AIT Based Randomness Testing of Quantum Random Bits

Cristian S. Calude

December 5, 2018

There is a huge demand of "randomness", hence there are many methods to produce "random bits": software based random generators (also called, pseudo-random generators) and hardware random generators (e.g. quantum random generators).

Ramsey Theory[3, 7] and Algorithmic Information Theory[1] have proved that there is no "true" randomness: in any finite or infinite sequence there are patterns. So, correlations and patterns exist no matter how randomness is generated, from the environment (for example, Brownian motion, with hardware random number generators), from the initial conditions in systems whose behaviour is very sensitive to small variations in initial conditions (such as pachinko machines and dice) or from software based random generators.

Tests of randomness can be used to determine whether a data set has a recognisable pattern, and therefore whether the process that generated it is significantly random. There are many tests of randomness, like *diehard* [5], *NIST* [6], or *TestU01* [4]). The standard test suites are often designed explicitly or implicitly to quantify the quality of the cyclic pseudo-random numbers generated by algorithms, so they are not useful for assessing hardware random number generators.

A detailed comparative analysis of bit strings of length 2^{32} obtained from two quantum random number generators[1] and three pseudo-random generators was presented [2]. The analysis used tests based on algorithmic information theory. All tests depend on the size of the analysed strings; the legitimacy of this approach is given by the fact that algorithmic randomness of finite or infinite string can be "uniformly read" in its prefixes (cf. [1]).

The project will assess a massive data of bits produced by a quantum random number generator using old and new tests of randomness inspired by algorithmic information theory.

References

[1] C. Calude. *Information and Randomness—An Algorithmic Perspective.* Springer, Berlin, second edition, 2002.

[2] C. S. Calude, M. J. Dinneen, M. Dumitrescu, and K. Svozil. Experimental evidence of quantum randomness incomputability. *Phys. Rev. A*, 82(2):022102, Aug 2010.

[3] R. Graham and J. H. Spencer. Ramsey theory. *Scientific American*, 262:112–117, Sept. 1990.

[4] P. L'Ecuyer and R. Simard. TestU01: A C library for empirical testing of random number generators. *ACM Transactions on Mathematical Software (TOMS)*, 33(4):Article 22, 1–40, 2007.

[1] The size correlates well with the square root of the cycle length used by cyclic pseudo-random generators; randomness properties of longer strings generated in this way are impaired.

[5] G. Marsaglia. The Marsaglia random number CDROM including the diehard battery of tests of randomness. www.stat.fsu.edu/pub/diehard/, 1995.

[6] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Hekert, J. Dray, and S. Vo. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22.* National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2001.

[7] A. Soifer. Ramsey theory before Ramsey, prehistory and early history: An essay in 13 parts. In A. Soifer, editor, *Ramsey Theory*, volume 285 of *Progress in Mathematics*, pages 1–26. Birkhäuser Boston, 2011.