Is Quantum Randomness Algorithmic Random? A Preliminary Attack

Cristian S. Calude, Michael J. Dinneen
Department of Computer Science
University of Auckland, New Zealand
{cristian,mjd}@cs.auckland.ac.nz

Quantum randomness has been confirmed by theoretical and experimental research. It is well-known that quantum randomness passes all reasonable statistical properties of randomness.

The first book containing a million of quantum random digits—generated by using radioactive decay from electronic vacuum tubes—was published by the RAND Corporation in 1955. Currently, quantum randomness can be easily, quickly and reliably produced: Quantis, a device produced by Id Quantique, a company affiliated with Geneva University, uses elementary quantum optics to produce quantum random bits at the rate of 4Mbits/sec. A photon generated by a source beamed to a semitransparent mirror is reflected or transmitted with 50 per cent chance, and these measurements can be translated into a string of quantum random bits.

The pitfalls of software-generated pseudo-randomness are well-known. In John von Neumann's words: "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin".

But, is quantum randomness "true" randomness?

First, and foremost, there is no such thing as "true" randomness!

Secondly, no software can produce infinitely many quantum random bits, not only practically, but also theoretically: if we adopt the standard model of quantum mechanics, quantum randomness is not Turing computable.

Thirdly, is randomness in quantum mechanics "algorithmically random"? Algorithmic randomness is proposed and studied by algorithmic information theory; algorithmic randomness is not Turing computable, hence no software-generated pseudo-randomness is algorithmic random. Further on, algorithmic randomness satisfies all computable enumerable statistical properties of randomness and it is algorithmically unpredictable. More importantly, every "decent" Monte Carlo simulation algorithm (like Rabin-Miller or Solovay-Strassen primality tests) powered with algorithmic random selection produces the result not only true with high probability, but *rigourously correct*.

Fourthly, why is it interesting to contrast quantum and algorithmic randomness? Theoretically, the question touches a fundamental problem in quantum mechanics: what is the nature of quantum randomness (recall that in the standard model, quantum randomness is postulated, not derived). It also revives the question of Turing computability of quantum mechanics as well as the question whether quantum randomness can be used to trespass the Turing's barrier. But there are practical questions as well: the most important is to evaluate the "quality" of Monte-Carlo simulations powered with quantum randomness.

Contrasting quantum and algorithmic randomness is a very difficult problem. In this talk we will present some preliminary theoretical lines of attack. Extensive experiments will be presented and commented. A few open problems will finally discussed.