scientific reports

Check for updates

OPEN

Binary quantum random number generator based on value indefinite observables

Cristian S. Calude[1] & Karl Svozil[2]✉

All quantum random number generators based on measuring value indefinite observables are at least three-dimensional because the Kochen–Specker Theorem and the Located Kochen–Specker Theorem are false in dimension two. In this article, we construct quantum random number generators based on measuring a three-dimensional value indefinite observable that generates binary quantum random outputs with the same randomness qualities as the ternary ones: the outputs are maximally unpredictable.

Keywords Three-dimensional quantum random generator quantum, Quantum value indefinite observable, Kochen–Specker Theorem, Located Kochen–Specker Theorem, Maximal unpredictable sequences

In 1946, J. von Neumann developed a pseudo-random generator (PRNG) with the following algorithm: "start with an initial random seed value, square it, and slice out the middle digits." A sequence obtained by repeatedly using this method exhibits *some* statistical properties of randomness. While the seeds completely determine PRNGs, hundreds of billions of pseudo-random numbers are used daily to encrypt electronic network data. Their pitfalls have been discovered in the Internet era. An example is the discovery in 2012 of a weakness in the encryption system RSA[1]; the flaw was traced to the numbers a PRNG has produced[2].

New types of random generators have been developed to remedy these flaws, specifically quantum random number generators (QRNGs). In the last decade, QRNGs proliferated because higher quality randomness is required in many areas, from cryptography, statistics, and information science to medicine and physics.

QRNGs are considered to be "better than PRNGs" because they are based on the "fundamental unpredictability of well-chosen and controlled quantum processes"[3], a weak assertion, particularly because it is well-known that the notion of "true randomness" interpreted as "lack of correlations" or "maximal randomness" is mathematically vacuous[4]. Can we construct QRNGs "provably better" than PRNGs? There are two types of QRNGs "theoretically certified": by the Bell inequalities[5–7] and by the Located Kochen–Specker Theorem[8,9], a form of the Kochen–Specker Theorem, see[10–12] for detailed reviews.

To date, only the second type of QRNGs has been mathematically proven to be better than *any* PRNG[8,13,14]. These QRNGs are three-dimensional: Since two-dimensional analogs of the Kochen–Specker Theorem as well as the Located Kochen–Specker Theorem are false, the generated sequences must be at least ternary[15]. Therefore, to obtain sequences of quantum random bits with the same quality of randomness, we need to apply a "three-to-two" symbol conversion algorithm that preserves the level of randomness. In this article, we pursue an alternative physical conversion: We construct quantum random generators based on measuring a three-dimensional value indefinite observable, and operationally—with physical means—generate binary quantum random outputs with the same quality of randomness as the ternary ones. Such outputs are maximally unpredictable[16]. Although the results are presented in $\mathbb{C}^3$, they can easily be generalized to $\mathbb{C}^n$ with $n > 3$.

Nomenclature and definitions

By n, we denote a positive integer. We denote by $\mathbb{C}$ the set of complex numbers and employ the standard quantum mechanical bra-ket notation. In this context, (unit) vectors in the Hilbert space $\mathbb{C}^n$ are represented as $|\cdot\rangle$. Our focus will be on one-dimensional projection observables. We denote by E_ψ the operator $E_\psi = |\psi\rangle\langle\psi|/|\langle\psi|\psi\rangle|$ projecting the Hilbert space $\mathbb{C}^n$ onto the linear subspace spanned by $|\psi\rangle$.

[1]School of Computer Science, University of Auckland, Private Bag 92019 Auckland, New Zealand. [2]Institute for Theoretical Physics, TU Wien, Wiedner Hauptstrasse 8-10/136, 1040 Vienna, Austria. ✉email: karl.svozil@tuwien.ac.at

In the following, we formalize hidden variables and the concept of value definiteness as in[9]. Fix $n > 1$. Consider $\mathcal{O} \subseteq \{E_\psi \mid |\psi\rangle \in \mathbb{C}^n\}$, a nonempty set of one-dimensional projection observables on the Hilbert space $\mathbb{C}^n$. A set $C \subset \mathcal{O}$ is a *context of* $\mathcal{O}$ if C has n elements (that is, $|C| = n$), and for all $E_\psi, E_\phi \in C$ with $E_\psi \neq E_\phi, \langle\psi|\phi\rangle = 0$.

Since distinct one-dimensional projection observables commute if and only if they project onto mutually orthogonal linear subspaces, a context C of $\mathcal{O}$ is a maximal set of compatible one-dimensional projection observables on $\mathbb{C}^n$. Due to the correspondence (up to a phase-shift) between unit vectors and one-dimensional projection observables, a context is uniquely defined by an orthonormal basis of $\mathbb{C}^n$.

A function is partial if it may be undefined for some values; a function defined everywhere is called total. The square root operation on the real numbers is partial because negative real numbers do not have real square roots. Partial functions were introduced in computability theory in 1930s[17] to model non-halting computations; they were used in quantum physics in[8].

