A Quantum Random Oracle

Alastair A. Abbott,[1] Cristian S. Calude,[1] Karl Svozil[2]

[1] *Department of Computer Science, University of Auckland*
Private Bag 92019, Auckland, New Zealand
[2] *Institut für Theoretische Physik, Vienna University of Technology,*
Wiedner Hauptstraße 8-10/136 A-1040 Vienna, Austria

1. Turing's oracles

Turing's oracles have been used for many years to successfully understand the world of the incomputable. Are these tools only pure mathematical constructs or are they more "real"? We will show how quantum measurements performed in specifically designed environments can produce incomputable sequences of bits, and discuss why they can hence be seen as physical Turing oracles.

An oracle is a black box capable of answering a set of questions, and an oracle Turing machine is a Turing machine which can query an oracle. According to Turing [8, p.173]

> We shall not go any further into the nature of this oracle apart from saying that it cannot be a machine.

In current terms, a Turing oracle is an incomputable set O of natural numbers or strings. The oracle Turing machine can perform all of the usual operations of a Turing machine, and can also query the oracle for an answer to finitely many questions of the form "is n in O?". Because O is incomputable, an oracle Turing machine is a hypercomputer: it performs tasks no Turing machine can do.

Turing studied oracles asserting the truth/falsity of "number-theoretic statements", i.e. statements of the form "$\theta(x)$ vanishes for infinitely many natural numbers", where $\theta(x)$ is a primitive recursive function. The class of number-theoretic statements includes, but does not coincide with, the class of Π_1 statements, i.e. statements of the form "$\forall n\, P(n)$", where $P(n)$ is a computable predicate. Both Fermat's Last Theorem and the Riemann Hypothesis are Π_1 statements, and hence number-theoretic statements. Some

number-theoretic statements are (trivially) computable, but most of them are not, so they satisfy the Turing incomputability condition.

In cryptography, a "random oracle" is a black box that responds to every query with a "randomly" chosen response,[1] picked uniformly from its output domain subject to the restriction that for any fixed query the answer returned is the same every time it receives that query. In the framework known as the "random oracle model", random oracles are used in schemes where the system or protocol is proved secure because an attacker is (seems to be) required to extract impossible information from the oracle. This approach has known limits: for example, in [5] it is proved that there exist signature and encryption schemes that are secure in the random oracle model, but for which any implementation of the random oracle results in insecure schemes.

Let O be a subset of the set of natural numbers and let $\mathbf{x} = x_1 x_2 \cdots x_n \cdots$ be an infinite binary sequence. The map $\mathbf{x} \mapsto O_{\mathbf{x}}$ defined by $O_{\mathbf{x}} = \{i \mid x_i = 1\}$ is bijective, so we can equally speak about oracles as infinite binary sequences or sets of natural numbers (or strings, by using, say, the quasi-lexicographical bijective enumeration of strings over a finite alphabet). Incomputability is preserved under this bijection. A query "is n in O?" is equivalent to "is $x_n = 1$?".

The condition imposed in the "random oracle" model requires that the oracle O is given by a uniformly distributed binary sequence. Some "random oracles" may be Turing oracles, others may not. Champernowne's sequence $0100011011000001010011100101110111000 0 \cdots$ is uniformly distributed, so it is a "random oracle"; this "random oracle" is computable (primitive recursive), so not a Turing oracle.

The set of codes of halting Turing machines (computably enumerable but not computable), as well as the set of algorithmically random strings (immune, i.e. strongly incomputable) are examples of Turing oracles [3].

Are Turing oracles "real" or just pure theoretical mathematical notions?

2. Value indefiniteness and the Kochen-Specker Theorem

Computability is based on Turing's model of a computing machine, a fundamentally deterministic concept. Quantum mechanics, however, has confronted physicists with a world that appears to behave randomly and is essentially non-deterministic. The failures of a deterministic viewpoint to

[1] "True" or "pure" randomness does not exists from a mathematical point of view [3].

account for the predictions of quantum mechanics are exemplified by "no-go" theorems which exclude the possibility of assigning "hidden variables" that predict the outcome of quantum measurements.

