第 58 卷 第 17 期/2021 年 9 月/激光与光电子学进展 研究论文

激光与光电子学进展

量子行走中随机性的研究

张融*，李文滔

南京邮电大学电子与光学工程学院，江苏 南京 210023

摘要 具有不可预测性的随机数是保证保密通信的关键因素。通过输入单比特量子态，基于量子行走的演化，制备了多路径相干叠加态，并通过一次量子测量，得到了多比特随机数。详细计算了输入状态、精确调控的演化过程以及演化步数对多比特量子纯态随机性的影响。对于目前的单光子探测技术，量子行走为随机数产生率的提升提供了很好的平台。

关键词 量子光学；量子行走；随机数；相干叠加态；量子测量

中图分类号 O413.1 **文献标志码** A **doi**：10.3788/LOP202158.1727001

Research on Randomness in Quantum Walks

Zhang Rong*, Li Wentao

College of Electronic and Optical Engineering, Nanjing University of Posts and Telecommunication, Nanjing, Jiangsu 210023, *China*

Abstract Unpredictable random numbers is the key to ensure the security of quantum communication. We discuss the multi-bit random number produced by the evolution of a quantum walk via the single-bit input, the preparation of multi-path coherent superposition state, and single quantum measurement. We have investigated in detail the influences of input state, precisely engineered evolution and number of evolution steps on the randomness of multi-bit quantum pure states. As for the current single-photon detection technology, quantum walks provide a good platform to increase the generation rate of random numbers.

Key words quantum optics; quantum walk; random numbers; coherent superposition state; quantum measurement

OCIS codes 270.1670; 270.5565; 270.5585

1 引 言

随机数在密码学、保密通信以及基础科学等领域有着广泛的应用，其不可预测性是确保通信安全的关键因素[1]。利用数学算法能够得到符合预期分布的随机数列，产生的数据是可以预测和重现的。这种方法产生的随机数在本质上具有确定性，所以特定算法产生的随机数称为伪随机数。在仿真计算领域，我们认为随机数发生器产生的随机数是足够随机的。但是，对于许多应用来说，不可预测性非常重要，比如保密通信[2]，可预测的随机数显然无法保证通信安全。通常把具有不可预测性的无关联的随机数称为真随机数。通过测量物理过程中不可预测的变量，利用测量结果输出真随机数序列。量子力学原理确保了处于叠加态的量子体系能够提供不可预测的真随机数[3-4]。非局域关联[5]是产生随机数的重要资源[6]。两粒子之间的非局域关联可被用于产生器件无关或者可自检测的真随机数，但是受限于目前的探测技术，其产生速率较低[7-11]。

收稿日期：2020-11-19；**修回日期**：2021-01-07；**录用日期**：2021-01-22

通信作者：*zhangr@njupt.edu.cn

多比特量子相干叠加性可以有效提高随机数的产生速率。在量子行走中，多路径叠加态可用于实现多比特真随机数。量子行走是经典随机行走在量子世界中的对应[12]。经典随机行走已被广泛应用于数学、计算机、遗传学和经济学等领域。由于相干叠加性，量子行走的性质与经典随机行走的性质有很大不同，前者的扩散速率更快，随演化时间的增加呈平方增长，而后者的扩散速率与演化时间呈正比关系[13]。因此，量子行走作为搜索算法的基础，可以有效提高搜索效率[14]，实现通用量子计算机[15]。量子行走作为一个理想的平台可模拟量子现象，比如 Anderson localization[16]。对于分立量子行走，硬币的初始状态和硬币操作可以控制行走者的状态，因此量子行走为量子态的传输和通用测量[17]、拓扑相位、生物系统中的随机现象等提供了研究平台。在量子信息的处理过程中，可以根据实际需要选择不同性质的量子行走。

本文基于量子行走，通过精确调控的多路径相干叠加态的一次测量，得到了多比特随机数。利用香农熵度量随机性，详细探讨了影响随机性的诸多因素，比如系统的初始状态、系统的演化算符以及演化步数。计算结果表明，随着演化步数的增大，随机性呈现上升的趋势。对于相同的演化步数，选择合适的系统初态和硬币操作，能够有效增大随机性，从而提高随机数的产生速率。