A *value assignment function (on* $\mathcal{O}$*)* is a *partial two-valued* function $v : \mathcal{O} \to \{0, 1\}$, assigning values to some (possibly all) observables in $\mathcal{O}$. While we could allow v to be a function of both the observable E and the context C containing E, enabling contextual value assignments for the sake of compactness, we define v as a *noncontextual* value assignment function; this property is also called *contextual independence*.

An observable $E \in \mathcal{O}$ is *value definite (under* v*)* if $v(E)$ is defined; otherwise, it is *value indefinite (under* v*)*. Similarly, a context $\mathcal{O}$ is value definite (under v) if every observable $E \in \mathcal{O}$ is value definite.

Assuming contextual independence, if $v(E) = 1$, the measurement of E in every context containing E must yield the outcome 1. More generally, every value (in)definite observable E in one context must also value (in) definite in all other contexts containing E. This unique value, 0, 1, or undefined, depends on a particular state preparation and a specific collection of observables and contexts, which can be compactly represented by a hypergraph[18,19] (for more details, see later Sect. 4).

Let $\mathcal{O}$ be a set of one-dimensional projection observables on $\mathbb{C}^n$, and let $v : \mathcal{O} \to \{0, 1\}$ be a value assignment function. Then, v is *admissible* if the following two conditions hold for every context C of $\mathcal{O}$:

(a) Exclusivity: If there exists an $E \in C$ with $v(E) = 1$, then $v(E') = 0$, for all $E' \in C \setminus \{E\}$.
(b) Completeness: If there exists an $E \in C$ with $v(E') = 0$, for all $E' \in C \setminus \{E\}$, then $v(E) = 1$.

Admissibility is a weaker requirement than the usual assumption of the existence of a two-valued state—a total value assignment—because fewer than $n - 1$ elements in a context on $\mathbb{C}^n$ may be assigned the value 0, and no element is assigned the value 1. If the value assignment is partial, then the observables corresponding to these remaining elements are value indefinite.

For example, in $\mathbb{C}^3$, consider a context that has no element with either value 0 or 1 (and thus the value assignments of all three elements are undefined) and another context that has only a single element that is assigned the value 0, and the other two undefined.

However, if the value assignment on a particular set $\mathcal{O}$ of one-dimensional projection observables on $\mathbb{C}^n$ is total, then admissibility coincides with the standard definition of two-valued state(s).

Admissibility permits undefined values, and thus value indefiniteness of an observable E if both outcomes (0 and 1) of a measurement of E are incompatible with the definite values of other observables sharing a context with E. An explicit construction of such a configuration has been presented in[9].

If $v(E) = 1$, the measurement of every observable in every context C containing E must yield the outcome 1 for E. Consequently, to avoid contradiction, the outcomes of measurements for all the other observables in the context must be 0, and vice versa. On the other hand, if $v(E) = 0$, then the measurements of the other observables in C could yield the values 1 and 0 (as long as only one yields 1).

Three-dimensional QRNGs

This section introduces the physical principles and assumptions on which the notion of being "better than any PRNG" operates[8,13,14]. We then proceed to an explicit example based on a configuration of observables that realizes a QRNG according to these principles.

Principles of three-dimensional QRNGs

In the articles[8,9,20], the following protocol was used to construct a class of 3-dimensional QRNGs:

repeatedly locate a value indefinite observable in C^3*, measure it and record the output*.

The Kochen–Specker Theorem[10] guarantees only the existence of value indefinite observables, so the above protocol cannot use it. In contrast, the located version of the theorem[8,20] allows the construction of value indefinite observables, which can then be measured. In detail, consider a quantum system described by the state $|\psi\rangle$ in a Hilbert space $\mathbf{C}^n$, $n \geq 3$ and choose a value indefinite observable (quantum state) $|\phi\rangle$ that is neither orthogonal nor parallel to $|\psi\rangle$ $(0 < |\langle\psi||\phi\rangle| < 1)$. If the following three conditions are satisfied:

1. admissibility, as defined in Sect. 2,
2. non-contextuality, the outcome obtained by measuring a value definite observable does not depend on other compatible observables which may be measured alongside it, and
3. Eigenstate principle, if a quantum system is prepared in the state $|\psi\rangle$, then the projection observable P_ψ is value definite,

then the projection observable P_ϕ is value indefinite.

Furthermore, in[14], it was proved that given every probability distribution (p_1, p_2, p_3) ($\sum_i p_i = 1$ and $0 \leq p_i < 1$), a value indefinite quantum state can be constructed which, by a *universal* measurement, produces the outcomes with probabilities p_i.

The *universal* measurement is described by the unitary operator given by the unitary matrix[14]: This is obtained in terms of the spin-1 operator in the x-direction S_x, and its associated unit eigenvectors (through its spectral decomposition).

$$U_x = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & -\sqrt{2} & 1 \end{pmatrix}. \tag{1}$$

The quantum state (modular phase factors)

$$|\psi\rangle = \left(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}\right)^T, \tag{2}$$

is value indefinite[14], Theorem 4.1. and the result of the measurement of $|\psi\rangle$ on U_x with respect to the Cartesian standard basis produces the outcome $i \in \{0, 1, 2\}$ with probability p_i.

