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\cite{3, 7} and Algorithmic Information Theory\cite{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 \cite{5}, NIST \cite{6}, or TestU01 \cite{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\footnote{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.} and three pseudo-random generators was presented \cite{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. \cite{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

\begin{thebibliography}{9}


\end{thebibliography}