2　物理模型

量子行走通常分为连续时间量子行走和分立时间量子行走。本文讨论分立的情况，整个系统包含量子硬币和行走者两个子系统。量子硬币是二维的量子系统，其状态用$|c\rangle$描述，其中$c=0,1$。行走者的位置状态为$|x\rangle(x\in\mathbf{Z})$，其中$x$是行走者所处的位置。量子行走的幺正演化算符为

$$U=S(\boldsymbol{C}\otimes\boldsymbol{I}),\tag{1}$$

式中：$\boldsymbol{I}$是单位操作；S是条件行走操作，具体形式是$S=|0\rangle\langle 0|\otimes|x-1\rangle\langle x|+|1\rangle\langle 1|\otimes|x+1\rangle\langle x|$，行走者根据硬币的状态$|0\rangle(|1\rangle)$决定向左(右)走；$\boldsymbol{C}$是量子硬币操作，该操作使得硬币处于$|0\rangle$和$|1\rangle$的相干叠加态，具体表示为

$$\boldsymbol{C}=\begin{bmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{bmatrix},\tag{2}$$

式中：硬币操作系数$\theta\in\left(0,\frac{\pi}{2}\right)$。

考虑行走者初始处于原点，硬币处于任意$|0\rangle$和$|1\rangle$的相干叠加态，整个系统的初态是

$$\psi(0)=|0\rangle\left(|0\rangle\cos\alpha+\mathrm{e}^{\mathrm{i}\beta}|1\rangle\sin\alpha\right),\tag{3}$$

式中：初始状态系数$\alpha\in\left[0,\frac{\pi}{2}\right]$；初始状态的相对相位$\beta\in[0,2\pi]$。重复(1)式中的幺正演化操作，使得行走者处于不同位置的相干叠加态，经过t步演化后，系统的状态为

$$\psi(t)=U^{t}|\psi(0)\rangle=\sum_{x}|x\rangle\left[a(x,t)|0\rangle+b(x,t)|1\rangle\right],\tag{4}$$

式中：$x=-t,t+2,\cdots,t$；叠加系数满足$\sum_{x}|a(x,t)|^{2}+|b(x,t)|^{2}=1$。施加合适的局域操作$\frac{1}{N_{x,t}}\begin{bmatrix}a(x,t) & b(x,t)\\ b(x,t) & -a(x,t)\end{bmatrix}$(其中$N_{x,t}=\sqrt{|a(x,t)|^{2}+|b(x,t)|^{2}}$)，使得所有位置的硬币态都处于$|0\rangle$，此时整个系统处于可分态。其中，行走者处于所有可能位置的相干叠加态为$\sum_{x}p_{x}|x\rangle$，该状态是纯态，具有内禀的随机性，可用于获取多比特真随机数。

3　行走者随机性的度量

根据量子力学态叠加原理以及量子测量假设可知，当行走者处于多路径叠加态时，通过一次测量，我们可以得到一系列经典比特的输出。例如，经过7步演化后，行走者处于8个位置状态$|x\rangle$的相干叠加态，其中$x=-7,-5,-3,\cdots,7$。如果是等概率幅的叠加态，经过一次测量后，我们以相同的概率得到$8=2^{3}$种可能的态，对应于经典信息，相当于得到了3 bit真随机数，如表1所示。根据波恩统计规律可知，当行走者处于$\sum_{x}p_{x}|x\rangle$时，进行位置的投影测量后，输出结果是位置x的概率为$|p_{x}|^{2}$。处于纯态的行走者的内禀随机性与测量得到的输出结果有关。根据以上分析，输入单量子比特态，通过量子行走演化，一次量子测量后即可得到多比特真随机数。利用熵度量其随机性，信息论中，熵用

表 1　3 bit 真随机数

Table 1　3 bit true random number

x	Random number
−7	000
−5	001
−3	010
−1	011
1	100
3	101
5	110
7	111

比特的形式表述，其中最简单的熵度量方法是香农熵 $R=-\sum_x|p_x|^2\ln\left(|p_x|^2\right)$。香农熵给出了一次测量后能够提取的信息的平均比特数。香农熵越高，表示概率分布越接近等概率分布。与非均匀分布相比较，从等概率分布的测量结果中可以提取出更多的随机比特数。另一个非常有效的随机性度量是最小熵，即 $E_{\min}=-\mathrm{lb}\left[\max\left(|p_x|^2\right)\right]$，其给出了随机性提取的下限[10]。在后续的讨论中，我们将具体计算香农熵和 Rényi 最小熵以定量描述行走者的内禀随机性。由于行走者所处的相干叠加态与系统的初态、硬币操作以及演化步数相关，因此我们分别研究了上述因素对随机性的影响，从而通过选择合适的系统参数以及增大演化步数，提高随机数的产生率。