In fact, *every unitary operator is universal with respect to the value indefinite quantum state* $|\psi\rangle$. This is easy to see for the identity matrix, the most elementary case. As every arbitrary unitary operator U can be written in terms of two orthonormal bases, $\{|f_1\rangle, |f_2\rangle, |f_3\rangle\}$ and the Cartesian standard basis $\{|e_1\rangle, |e_2\rangle, |e_3\rangle\}$, as

$$U = |f_1\rangle\langle e_1| + |f_2\rangle\langle e_2| + |f_3\rangle\langle e_3|,$$

we have by (2):

$$|\psi\rangle = \sqrt{p_1}|e_1\rangle + \sqrt{p_2}|e_2\rangle + \sqrt{p_3}|e_3\rangle. \tag{3}$$

If we measure the value indefinite $|\psi\rangle$ by U in terms of the orthonormal basis $\{|f_1\rangle, |f_2\rangle, |f_3\rangle\}$

we get the outcome $i \in \{0, 1, 2\}$ with probability p_i. If we measure the output of U in terms of the Cartesian standard basis $\{|e_1\rangle, |e_2\rangle, |e_3\rangle\}$, then the input state has to be pre-processed: $U^{-1}|\psi\rangle = U^\dagger|\psi\rangle$, where † stands for the Hermitian adjoint.

Finally, using the main result in[21], running the above quantum protocol indefinitely, we *always* obtain a maximally unpredictable ternary sequence.

The first 3-dimensional QRNG[8] was constructed by (a) choosing the quantum state $|a\rangle = \left(0, 1, 0\right)^T$—which is value definite with respect to any context containing the observable $|a\rangle\langle a| = \text{diag}\left(1, 0, 0\right)$ because $|a\rangle$ is not in the context formed by the row vectors of U_x, (b) choosing a quantum state that is neither orthogonal nor parallel to it and (c) applying the measurement (1). The probabilities of the outputs 0, 1, and 2 generated by this quantum random generator are $\frac{1}{2}$, 0 and $\frac{1}{2}$, respectively, so theoretically, every sequence generated by this protocol is binary.

Does the probability 0 output endanger the applicability of the Kochen–Specker Theorem (see also the principle of three and higher-dimensionality of QRNGs[15])? The experimental analysis[22], based on the experiments reported in[23], suggested that the answer to the question posed in[24], is negative. A very small number of outputs 2 have been obtained.

We can now provide a theoretical negative answer using the *universal* measurement (1) to value indefinite quantum states.

By changing the input quantum state $|a\rangle = \left(0, 1, 0\right)^T$ to $|a\rangle = \left(1, 0, 0\right)^T$ and using the measurement (1) we obtain ternary quantum random numbers 0,1,2 generated with with probabilities 1/2, 1/4, 1/4, respectively, hence "genuine" ternary sequences.

As many current applications require random binary sequences, in[14], the computable alphabetic morphism $\varphi : \{0, 1, 2\} \to \{0, 1\}$

$$\varphi(x) = \begin{cases} 1, & \text{if } x = 0, \\ 0, & \text{if } x = 1, \\ 0, & \text{if } x = 2, \end{cases} \tag{4}$$

A slightly modified version of this alphabetic morphism was used to transform ternary sequences into binary ones and preserve their maximal unpredictability for the probability distributions $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$ and $\frac{1}{2}, \frac{1}{2}$, respectively; see[25] and Sect. 7 in[13]. Can we "quantize" the algorithmic post-processing (4)?

Quantum mechanically, this alphabetic morphism corresponds to a post-processing of the output of $U_x|a\rangle$. In general, by post-processing of a unitary transformation A we mean the unitary transformation $B = U'A$, where U' is a suitable unitary transformation. Physically, this corresponds to the serial composition of beam splitters, first applying A and then U'.

The post-processing of (4) results in the 'merging' of a state with three nonzero components (or coordinates with respect to a particular basis, here the Cartesian standard basis) into a state with two nonzero components. The merging is justified only if the corresponding input ports belong to the same context. In other words, the corresponding observables have mutually exclusive outcomes—a condition satisfied by a beam splitter realizing U_x. The schema is presented in Figure 1. Thereby, the unitary matrix is

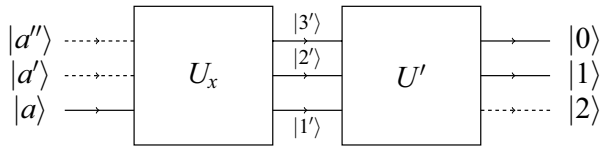

Figure 1. A horizontal schema of two beam splitters U_x and U' in serial composition $U'U_x$, with the 'input' state prepared in $|a\rangle$, and two 'active output' ports in states $|0\rangle$ and $|1\rangle$.