According to Bell's Theorem there is no hidden variable theory which gives the same statistical predictions as quantum mechanics and satisfies *value definiteness* (i.e., all possible observables—including non-compatible ones—simultaneously have predefined values) and *locality* (i.e., two space-like separated events cannot influence each other in any way).

Bell's Theorem manifests itself in statistical inequalities—the class of which are called *Bell-type inequalities*—which pose a bound on the possible correlation between outcomes of spatially separated events subject to local realism, but of which quantum mechanics predicts violations. As Bell's Theorem deals with the statistical predictions of quantum mechanics, it might not be totally unreasonable to ask whether there are "stronger" no-go theorems which can tell us something deeper about the outcome of *individual* quantum measurements. The answer is affirmative.

A measurement *context* is a maximal set of pairwise co-measurable observables. For a measurement context $\mathcal{C} = \{A_1, A_2, \ldots\}$, the values corresponding to outcomes of measurements of observables $A_1, A_2, \ldots$ are $v(A_1, \mathcal{C})$, $v(A_2, \mathcal{C})$, ... The Kochen-Specker Theorem states that for a quantum mechanical system represented by a Hilbert space of dimension greater than two, it is impossible for a hidden variable theory to fulfill the predictions of quantum mechanics and satisfy the following two conditions: *value definiteness* and *non-contextuality* (i.e., the value corresponding to the outcome of a measurement of an observable A, $v(A)$, is independent of the other compatible observables measured alongside it).

3. An example of a quantum random oracle

Consider a quantum random number generator which outputs bits produced by successive preparation and measurement of a state in which each outcome has probability one-half. By envisaging this device running ad infinitum, we can consider the infinite sequence $\mathbf{x}$ it produces. If we assume a standard picture of quantum mechanics, i.e. a Copenhagen-like interpretation in which measurement irreversibly alters the quantum state,[2] that the experimenter has freedom in the choice of measurement basis[3] (the "free-will

[2] A "many-worlds" interpretation is excluded.

[3] In a truly deterministic theory—sometimes called superdeterminism—the experimenter might have the illusion of exercising her independent free choice, but in reality

assumption"), and that we reject the notion of contextual hidden variables and can hence, by the uniformity and symmetry of the Kochen-Specker construction conclude that all observables are value indefinite, then some surprising conclusions about $\mathbf{x}$ can be made [4]. If $\mathbf{x}$ were computable, then (in principle) it would be possible to predict the outcome of each measurement in advance. This amounts to the existence of hidden variables for these observables and hence is in contradiction with the value indefiniteness due to the Kochen-Specker Theorem forbidding the existence of such a consistent, context-independent pre-assignment of measurement outcomes. The free-will assumption guarantees that even for an unknown initial state preparation the measurement basis in general is not pre-determined, thereby avoiding the possibility that only the measured observable together with a particular context had a definite pre-assigned value [6]. Put differently, if $\mathbf{x}$ were computable then the device would behave deterministically (and hence classically) rather than quantum mechanically, and would contain infinitely many computable correlations. Hence, we have to conclude that $\mathbf{x}$ must be incomputable. In fact, the argument is readily seen to prove the stronger property of bi-immunity of $\mathbf{x}$.[4]

Bi-immunity is the weakest possible notion of randomness: every binary sequence which is not bi-immune contains an infinite computable subsequence, i.e. a computable subset. This fact allows a computable martingale[5] to succeed on this sequence, so the unpredictability of the sequence is infinitely many times compromised [7].

A sequence $\mathbf{x}$ is called Martin-Löf random if it is not contained in any effective null set.[6] A sequence $\mathbf{x}$ is called Kurtz random if it belongs to every computable open class of Lebesgue measure one. Every Omega number

she just obeys the rules of the theory.