对于给定的步数 $t=60$，表征随机性的香农熵和最小熵与系统初态以及硬币操作的关系分别如图 1、2 所示。我们首先计算了硬币操作系数为 $\theta=\pi/16,\pi/8,\pi/4$ 时，香农熵和最小熵随着初始状态系数 α 的改变，其中图 1(a)、(c)对应 $\beta=\pi/2$ 的情况，图 1(b)、(d)对应 $\beta=0$ 的情况。从图 1 可以看出，对于给定的参数 t、θ 和 β，可以通过选择合适的 α，提高香农熵和最小熵的数值。

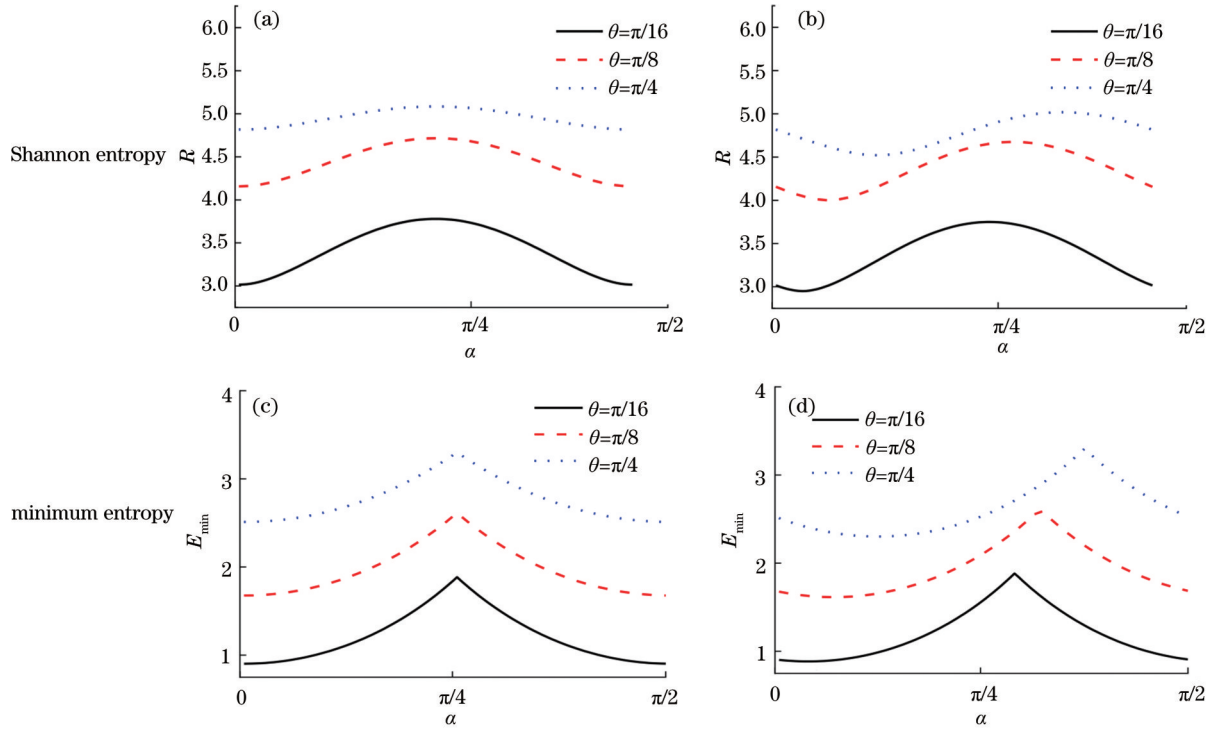

图 1　香农熵和最小熵随着 α 的变化情况。(a)(c) $\beta=\pi/2$；(b)(d) $\beta=0$

Fig. 1　Shannon entropy and minimum entropy versus α. (a) (c) $\beta=\pi/2$; (b) (d) $\beta=0$