$$U' = \frac{1}{2\sqrt{2}} \begin{pmatrix} 1+\sqrt{2} & \sqrt{2} & 1-\sqrt{2} \\ 1-\sqrt{2} & \sqrt{2} & 1+\sqrt{2} \\ \sqrt{2} & -2 & \sqrt{2} \end{pmatrix} \tag{5}$$

corresponds to the alphabetic morphism φ. Then, the combined transformation is

$$U'U_x = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & \sqrt{2} \end{pmatrix}. \tag{6}$$

This unitary matrix $U'U_x$ corresponds to a beam splitter configuration that first allows a state $|a\rangle$ to be 'expanded' by a unitary matrix U_x with three nonzero components. Simultaneously, given $|a\rangle$, the output state $U_x|a\rangle$ is a value-indefinite observable 'merged' or 'folded' by the unitary matrix U', representing a serially concatenated beam splitter that transforms this state into one with two nonzero components of equal probability amplitudes. On input $|a\rangle$ the unitary transformation $U'U_x$ generates a ternary output with the probability distribution $\left(\frac{1}{2}, \frac{1}{2}, 0\right)$, which corresponds to the binary output with the probability distribution $\left(\frac{1}{2}, \frac{1}{2}\right)$.

How can we realize this transformation in terms of unitary equivalence? Two transformations, A and B, are unitarily equivalent if there exists a unitary matrix V such that $B = V^\dagger AV$, where $V^\dagger$ means the Hermitian adjoint, or conjugate transpose, of V. If V is real-valued then $V^\dagger = V^T$ is just the transpose V^T of V.

From Specht's Theorem[26,27], two unitary matrices are unitary equivalent if their eigenvalues coincide. In our case, both U_x in (1) as well as $U'U_x$ in (5) have one eigenvalue -1, and a double eigenvalue 1. More explicitly, the matrix

$$V = \begin{pmatrix} \frac{1}{2\sqrt{3}}\sqrt{2-\sqrt{2+\sqrt{3}}} & \frac{1}{2\sqrt{3}}\sqrt{2+\sqrt{2+\sqrt{3}}} & \sqrt{\frac{2}{3}} \\ -\frac{1}{\sqrt{6}}\sqrt{2-\sqrt{2+\sqrt{3}}} & -\frac{1}{\sqrt{6}}\sqrt{2+\sqrt{2+\sqrt{3}}} & \frac{1}{\sqrt{3}} \\ \frac{1}{2}\sqrt{2+\sqrt{2+\sqrt{3}}} & -\frac{1}{2}\sqrt{2-\sqrt{2+\sqrt{3}}} & 0 \end{pmatrix}$$

satisfies the equality $V^T U_x V = U'U_x$: this proves that the matrix U_x defined in (1) is unitarily equivalent to the matrix combination $U'U_x$ in (6).

Configuration of observables realizing the principles of three-dimensional QRNGs

For the sake of an example, take a configuration of observables enumerated in[28], Table I presented in Fig. 4, as $v(a) = 1$, in the context $\{b, 2, 3\}$, the observable 2 is value definite with $v(2) = 0$, whereas both observables b and 3 are value indefinite. Therefore, not all elements of $C \setminus \{E\}$ need to be value indefinite: Indeed, in the context $\{b, 2, 3\}$, the observable b is value indefinite. But from the two remaining elements in $\{b, 2, 3\} \setminus \{b\} = \{2, 3\}$, 2 is value definite with $v(2) = 0$, and 3 is value indefinite.

For the sake of an example, we shall use a hypergraph introduced in[9] and split it into segments serving as true-implies-false (TIFS) and true-implies-true (TITS) gadgets[28].

The hypergraph corresponding to the TIFS gadget in Fig. 2 illustrates the orthogonality relations among vector labels of the elements of hyperedges[29], as detailed in[28], Table I. By subsequently applying the admissibility rules[30], Figure (24.2.a) a single consistent value assignment, as in Fig. (2a) allows $v(a) = 1$ and $v(b) = 0$, whereas an inconsistent value assignment arises when assuming $v(a) = v(b) = 1$. Therefore, for any such configuration of quantum observables, there exists no classical admissible value assignment v satisfying the constraint on the input and output ports $v(a) = v(b) = 1$. Consequently, if a has a preselected input state $v(a) = 1$, then the value assignment $v(b)$ for the output state b cannot be 1. Therefore, $v(b)$ can only be 0 or undefined. In the latter case, b is value indefinite.

Conversely, the TITS gadget hypergraph in Fig. 3 illustrates the orthogonality relations among vector labels of the elements of hyperedges[29], as detailed in[28], Table I. Using the admissibility rules[30], Fig. (24.2.a) a single consistent value assignment, as in Fig. (3a) implies $v(a) = 1$ and $v(b) = 1$, in contrast with the value assignment when assuming $v(a) = 1$ and $v(b) = 0$.

