1\omega_2\ldots\omega_s)[J]\cdot\Delta_s\frac{\hbar}{2\varepsilon}[J^{-1}\cdot Js]\geq\frac{\hbar}{2}[Js].$$

In this sense, we claim that Heisenberg's uncertainty relation is equivalent to (2).

The uncertainty principle now says that getting one more bit of Ω_U requires (asymptotically) twice as much energy.

As Heisenberg's uncertainty principle, our formal uncertainty principle is a general one; they both apply to *all* systems governed by the wave equation, not just quantum waves.

From randomness to incompleteness

Fix a universal self-delimiting Turing machine U. Let $x_1x_2\ldots$ be a binary infinite sequence and let F be a strictly increasing function mapping positive integers into positive integers. If the set

$$\{(F(i), x_{F(i)}) \mid i \geq 1\}$$

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

$$\Delta_U(x_1x_2\ldots x_{F(k)}) \leq \varepsilon \cdot 2^{F(k)-k}.$$

Under the hypothesis above the uncertainty relation (2) is violated:

$$\varepsilon_1 \cdot \frac{1}{\Delta_{F(k)}} \leq \Delta_U(x_1\ldots x_{F(k)}) \leq \varepsilon \cdot 2^{F(k)-k},$$

so we obtain Chaitin's information-theoretic incompleteness theorem: there exists a bound N such that ZFC cannot determine more than N scattered digits of $\Omega_U = 0.\omega_1\omega_2\ldots$.

Chaitin's "heuristic principle"

"A set of axioms of complexity N cannot yield a theorem of complexity substantially greater than N".

This principle is false for the program-size complexity H.

Can it be rescued? The answer is affirmative for the complexity $\delta(x) = \log_2(\nabla(x)) - |x|$:

Consider a consistent finitely-specified theory strong enough to formalise arithmetic and denote by $\mathcal{T}$ its set of theorems. Then, there exists a constant N, which depends upon U and $\mathcal{T}$, such that $\mathcal{T}$ does not contain any x with $\delta(x) > N$, i.e., such an x is unprovable in the theory.

The probability that a statement of length n is provable in such a theory tends to zero when n tends to infinity.

Is quantum randomness "algorithmically random"?

There is no such thing as "software generated" genuine randomness.

John von Neumann: "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin".

Quantum randomness is postulated and is not at all a mathematical consequence of the standard model of quantum mechanics.

Pragmatically, perhaps we can accept the randomness because of the immense success of the applications of quantum mechanics.

Wolfram: "a priori, there may in the end be no clear way to tell whether randomness is coming from an underlying quantum process that is being measured, or from the actual process of measurement."

Strong *computational* similarity: both algorithmic and quantum randomness are *uncomputable*, they cannot be generated/simulated by any machine.

The hybrid computer, PC + quantum random bits, is provable to leapfrog Turings barrier.

The reason (Feynman): "It is impossible to represent the results of quantum mechanics with a classical universal device.

This hybrid computer already exsists!. It can use

Figure 5: Quantis: OEM and PCI

More open questions

This "machine" (which is different from the classical probabilistic Turing machine) can, at any time of the computation, ask the "quantum oracle" to supply an arbitrarily long (but finite) quantum random string.

- *Exactly how much more powerful a Turing machine working with "an oracle of quantum random bits" can be?*
- *Can this immense power be exploited?*

Conclusions

- Algorithmic randomness is equivalent to a "formal uncertainty principle" which implies incompleteness. Incompleteness is pervasive.
- For every machine whose halting probability is computable, one can construct a quantum computer for which the uncertainty relation describes conjugate observables.
- Quantum randomness is fundamentally different from "deterministic chaos" (computable systems in which unobservably small causes can produce large effects) or software pseudo-randomness.
- Even if quantum randomness is not algorithmic random, the hybrid device, PC + quantum random bits, is provable superior to conventional computers.