[4]A sequence $\mathbf{x}$ is bi-immune if only finitely many bits of $\mathbf{x}$ are computable. Every bi-immune sequence is incomputable, but the converse is not true.

[5]A martingale is a function M from binary strings to positive reals satisfying the following fairness condition: $M(\sigma) = (M(\sigma 0) + M(\sigma 1))/2$. The martingale M succeeds on a sequence $\mathbf{x}$ if $\limsup_n M(\mathbf{x} \upharpoonright n) = \infty$.

[6]The set of all infinite sequences beginning with a string σ—the cylinder generated by σ—is a basic open set in Cantor space. The Lebesgue measure of the cylinder generated by σ is $2^{-|\sigma|}$. Every open subset of Cantor space is the union of a countable sequence of disjoint basic open sets, and the measure of an open set is the sum of the measures of any such sequence. A computably (computable) open set is an open set that is the union of the sequence of basic open sets determined by a computably enumerable (computable) sequence of binary strings. A constructive null set is a computably enumerable sequence X_i of effective open sets such that $X_{i+1} \subseteq X_i$ and Lebesgue measure of X_i is smaller than 2^{-i}, for each i. The intersection of the sets X_i has Lebesgue measure zero.

(halting probability [4]) is Martin-Löf random and every Martin-Löf random real is Kurtz random; the converse implications are not true. Open question: Is the quantum random sequence previously described Kurtz random?

4. A quantum random number generator certified by value indefiniteness

Can a quantum device generating a bi-immune sequence really be constructed? Many quantum random number generators have been described and, while it is not readily clear which of the existing devices do produce an incomputable sequence of bits, it is not difficult to conceive designs which are explicitly certified by value indefiniteness to do so. One such device was proposed in [1].

5. Hypercomputation via quantum random oracles

As noted before, an oracle Turing machine is a hypercomputer. In particular, a Turing machine working with a bi-immune quantum random oracle [1] is a hypercomputer.

The undecidability proof of the halting problem still applies to such machines; although they determine whether particular Turing machines will halt on specific inputs, they cannot determine, in general, if machines equivalent to themselves will halt. This fact creates a hierarchy of machines, closely related to the arithmetical hierarchy in mathematical logic, each with a more powerful halting oracle and an even harder halting problem.

Arguably the most important open question regarding quantum random oracles is: *What is the computational power of a Turing machine working with a bi-immune quantum random oracle?* We believe that such an oracle Turing machine cannot solve the halting problem, but it may solve a weaker undecidable problem, for example, the lesser limited principle of omniscience which states that, if the existential quantification of the conjunction of two decidable predicates is false, then one of their separate existential quantifications is false [2].

Acknowledgement

We thank Mike Stay for illuminating discussions and Marcus Hutter for useful comments which improved the paper.

[1] A. A. Abbott, C. S. Calude, and K. Svozil. A quantum random number generator certified by value indefiniteness. *CDMTCS Research Report*, 396, 2010.

[2] D. Bridges and F. Richman. *Varieties of Constructive Mathematics*. Number 97 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1987.

[3] C. S. Calude. *Information and Randomness: An Algorithmic Perspective*. Springer-Verlag, Berlin, 2nd edition, 2002.

[4] C. S. Calude and K. Svozil. Quantum randomness and value indefiniteness. *Advanced Science Letters*, 1(165–168), 2008.

[5] R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. In *Proceedings of the 30th Annual ACM Symposium on the Theory of Computing*, pages 209–218, 1998.

[6] M. J. W. Hall. Local deterministic model of singlet state correlations based on relaxing measurement independence. *Physical Review Letters*, 105(250404), 2010.

[7] B. Kjos-Hanssen, F. Stephan, and J. R. Teutsch. Enumerating randoms. *arXiv:1008.4825v1*, 2010.

[8] A. M. Turing. Systems of logic based on ordinals. *Proceedings of the London Mathematical Society, Series 2*, 45:161–228, 1939.