As before, for any such configuration of quantum observables, there exists no classical admissible value assignment v satisfying the constraint on the input and output ports $v(a) = 1$ and $v(b) = 0$, respectively. Consequently, if a has a preselected input state $v(a) = 1$, then the value assignment $v(b)$ for the output state b must be either 1 or undefined, that is, value indefinite.

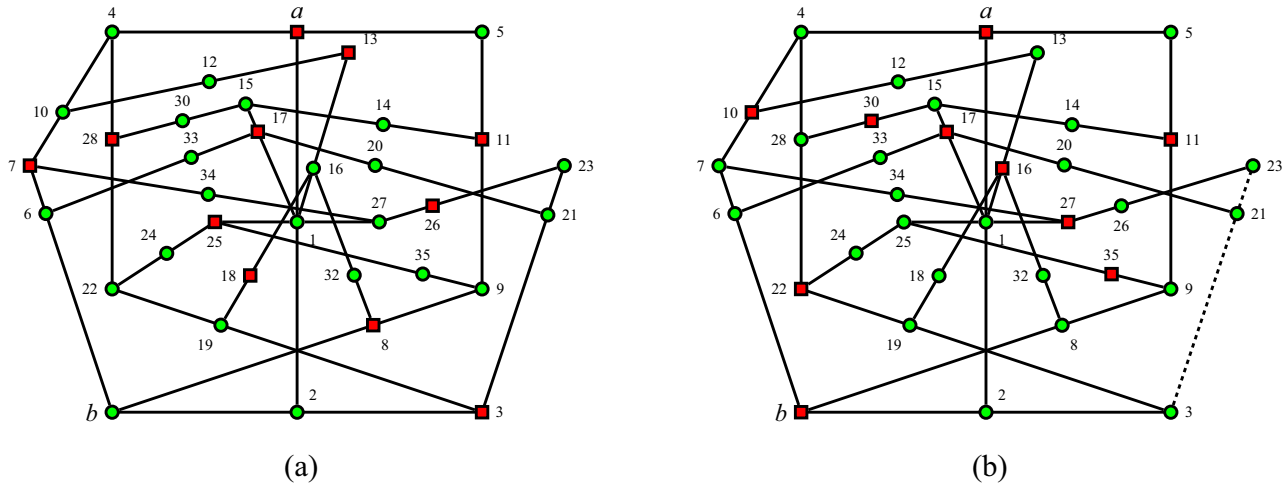

Figure 2. The TIFS gadget hypergraph for b given $\nu(a) = 1$, as well as the TITS gadget hypergraph for 3 given $\nu(a) = 1$, illustrates the orthogonality relations among vector labels of the elements of hyperedges[29] within a subset of quantum observables—also known as a faithful orthogonal representation[31] or coordinatization[32], as enumerated in[28], Table I. Red squares represent the value 1, and green circles represent the value 0. (**a**) A singular, consistent value assignment is obtained by assuming $\nu(a) = 1$ and $\nu(b) = 0$ and applying the admissibility rules successively[30], Figure (24.2.a). (**b**) An inconsistent value assignment is obtained by assuming $\nu(a) = \nu(b) = 1$ and applying the admissibility rules successively: the context $\{3, 21, 23\}$, shown dotted, contains three observables with the value 0; hence no admissible value assignment ν with the constraint on the input and output ports $\nu(a) = \nu(b) = 1$ exists. Therefore, if a has a preselected input state $\nu(a) = 1$, then the value assignment $\nu(b)$ for the output state b has either to be 0 or needs to be undefined, that is, b is value indefinite.

