Three criteria for quantum random number generators based on beam splitters

Karl Svozil
Vienna University of Technology

CDMTCS-362
March 2009

Centre for Discrete Mathematics and
Theoretical Computer Science
Three criteria for quantum random number generators based on beam splitters

Karl Svozil*

Institute for Theoretical Physics, Vienna University of Technology,
Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria

Abstract

We propose three criteria for the generation of random digital strings from quantum beam splitters: (i) three or more mutually exclusive outcomes corresponding to the invocation of three- and higher dimensional Hilbert spaces; (ii) the mandatory use of pure states in conjugated bases for preparation and detection; and (iii) the use of entangled singlet (unique) states for elimination of bias.

PACS numbers: 03.67.Hk,03.65.Ud

Keywords: Quantum information, quantum cryptography, singlet states, entanglement, quantum nonlocality
Randomness is a notorious property, both from theoretical and practical points of view. It is commonly accepted that there is a satisfactory definition [1] of infinite random sequences in terms of algorithmic incompressibility [2] as well as of the equivalent statistical tests [3]. Besides the obvious fact that all computable and physically operational entities are limited to finite objects and methods, algorithmic pseudo-random generators suffer from von Neumann’s verdict that [4]: “anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.” The halting probability Ω [5] shares three perplexing properties: it is computably enumerable (computable in a weak sense), provable random (which implies that Ω is non-computable), as well as infinitely knowledgeable in its role as a “rosetta stone” for all decision problems encodable as halting problems [1]. A few of its starting bits have been computed [6], yet due to its randomness, only finitely many bits of this number can ever be computed (irrespective of classical computational resources).

From the numerous random numbers generators based on physical processes (cf. Refs. [7–12] to name but a few), the use of single quanta (of light) subjected to beam splitters appears particularly promising [13–16] for the following reasons: (i) due to (ideally) single-quanta events, the physical systems are “elementary;” (ii) they can be controlled to a great degree; and (iii) they can be certified to be random relative to the postulates of quantum theory [17].

Three features of quantum theory directly relate to random sequences generated from beam splitter experiments: (i) the randomness of individual events (cf. Ref. [18, p. 866] and Ref. [19, p. 804]); (ii) complementarity [20, p. 7]; and (iii) value indefiniteness; i.e., the absence of two-valued states interpretable as “global” (i.e., valid on all observables) truth functions [21]. In order to fully implement these quantum features, we propose three improvements to existing protocols [13–16, 22–24].

The first criterion ensures that the quantum random number generators can be certified to be subject to quantum value indefiniteness. A necessary condition for this to apply is the possibility of three or more mutually exclusive outcomes in measurements of single quanta. Formally, this is due to the fact that violations of Bell-type inequalities, as well as proofs of Gleason’s and Kochen-Specker-type theorems are only realizable [25] in three- and higher dimensional Hilbert spaces. Only from three-dimensional vector space onwards it is possible to nontrivially interconnect bases through one (or up to \(n-2\) for \(n\)-dimensional Hilbert space) common base elements; i.e., vectors orthogonal to the rest of the elements of the interconnected bases. This can be explicitly demonstrated by certain, even dense [26–28], “dilutions” of bases, which break up the possibility to
interconnect, thus allowing value definiteness.

Of course, one could still argue that protocols based on two outcomes are still protected by quantum complementarity, and the full range of quantum indeterminism, so in particular quantum value indefiniteness, is not needed. There is also the possibility that the Born rule might be derived through some other argument (possibly from another set of axioms) than Gleason’s theorem [29–32]. However, there exist sufficiently many two-valued states on propositional structures with two outcomes to allow for a homeomorphic embedding of this structure into a classical Boolean algebra. In any case, it appears prudent to use all the “mind-boggling” features of quantum mechanics against cryptanalytic attacks on some quantum-generated sequence.

