Multi-bit quantum random number generation from a single qubit quantum walk

Dillon Broaders   Prof. Felix Binder

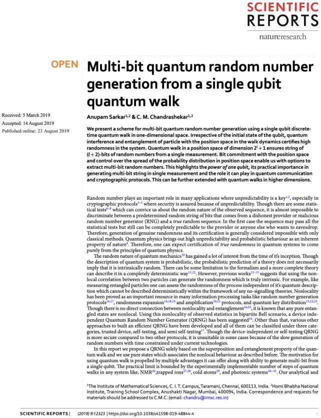
Trinity College Dublin

broaderd@tcd.ie

Special Topics Python Project

Objectives

- Generate a Quantum Random Walk over N steps.
- Calculate the Shannon Entropy H for resulting probability distribution.
- Plot H vs N and interpret results.



SCIENTIFIC REPORTS

natureresearch

OPEN

Multi-bit quantum random number generation from a single qubit quantum walk

Received: 5 March 2019
Accepted: 14 August 2019
Published online: 23 August 2019

Anupam Sarkar[1,2] & C. M. Chandrashekar[1,2]

We present a scheme for multi-bit quantum random number generation using a single qubit discrete-time quantum walk in one-dimensional space. Irrespective of the initial state of the qubit, quantum interference and entanglement of particle with the position space in the walk dynamics certifies high randomness in the system. Quantum walk in a position space of dimension 2^l+1 ensures string of $(l+2)$-bits of random numbers from a single measurement. Bit commitment with the position space and control over the spread of the probability distribution in position space enable us with options to extract multi-bit random numbers. This highlights the *power of one qubit*, its practical importance in generating multi-bit string in single measurement and the role it can play in quantum communication and cryptographic protocols. This can be further extended with quantum walks in higher dimensions.

Random number plays an important role in many applications where unpredictability is a key[1,2], especially in cryptographic protocols[3–5] where security is assured because of unpredictability. Though there are some statistical tests[6–8] which can convice us about the random nature of the observed sequence, it is almost impossible to discriminate between a predetermined random string of bits that comes from a dishonest provider or malicious random number generator (RNG) and a *true* random sequence. In the first case the sequence may pass all the statistical tests but still can be completely predictable to the provider or anyone else who wants to eavesdrop. Therefore, generation of genuine randomness and its certification is generally considered impossible with only classical methods. Quantum physics brings out high unpredictability and probabilistic behaviour as an inherent property of nature[9]. Therefore, one can expect certification of *true randomness* in quantum systems to come purely from the principles of quantum physics.

The random nature of quantum mechanics[10] has gained a lot of interest from the time of it's inception. Though the description of quantum system is probabilistic, the probabilistic prediction of a theory does not necessarily imply that it is intrinsically random. There can be some limitation to the formalism and a more complete theory can describe it in a completely deterministic way[11,12]. However, previous works[13–15] suggests that using the non-local correlation between two particles can generate the randomness which is truly intrinsic. For example, like measuring entangled particles one can assess the randomness of the process independent of it's quantum description which cannot be described deterministically within the framework of any no-signalling theories. Nonlocality has been proved as an important resource in many information processing tasks like random number generation protocols[16,17], randomness expansion[16,18,19] and amplification[20,21] protocols, and quantum key distribution[15,22,23]. Though there is no direct connection between nonlocality and entanglement[24,25], it is known that any pure entangled states are nonlocal. Using this nonlocality of observed statistics in bipartite Bell scenario, a device independent Quantum Random Number Generator (QRNG) has been suggested[16]. Other than that, various other approaches to built an efficient QRNG have been developed and all of them can be classified under three categories, trusted device, self-testing, and semi self-testing[17]. Though the device-independent or self-testing QRNG is more secure compared to two other protocols, it is unsuitable in some cases because of the slow generation of random numbers with time constrained under current technologies.