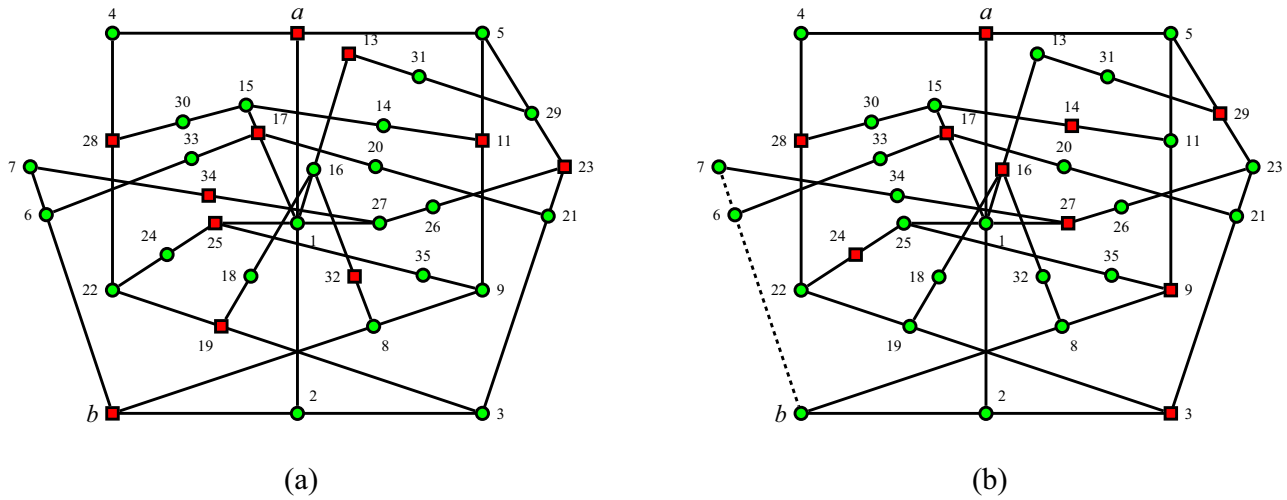

Figure 3. The TITS gadget hypergraph for b given $\nu(a) = 1$, as well as the TIFS gadget hypergraph for 3 given $\nu(a) = 1$, which is partly reflection symmetric along the $\{a, 1, 2\}$ context to the TIFS gadget hypergraph in Fig. 2, illustrates the orthogonality relations among vector labels of the elements of hyperedges[29] within a subset of quantum observables—also known as a faithful orthogonal representation[31] or coordinatization[32], as enumerated in[28], Table I. Red squares represent the value 1, and green circles represent the value 0. (**a**) A single consistent value assignment is obtained by assuming $\nu(a) = 1$ and $\nu(b) = 1$ and applying the admissibility rules successively[30], Figure (24.2.b). (**b**) An inconsistent value assignment is obtained by assuming $\nu(a) = 1$ and $\nu(b) = 0$ and applying the admissibility rules successively: because the context $\{6, 7, b\}$, shown dotted, contains three observables with the value 0, no admissible value assignment ν exists with the constraint on the input and output ports $\nu(a) = 1$ and $\nu(b) = 0$. Therefore, if a has a preselected input state $\nu(a) = 1$, then the value assignment $\nu(b)$. For the output state, b has to be 1 or undefined; that is, b is an indefinite value.

Therefore, the concatenation of the two hypergraphs depicting TIFS and TITS gadgets, originally introduced by Abbott and the authors in[28], and shown in Figs. 2 and 3 respectively, excludes both admissible value assignments of 0 and 1, rendering $\nu(b)$ undefined and thus the observable b value indefinite. Indeed, as in Fig. 4 the penetration of admissible value assignments is rather limited: if the system is prepared in state a, then admissibility merely allows "star-shaped" value definite observables along the two contexts $\{a, 1, 2\}$ and $\{a, 4, 5\}$. Note that

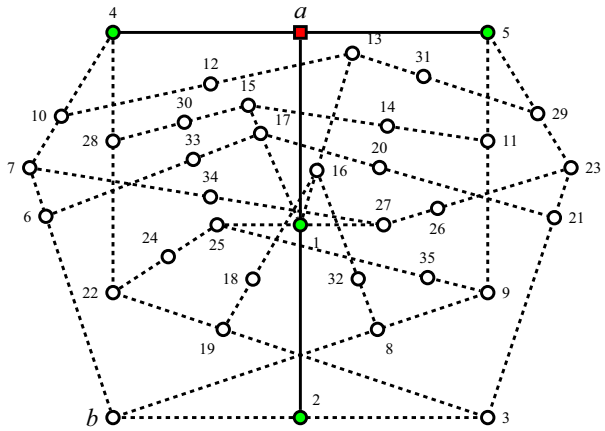

Figure 4. Concatenated hypergraph from the hypergraphs depicting TIFS and TITS gadgets shown in Figs. 2 and 3, respectively. Admissibility merely allows "star-shaped" value definite observables along the two contexts $\{a, 1, 2\}$ and $\{a, 4, 5\}$ if the system is prepared in state a.

all contexts $\{b, 2, 3\}$, $\{b, 6, 7\}$, and $\{b, 8, 9\}$, in which b is an element, have at least one more element with indefinite value. This is because the set of observables $O = \{a, b, 1, \ldots, 35\}$ is not unital[33], that is, all eight admissible (or global) value assignments must assign the value 1 to the observable 1, and thus the value 0 to a. There does not exist any value assignment $v(a) = 1$[30], Table 24.1. However, such value assignments with $v(a) = 1$ exist for the reduced set of observables $O \setminus \{29, 31\}$ and $O \setminus \{10, 12\}$ forming TIFS and TITS, respectively.

A very similar argument uses the same hypergraphs as in Figs. 2 and 3 as TITS and TIFS gadgets for 3 given $v(a) = 1$, respectively. Therefore, $v(3)$ is undefined, and the observable 3 is value indefinite.

Finally, what are the effects of errors and system imperfections? This question requires a technical long discussion, which will be the object of another study. Here, we argue only about the stability of the construction of our QRNGs due to variations in the indefinite observable value and measurement.

1. The stability of the choice of value indefinite observable comes from the Located Kochen–Specker Theorem[8,9] stated at the beginning of this section: The projection observable P_ϕ of *any state* $|\phi\rangle$ *such that* $0 < |\langle\psi||\phi\rangle| < 1$ is value indefinite.