The resulting trivalent or multi-valued sequences can be easily “downgraded” or “translated” to binary sequences through elimination or identification without loss of randomness: systematically eliminating any symbol will transform a random sequence on an alphabet with \( n > 3 \) symbols into a random sequence on a an alphabet with \( n - 1 \geq 2 \) symbols [1].

The second criterion proposes the mandatory use of pure states from maximally conjugated bases for preparation and detection. This requirement deals with the single particle source of quantum random number generators. Although it is generally believed that mixed (nonpure) quantum states can be “produced” and operationalized “for all practical purposes,” one might cautiously argue that this may actually be a subjective statement on behalf of the observer: whereas the experimenter might “pretend” that the exact state leaving the particle source is unknown, it might still be possible to conceive of the state to be in some, albeit unknown but not principally unknowable, unique pure state. This is related to the question of whether or not mixed states should be thought of as merely subjective constructions which even in the epistemic view — as the wave function (the quantum state) representing a catalogue of expectations [33] — represent only certain partial, incomplete representations of systems which might be completely defined by a single unique context.

Even if one is unwilling to accept these principal concerns, it remains prudent not to expose the protocols for generating quantum randomness to the possibility of hidden regularities of the source. After all, beam splitters are just one-to-one bijective devices representable by reversible unitary operators [34–36]; a fact which can be seen by recombining the two paths by a second beam splitter in a Mach-Zender interferometer, thereby recovering the original signal. Thus, in order to assure quantum randomness, the beam splitter should not be considered as an isolated element, but has to be examined in combination with the source. In accordance with this principle,
a mismatch between state preparation and measurement guarantees that quantum complementarity ensures the indeterministic outcome. This can for instance be implemented by preparing the single particle in a pure state which corresponds to an element of a certain basis, and then measuring it in a different basis, in which the original state is in a coherent superposition of more than one states (cf. Ref. [13] and the first protocol using beam splitting polarizers in Ref. [15]).

Thirdly and finally, in order to eliminate any possible bias (for some “classical” methods to eliminate bias, we refer to Refs. [37–40]), we propose to utilize Einstein-Podolsky-Rosen type measurements of two quanta in a unique entangled state. Any state satisfying the uniqueness property [41] in at least two directions, such as the singlet states $\frac{1}{\sqrt{2}} (|+\rangle - |\rangle)$, $\frac{1}{\sqrt{3}} (-|00\rangle + | -1 + 1 \rangle + | + 1 - 1 \rangle)$, or $\frac{1}{2} (|\frac{3}{2}, -\frac{3}{2}\rangle - | -\frac{3}{2}, -\frac{3}{2}\rangle + | \frac{1}{2}, 1\rangle - | -\frac{1}{2}, \frac{1}{2}\rangle)$ of two spin-$\frac{1}{2}$, 1, and $\frac{3}{2}$ particles, could be used for this purpose. In that way, the outcome of one particle can be combined with the outcome of the other particle to eliminate bias.

For the sake of demonstration, suppose Alice and Bob share successive pairs of quanta in the singlet Bell state $\frac{1}{\sqrt{2}} (|+\rangle - |\rangle)$. Denote Alice’s and Bob’s outcomes in the $j^{th}$ measurement by $a_j$ and $b_j$, with the coding $a_j, b_j \in \{0, 1\}$, respectively. “Xoring” their combined results by a product modulo two of $a_j$ and $b_j$; i.e., by defining $s_j = a_j \oplus b_j = a_j b_j \mod 2$, yields a totally unbiased sequence $s_j$ of bits. Remarkably, as the state guarantees a 50:50 occurrence of 0’s and 1’s on either side, the associated bases of Alice and Bob need not even be maximally “apart”: one outcome on Alice’s side can be thought of as serving as “one time pad” in encrypting the other outcome on Bob’s side, and vice versa. Again, this method will be as good as the entangled particle source. In order to eliminate causal influences, the events recorded by Alice and Bob should be separated by strict Einstein locality conditions [42, 43]. Alternatively, in an adaptive “delayed choice” experiment the outcome on Alice’s side could be transferred to Bob, who adjusts his experiment (e.g., by changing the direction of spin state measurements) according to Alice’s input [44]. This method resembles the previously implemented self-calibration techniques utilizing coincidence measurements [22], entropy measures [24], and iterative sampling [23]. Whether or not it could also be used for classical angular momentum zero states “exploding” into two parts [45] remains unknown.