为了研究硬币初态中的相对相位对随机性的影响，在给定步数 $t=60$、硬币操作系数 $\theta=\pi/4$、硬币初始状态系数 $\alpha=\pi/4$ 的条件下，分别计算了香农熵和最小熵随初态相对相位 β 的变化，结果如图 2 所示。可以看出，熵值都呈现周期性变化，且当 $\beta=\pi/2,3\pi/2$ 时，香农熵和最小熵取最大值。

对于给定的 $\alpha=\pi/4$，$\beta=\pi/2$，选择不同的硬币操作，香农熵和最小熵随演化步数的变化情况分别如图 3(a)、(b)所示。可以看出，香农熵随着演化步数的增加而增大，而最小熵随着演化步数的增加整体呈现上升的趋势，在小范围内通过选取合适的步数，才能得到增大的最小熵。对于等概率幅叠加的

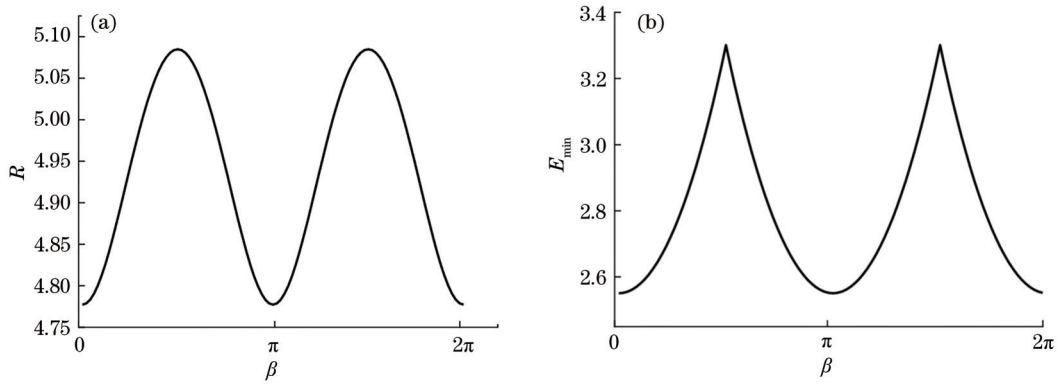

图 2　当 $\theta=\pi/4$, $\alpha=\pi/4$, $t=60$ 时香农熵和最小熵随 β 的变化情况。(a)香依熵;(b)最小熵

Fig. 2　Shannon entropy and minimum entropy versus β when $\theta=\pi/4$, $\alpha=\pi/4$, and $t=60$. (a) Shannon entropy; (b) minimum entropy

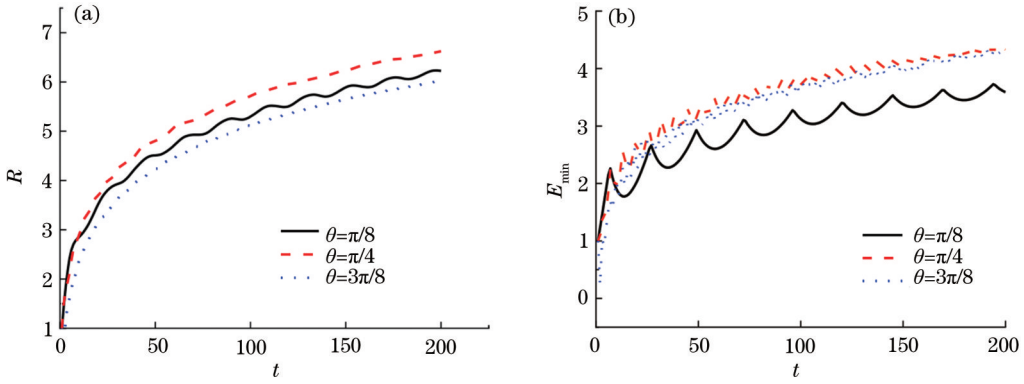

图 3　当 $\alpha=\pi/4$, $\beta=\pi/2$ 时香农熵和最小熵随演化步数的变化情况。(a)香农熵;(b)最小熵

Fig. 3　Shannon entropy and minimum entropy versus number of evolution steps when $\alpha=\pi/4$ and $\beta=\pi/2$. (a) Shannon entropy; (b) minimum entropy