2. The stability of the measurement comes from the result proved at the beginning of this section, stating that any unitary operator is *universal*.

Binary QRNG based on value indefinite observables

Subsequently, we present in detail an example of a configuration that illustrates a scenario where two observables within a context are value-indefinite, while the third observable is value-definite.

Here, value indefiniteness is contingent upon two factors: (i) the state that is (pre-)selected and prepared, and (ii) the specific set of observables arranged within a particular configuration of intertwined contexts. To establish value indefiniteness within this configuration, the (pre-)selected state and the state characterized by value indefiniteness must be elements of the setup. Therefore, any explicit assertion regarding the value indefiniteness of an observable should include a reference to the specific conditions upon which this claim relies.

Quantum versus classical models

A quantum realization of the construction in Figs. 2, 3 and 4 can be obtained from the faithful orthogonal representation of the elements of the hyperedges as vectors. One such representation was given in[28], Table I. It assigns the (superscript T indicates transposition) $|a\rangle = (1, 0, 0)^T$ to (the pure state) a, also representable by the trace-class one orthogonal (that is, positive, self-adjoint) projection operator whose matrix representation with respect to the Cartesian standard basis is a diagonal matrix $E_a = |a\rangle\langle a| = \mathrm{diag}\,(1, 0, 0)^T$ and $|b\rangle = \left(\frac{1}{\sqrt{2}}, \frac{1}{2}, \frac{1}{2}\right)^T$ as well as $|3\rangle = \left(\frac{1}{\sqrt{2}}, -\frac{1}{2}, -\frac{1}{2}\right)^T$ to the observables b and 3, respectively. Therefore, if the system is preselected (or prepared) in state $|a\rangle$, the output of the measurement of

$$E_b = |b\rangle\langle b| = \frac{1}{2}\begin{pmatrix} 1 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{\sqrt{2}} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

along $|b\rangle$ is obtained with the probability

$$\mathrm{Tr}\left(E_a \cdot E_b\right) = |\langle b|a\rangle|^2 = \frac{1}{2}.$$

Likewise, the output of the measurement of

$$E_3 = |3\rangle\langle 3| = \frac{1}{2}\begin{pmatrix} 1 & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{\sqrt{2}} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

along $|b\rangle$ is obtained with the probability

$$\mathrm{Tr}\left(E_a \cdot E_3\right) = |\langle 3|a\rangle|^2 = \frac{1}{2}.$$

As $|2\rangle$ is orthogonal to $|a\rangle$, $\mathrm{Tr}\left(E_a \cdot E_2\right) = |\langle 2|a\rangle|^2 = 0$, and the observable 2 is defined. Hence, when the observable a is preselected in the state $|a\rangle$, both observables b and 3 become value-indefinite (relative to admissibility), while observable 2 has value $v(2) = 0$. A quantum calculation confirmes what is posited in the (Located) Kochen–Specker Theorem, that both b and 3 occur with a probability of $\frac{1}{2}$.

To emphasize the three-dimensionality of the configuration, even if only two observables have nonzero probabilities, the sum of frequencies of the remaining quantum observables 2 and 3 in the complement $\{2, 3\}$ of the context $\{b, 2, 3\}$ containing b is 1/2. More explicitly, expressed in terms of orthogonal projection operators, the observable corresponding to $\{2, 3\}$ is given by a matrix corresponding to the orthogonal projection operator $E_{2,3}$:

$$E_{2,3} = E_2 + E_3 = |2\rangle\langle 2| + |3\rangle\langle 3| = \frac{1}{2}\begin{pmatrix} 1 & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{3}{2} & -\frac{1}{2} \\ -\frac{1}{\sqrt{2}} & -\frac{1}{2} & \frac{3}{2} \end{pmatrix}.$$

The vectors in $E_{2,3} \in \mathbb{C}^3$ are orthogonal to vectors in $E_b \in \mathbb{C}^3$. Together, $E_b + E_{2,3} = |b\rangle\langle b| + |2\rangle\langle 2| + |3\rangle\langle 3| = I_3$ yield the identity $I_3 = \mathrm{diag}\,(1, 1, 1)$.

Classically, there is no realization of the set of observables $O = \{a, b, 1, \ldots, 35\}$ in Fig. 4 because some elements of O are assigned the value 0 for all two-valued states[30], Table 24.1, hence not separable[10], Theorem 0. This result holds for total value assignments—a stronger assumption than admissibility. Indeed, in this case the "central" point 1 must be classically assigned the value $v(1) = 1$, and, therefore, all remaining eight elements $\{a, 2, 13, 15, 16, 17, 25, 27\}$ in the four contexts $\{a, 1, 2\}, \{1, 13, 16\}, \{1, 15, 17\}$, and $\{1, 25, 27\}$ containing 1 to be zero.