In summary we have argued that the present protocols for generating quantum random sequences with beam splitters should be improved to be certifiable against value definiteness and hidden bias of the source. We have also proposed a procedure to eliminate bias by using one particle of a singlet in an Einstein-Podolsky-Rosen configuration as a one-time pad for the other
Acknowledgements
The author gratefully acknowledges discussions with and suggestions by Cristian Calude, as well as the kind hospitality of the Centre for Discrete Mathematics and Theoretical Computer Science (CDMTCS) of the Department of Computer Science at The University of Auckland. This work was also supported by The Department for International Relations of the Vienna University of Technology.

* Electronic address: svozil@tuwien.ac.at; URL: http://tph.tuwien.ac.at/~svozil

[1] C. Calude, Information and Randomness—An Algorithmic Perspective (Springer, Berlin, 2002), 2nd edn.

[2] G. J. Chaitin, “Algorithmic Information Theory,” IBM Journal of Research and Development 21, 350–359, 496 (1977), reprinted in [46].

[3] P. Martin-Löf, “The definition of random sequences,” Information and Control 9, 602–619 (1966).
http://dx.doi.org/10.1016/0030-4018(87)90271-9

[4] J. von Neumann, “Various Techniques Used in Connection With Random Digits,” National Bureau of Standards Applied Math Series 3, 36–38 (1951), reprinted in John von Neumann, Collected Works, (Vol. V), A. H. Traub, editor, MacMillan, New York, 1963, p. 768.

[5] G. J. Chaitin, Exploring Randomness (Springer Verlag, London, 2001).

[6] C. S. Calude and M. J. Dinneen, “Exact Approximations of Omega Numbers,” International Journal of Bifurcation and Chaos 17, 1937–1954 (2007), CDMTCS report series 293.
http://dx.doi.org/10.1142/S0218127407018130

[7] The RAND Corporation, A Million Random Digits with 100,000 Normal Deviates Free Press Publishers (Knolls Atomic Power Lab. Report KAPL-3147, Glencoe, Illinois, 1955), the data digits are obtainable via http://www.rand.org/pubs/monograph_reports/2005/digits.txt.zip, the introduction via http://www.rand.org/pubs/monograph_reports/MR1418/index2.html.
http://www.rand.org/pubs/monograph_reports/MR1418/

[8] C. H. Vincent, “The generation of truly random binary numbers,” Journal of Physics E: Scientific
Instruments 3, 594–598 (1970).
http://dx.doi.org/10.1088/0022-3735/3/8/303

[9] T. Erber and S. Putterman, “Randomness of quantum mechanics: nature’s ultimate cryptogram?”
Nature 318, 41–43 (1985).
http://dx.doi.org/10.1038/318041a0

[10] H. Schmidt, “Quantum-Mechanical Random-Number Generator,” Journal of Applied Physics 41,
462–468 (1970).
http://dx.doi.org/10.1063/1.1658698

[11] A. J. Martino and G. M. Morris, “Optical random number generator based on photoevent locations,”
Applied Optics 30, 981–989 (1991).
http://ao.osa.org/abstract.cfm?URI=ao-30-8-981

[12] J. Walker, “HotBits Hardware,” (1986-2009).
http://www.fourmilab.ch/hotbits/hardware3.html

[13] K. Svozil, “The quantum coin toss—Testing microphysical undecidability,” Physics Letters A 143,
433–437 (1990).
http://dx.doi.org/10.1016/0375-9601(90)90408-G

[14] J. G. Rarity, M. P. C. Owens, and P. R. Tapster, “Quantum Random-number Generation and Key
Sharing,” Journal of Modern Optics 41, 2435–2444 (1994).
http://dx.doi.org/10.1080/09500349414552281

