Computer Physics Communications 184 (2013) 257–258

Contents lists available at SciVerse ScienceDirect

Computer Physics Communications

journal homepage: www.elsevier.com/locate/cpc

Employing online quantum random number generators for generating truly random quantum states in *Mathematica*☆

Jarosław Adam Miszczak *

Institute of Theoretical and Applied Informatics, Polish Academy of Sciences, Bałtycka 5, 44-100 Gliwice, Poland

ARTICLE INFO

Article history:
Received 4 June 2012
Accepted 20 August 2012
Available online 25 August 2012

Keywords:
Random density matrices
Quantum information
Quantum random number generator
On-line quantum random number generator service

ABSTRACT

The presented package for the *Mathematica* computing system allows the harnessing of quantum random number generators (QRNG) for investigating the statistical properties of quantum states. The described package implements a number of functions for generating random states. The new version of the package adds the ability to use the on-line quantum random number generator service and implements new functions for retrieving lists of random numbers. Thanks to the introduced improvements, the new version provides faster access to high-quality sources of random numbers and can be used in simulations requiring large amount of random data.

New version program summary

Program title: TRQS
Catalogue identifier: AEKA_v2_0
Program summary URL: http://cpc.cs.qub.ac.uk/summaries/AEKA_v2_0.html
Program obtainable from: CPC Program Library, Queen's University, Belfast, N. Ireland
Licensing provisions: Standard CPC licence, http://cpc.cs.qub.ac.uk/licence/licence.html
No. of lines in distributed program, including test data, etc.: 18 134
No. of bytes in distributed program, including test data, etc.: 2 520 49
Distribution format: tar.gz
Programming language: Mathematica, C.
Computer: Any supporting Mathematica in version 7 or higher.
Operating system: Any platform supporting Mathematica; tested with GNU/Linux (32 and 64 bit).
RAM: Case-dependent
Supplementary material: Fig. 1 mentioned below can be downloaded.
Classification: 4.15.
External routines: Quantis software library (http://www.idquantique.com/support/quantis-trng.html)
Catalogue identifier of previous version: AEKA_v1_0
Journal reference of previous version: Comput. Phys. Comm. 183(2012)118
Does the new version supersede the previous version?: Yes

Nature of problem:
Generation of random density matrices and utilization of high-quality random numbers for the purpose of computer simulation.

Solution method:
Use of a physical quantum random number generator and an on-line service providing access to the source of true random numbers generated by quantum real number generator.

Reasons for new version:
Added support for the high-speed on-line quantum random number generator and improved methods for retrieving lists of random numbers.

Summary of revisions:

☆ This paper and its associated computer program are available via the Computer Physics Communication homepage on ScienceDirect (http://www.sciencedirect.com/science/journal/00104655).

* Tel.: +48 322317319.
E-mail address: miszczak@iitis.pl.

doi:10.1016/j.cpc.2012.08.012

The presented version provides two signicant improvements. The first one is the ability to use the on-line Quantum Random Number Generation service developed by PicoQuant GmbH and the Nano-Optics groups at the Department of Physics of Humboldt University. The on-line service supported in the version 2.0 of the **TRQS** package provides faster access to true randomness sources constructed using the laws of quantum physics. The service is freely available at https://qrng.physik.hu-berlin.de/. The use of this service allows using the presented package with the need of a physical quantum random number generator.
The second improvement introduced in this version is the ability to retrieve arrays of random data directly for the used source. This increases the speed of the random number generation, especially in the case of an on-line service, where it reduces the time necessary to establish the connection. Thanks to the speed improvement of the presented version, the package can now be used in simulations requiring larger amounts of random data. Moreover, the functions for generating random numbers provided by the current version of the package more closely follow the pattern of functions for generating pseudo-random numbers provided in Mathematica.

Additional comments:
Speed comparison: The implementation of the support for the QRNG on-line service provides a noticeable improvement in the speed of random number generation. For the samples of real numbers of size 10^1; $10^2, \ldots, 10^7$ the times required to generate these samples using Quantis USB device and QRNG service are compared in Fig. 1. The presented results show that the use of the on-line service provides faster access to random numbers. One should note, however, that the speed gain can increase or decrease depending on the connection speed between the computer and the server providing random numbers.

Running time:
Depends on the used source of randomness and the amount of random data used in the experiment.
References:
[1] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, O. Benson., An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements, Applied Physics Letters, Vol. 098, 171105 (2011). http://dx.doi.org/10.1063/1.3578456.

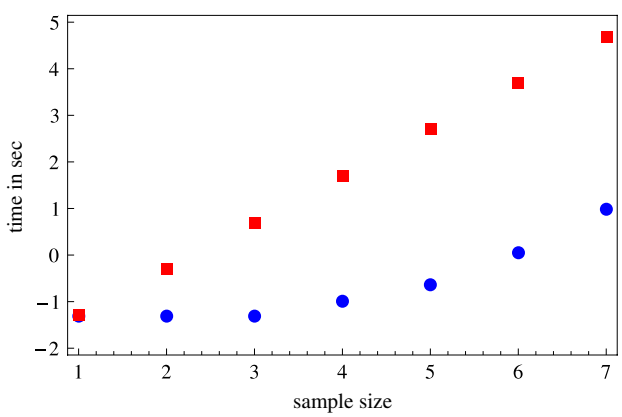

Fig. 1. Comparison of the times required to generate a sample of random numbers using the Quantis device (red squares) and the QRNG service (blue dots) in log–log scale. In the case of the QRNG service the plot presents the time averaged over three experiments. In both cases the results were obtained by generating matrices of random real numbers from [0, 1] using TrueRandomReal function.

Acknowledgments

The author would like to thank R. Heinen and M. Wahl for bringing his attention to Ref. [1], motivating this work and helping during its development. This work was supported by the Polish Ministry of Science and Higher Education under grant number IP2011 036371.