In this report we propose a QRNG solely based on the superposition and entanglement property of the quantum walk and we use pure states which associates the nonlocal behaviour as described before. The motivation for using quantum walk is propelled by multiple advantages it can offer along with ability to generate multi-bit from a single qubit. The practical limit is bounded by the experimentally implementable number of steps of quantum walks in any system like, NMR[26],trapped ions[27,28], cold atoms[29], and photonic systems[30–33]. Our analytical and

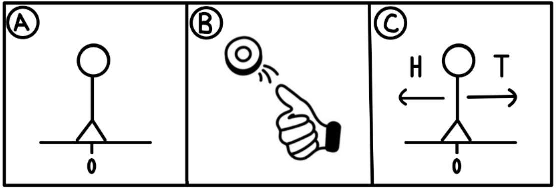
[1]The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai, 600113, India. [2]Homi Bhabha National Institute, Training School Complex, Anushakti Nagar, Mumbai, 400094, India. Correspondence and requests for materials should be addressed to C.M.C. (email: chandru@imsc.res.in)

SCIENTIFIC REPORTS | (2019) 9:12323 | https://doi.org/10.1038/s41598-019-48844-4

Recreate the QW line from Fig.4 in Sarkar et al (2019).

Random Walks

- Build Intuition for Quantum Random Walks (QW) by first understanding their classical counterpart (CW).



- Take ingredients of CW and "Quantumize" them.

Method

- The workflow consisted of the following steps:

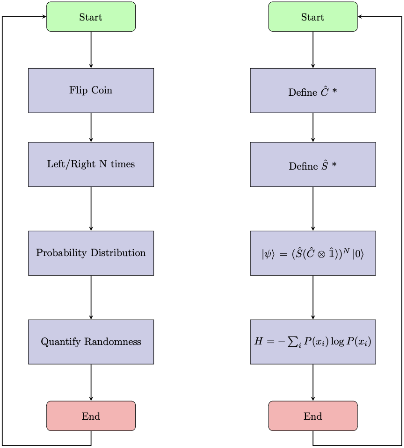


Figure: Classical Workflow (*left) and Quantum Workflow (right)*

Results

- Two equidistant peaks ($\approx \pm\frac{N}{\sqrt{2}}$) for symmetrical coin.
- Standard deviation is N.

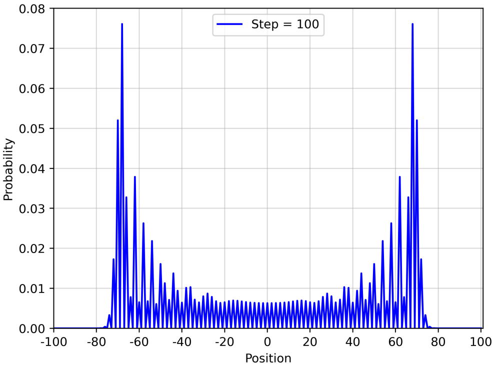


Figure: Probability distribution for position with 100 QW steps.

Results

- Oscillations are caused by interference effects.

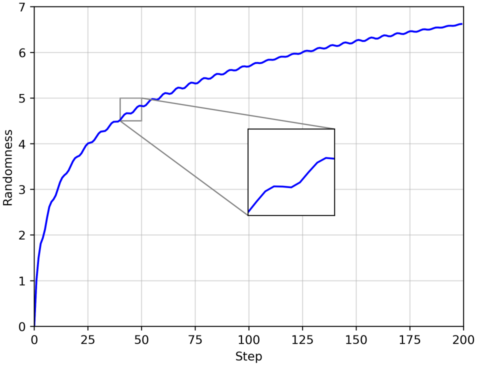


Figure: Randomness in system as a function of QW steps

References

Sarkar, A. and Chandrashekar, C.M. Multi-bit quantum random number generation from a single qubit quantum walk. Sci Rep 9, 12323 (2019).

The End

Questions ?