[15] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, “A Fast and Compact Quan-
tum Random Number Generator,” Review of Scientific Instruments 71, 1675–1680 (2000).
http://dx.doi.org/10.1063/1.1150518

[16] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, “Optical quantum random number
generator,” Journal of Modern Optics 47, 595–598 (2000).
http://dx.doi.org/10.1080/095003400147908

[17] A. Zeilinger, “The message of the quantum,” Nature 438, 743 (2005).
http://dx.doi.org/10.1038/438743a

[18] M. Born, “Zur Quantenmechanik der Stoßvorgänge,” Zeitschrift für Physik 37, 863–867 (1926).
http://dx.doi.org/10.1007/BF01397477

[19] M. Born, “Quantenmechanik der Stoßvorgänge,” Zeitschrift für Physik 38, 803–827 (1926).
http://dx.doi.org/10.1007/BF01397184
[20] W. Pauli, “Die allgemeinen Prinzipien der Wellenmechanik,” in Handbuch der Physik. Band V, Teil 1. Prinzipien der Quantentheorie I, S. Flügge, ed. (Springer, Berlin, Göttingen and Heidelberg, 1958), pp. 1–168.

[21] S. Kochen and E. P. Specker, “The Problem of Hidden Variables in Quantum Mechanics,” Journal of Mathematics and Mechanics (now Indiana University Mathematics Journal) 17, 59–87 (1967), reprinted in [47, pp. 235–263].
http://dx.doi.org/10.1512/iumj.1968.17.17004

[22] M. Hai-Qiang, W. Su-Mei, Z. Da, C. Jun-Tao, J. Ling-Ling, H. Yan-Xue, and W. Ling-An, “A Random Number Generator Based on Quantum Entangled Photon Pairs,” Chinese Physics Letters 21, 1961–1964 (2004).
http://dx.doi.org/0256-307X/21/1961

[23] P. X. Wang, G. L. Long, and Y. S. Li, “Scheme for a quantum random number generator,” Journal of Applied Physics 100, 056107 (2006).
http://dx.doi.org/10.1063/1.2338830

[24] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, “Secure self-calibrating quantum random-bit generator,” Physical Review A (Atomic, Molecular, and Optical Physics) 75, 032 334 (2007).
http://dx.doi.org/10.1103/PhysRevA.75.032334

[25] K. Svozil and J. Tkadlec, “Greechie diagrams, nonexistence of measures in quantum logics and Kochen–Specker type constructions,” Journal of Mathematical Physics 37, 5380–5401 (1996).
http://dx.doi.org/10.1063/1.531710

[26] C. D. Godsil and J. Zaks, “Coloring the sphere,” (1988), university of Waterloo research report CORR 88-12.

[27] D. A. Meyer, “Finite precision measurement nullifies the Kochen-Specker theorem,” Physical Review Letters 83, 3751–3754 (1999).
http://dx.doi.org/10.1103/PhysRevLett.83.3751

[28] H. Havlicek, G. Krenn, J. Summhammer, and K. Svozil, “Colouring the rational quantum sphere and the Kochen-Specker theorem,” J. Phys. A: Math. Gen. 34, 3071–3077 (2001).
http://dx.doi.org/10.1088/0305-4470/34/14/312

[29] A. M. Gleason, “Measures on the closed subspaces of a Hilbert space,” Journal of Mathematics and Mechanics (now Indiana University Mathematics Journal) 6, 885–893 (1957).
[30] I. Pitowsky, “Infinite and finite Gleason’s theorems and the logic of indeterminacy,” Journal of Mathematical Physics 39, 218–228 (1998).
http://dx.doi.org/10.1063/1.532334

[31] F. Richman and D. Bridges, “A constructive proof of Gleason’s theorem,” Journal of Functional Analysis 162, 287–312 (1999).
http://dx.doi.org/10.1006/jfan.1998.3372

[32] A. Dvurečenskij, Gleason’s Theorem and Its Applications (Kluwer Academic Publishers, Dordrecht, 1993).