初态,当硬币操作系数选择 $\theta=\pi/4$ 时,在相同演化步数下,香农熵和最小熵取值最大。

4　结　　论

主要讨论了基于量子行走演化获取多比特随机数的方案。通过输入单比特量子态,基于量子行走的演化过程,制备了多路径相干叠加态,通过投影测量,可以输出多比特随机数。利用香农熵和最小熵定量描述位置相干叠加态的随机性。具体计算了香农熵和最小熵随初态、硬币操作以及演化步数的变化情况。计算结果表明,选取 $\theta\in(0,\pi/2)$、$\alpha\in[0,\pi/2]$ 和 $\beta\in[0,\pi/2)$,经过 t 步演化操作后,行走者处于所有可能位置的叠加态,经过量子测量后,该叠加态以一定的概率塌缩到其中一个位置态上,其随机性与初态、系统演化操作以及演化步数有关。香农熵随演化步数的增大而增大,而最小熵随演化步数的增大整体呈现增大的趋势,但是最小熵会出现略有下降的情况。当选择 $\theta=\pi/4$, $\alpha=\pi/4$, $\beta=\pi/2$ 时,对于相同的演化步数,香农熵和最小熵均最大。基于量子行走的演化,通过一次测量即可得到多比特随机数。针对目前的单光子探测技术,量子行走为随机数产生率的提升提供了很好的平台。

参　考　文　献

[1] Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography[J]. Reviews of Modern Physics, 2002, 74(1): 145-195.

[2] Tang J, Shi L, Wei J H, et al. Quantum key agreement protocols immune to collective noise[J]. Laser & Optoelectronics Progress, 2020, 57(17): 172703.
唐杰, 石磊, 魏家华, 等. 免疫集体噪声的量子密钥协商协议[J]. 激光与光电子学进展, 2020, 57(17): 172703.

[3] Born M. Statistical interpretation of quantum mechanics[J]. Science, 1955, 122(3172): 675-679.

[4] Acín A, Masanes L. Certified randomness in quantum physics[J]. Nature, 2016, 540(7632): 213-219.

[5] Ekert A K. Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, 1991, 67(6): 661-663.

[6] Ma X F, Yuan X, Cao Z, et al. Quantum random number generation[J]. npj Quantum Information, 2016, 2(1): 1-9.

[7] Colbeck R, Kent A. Private randomness expansion with untrusted devices[J]. Journal of Physics A: Mathematical and Theoretical, 2011, 44(9): 095305.

[8] Coudron M, Yuen H. Infinite randomness expansion with a constant number of devices[C]//Proceedings of the forty-sixth annual ACM symposium on Theory of computing, May 31, 2014, New York, NY, USA. New York: ACM, 2014: 427-436.

[9] Colbeck R, Renner R. Free randomness can be amplified[J]. Nature Physics, 2012, 8(6): 450-453.

[10] Herrero-Collantes M, Garcia-Escartin J C. Quantum random number generators[J]. Reviews of Modern Physics, 2017, 89: 015004.

[11] Sarkar A, Chandrashekar C M. Multi-bit quantum random number generation from a single qubit quantum walk[J]. Scientific Reports, 2019, 9(1): 1-11.

[12] Aharonov Y, Davidovich L, Zagury N. Quantum random walks[J]. Physical Review A, 1993, 48(2): 1687-1690.

[13] Venegas-Andraca S E. Quantum walks: a comprehensive review[J]. Quantum Information Processing, 2012, 11(5): 1015-1106.

[14] Chakraborty S, Novo L, Ambainis A, et al. Publisher's note: spatial search by quantum walk is optimal for almost all graphs[J]. Physical Review Letters, 2016, 116(24): 249901.

[15] Childs A M. Universal computation by quantum walk [J]. Physical Review Letters, 2009, 102(18): 180501.

[16] Schreiber A, Cassemiro K N, Potoček V, et al. Decoherence and disorder in quantum walks: from ballistic spread to localization[J]. Physical Review Letters, 2011, 106(18): 180403.

[17] Bian Z H, Li J, Qin H, et al. Realization of single-qubit positive-operator-valued measurement via a one-dimensional photonic quantum walk[J]. Physical Review Letters, 2015, 114(20): 203602.