[33] E. Schrödinger, “Die gegenwärtige Situation in der Quantenmechanik,” Naturwissenschaften 23, 807–812, 823–828, 844–849 (1935), English translation in [48] and [49, pp. 152-167].
http://dx.doi.org/10.1007/BF01491891,
http://dx.doi.org/10.1007/BF01491914,
http://dx.doi.org/10.1007/BF01491987

[34] Z. Ou, C. Hong, and L. Mandel, “Relation between input and output states for a beam splitter,” Optics Communications 63, 118–122 (1987).
http://dx.doi.org/10.1016/0030-4018(87)90271-9

[35] D. M. Greenberger, M. A. Horne, and A. Zeilinger, “Multiparticle interferometry and the superposition principle,” Physics Today 46, 22–29 (1993).

[36] A. Zeilinger, “General properties of lossless beam splitters in interferometry,” American Journal of Physics 49, 882–883 (1981).
http://dx.doi.org/10.1119/1.12387

[37] P. Elias, “The Efficient Construction of an Unbiased Random Sequence,” Ann. Math. Statist. 43, 865–870 (1972).
http://dx.doi.org/10.1214/aoms/1177692552

[38] Y. Peres, “Iterating Von Neumann’s procedure for extracting random bits,” The Annals of Statistics 20, 590–597 (1992).
http://www.jstor.org/stable/2242181

[39] M. Dichl, “Bad and Good Ways of Post-processing Biased Physical Random Numbers,” in Fast Software Encryption. Lecture Notes in Computer Science Volume 4593/2007, A. Biryukov, ed. (Springer, Berlin and Heidelberg, 2007), pp. 137–152, 14th International Workshop, FSE 2007, Luxembourg,
[40] P. Lacharme, “Post-Processing Functions for a Biased Physical Random Number Generator,” in *Fast Software Encryption. Lecture Notes in Computer Science Volume 5086/2008*, K. Nyberg, ed. (Springer, Berlin and Heidelberg, 2008), pp. 334–342, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers.
http://dx.doi.org/10.1007/978-3-540-74619-5_9

[41] K. Svozil, “Are simultaneous Bell measurements possible?” New Journal of Physics 8, 39 (2006).
http://dx.doi.org/10.1088/1367-2630/8/3/039

[42] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, “Violation of Bell’s Inequality under Strict Einstein Locality Conditions,” Phys. Rev. Lett. 81, 5039–5043 (1998).
http://dx.doi.org/10.1103/PhysRevLett.81.5039

[43] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. Langford, T. Jennewein, and A. Zeilinger, “Violation of local realism with freedom of choice,” (2008), eprint: arXiv:0811.3129.
http://arxiv.org/abs/0811.3129

[44] V. Jacques, E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect, and J.-F. Roch, “Experimental Realization of Wheeler’s Delayed-Choice Gedanken Experiment,” Science 315, 966–968 (2007).
http://dx.doi.org/10.1126/science.1136303

[45] A. Peres, “Unperformed experiments have no results,” American Journal of Physics 46, 745–747 (1978).
http://dx.doi.org/10.1119/1.11393

[46] G. J. Chaitin, *Information, Randomness and Incompleteness* (World Scientific, Singapore, 1990), 2nd edn., this is a collection of G. Chaitin’s early publications.

[47] E. Specker, *Selecta* (Birkhäuser Verlag, Basel, 1990).

[48] J. D. Trimmer, “The present situation in quantum mechanics: a translation of Schrödinger’s “cat paradox”,” Proceedings of the American Philosophical Society 124, 323–338 (1980), reprinted in [49, pp. 152-167].
http://www.tu-harburg.de/rzt/rzt/it/QM/cat.html

[49] J. A. Wheeler and W. H. Zurek, *Quantum Theory and Measurement* (Princeton University Press, Princeton, 1983).