Finally, using the Eigenstate principle and Theorem 5.6 in[14], we deduce that the QRNG described above generates maximally unpredictable binary random digits.

Beam splitter realizations

Figure 5 presents a triangular array of quantum beam splitters which physically transforms the preparation context $\{a, 4, 5\}$ into the measurement context $\{b, 2, 3\}$.

The vector coordinatization[28], Table I $|a\rangle = \left(1, 0, 0\right)^T$, $|b\rangle = \left(\frac{1}{\sqrt{2}}, \frac{1}{2}, \frac{1}{2}\right)^T$, $|2\rangle = \left(0, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)^T$, $|3\rangle = \left(\frac{1}{\sqrt{2}}, -\frac{1}{2}, -\frac{1}{2}\right)$, $|4\rangle = \left(0, 0, 1\right)^T$, and $|5\rangle = \left(0, 1, 0\right)^T$ computes the unitary transformation matrix[34,35] that transforms the input state $|a\rangle$ into the output state $|b\rangle$, the input state $|4\rangle$ into the output state $|2\rangle$, and the input state $|5\rangle$ into the output state $|3\rangle$:

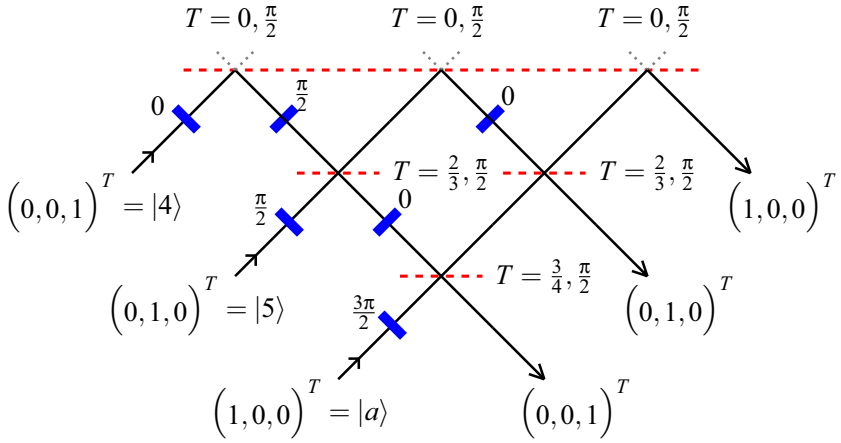

Figure 5. A triangular array of quantum mechanical beam splitters is a realization of the input or preparation context $\{a, 4, 5\}$ and the output or measurement context $\{b, 2, 3\}$.

$$U = |b\rangle\langle a| + |2\rangle\langle 4| + |3\rangle\langle 5| = \frac{1}{2}\begin{pmatrix} \sqrt{2} & \sqrt{2} & 0 \\ 1 & -1 & \sqrt{2} \\ 1 & -1 & -\sqrt{2} \end{pmatrix}.$$

This unitary matrix realizes a beam splitter[36–38] using the parametrization of the unitary group[39]. Besides phase shifters operating in one-dimensional subspaces (in this particular case, all zero but one), these concatenations of optical elements contain beam splitters operating in two-dimensional subspaces. These beam splitters have a parametrization unitary matrix

$$B(\omega, \varphi) = \begin{pmatrix} \sin\omega & \cos\omega \\ e^{-i\varphi}\cos\omega & -e^{-i\varphi}\sin\omega \end{pmatrix}.$$

depending on two parameters: ω is the transmissivity $T = \sin^2\omega$ and reflectivity $R = 1 - T = \cos^2\omega$, and φ is the phase change at reflection.

The output wave function, given the input wave function, is the coherent superposition of the contributions of all the possible forward passes from the input port(s) toward the output port(s). Thereby, the transmissibility and reflectivity contribute by the square roots $\sqrt{T} = \sin\omega$ and reflectivity $\sqrt{R} = \cos\omega$ of T and R[40]. The sum of the phase shifts between reflected and transmitted waves excited by a wave incident from the side of the beam splitter, and the corresponding phase shift for a wave incident from the opposing side, contribute with π[41]. For a symmetric lossless dielectric plate[42], the reflected and transmitted parts are $\pi/2$ out of phase[40,43].

The relations (7) present a computation of the effects on the input ports of the beam splitter in Fig. 5 by successive applications of phase shifts and beam mixings.

$$\begin{aligned}
|a\rangle &\longrightarrow e^{i\frac{3\pi}{2}}\left\{e^{i\frac{\pi}{2}}\sqrt{\frac{1}{4}}\begin{pmatrix}0\\0\\1\end{pmatrix} + \sqrt{\frac{3}{4}}\left[e^{i\frac{\pi}{2}}\sqrt{\frac{1}{3}}\begin{pmatrix}0\\1\\0\end{pmatrix} + \sqrt{\frac{2}{3}}e^{i\frac{\pi}{2}}\begin{pmatrix}1\\0\\0\end{pmatrix}\right]\right\} = |b\rangle, \\
|5\rangle &\longrightarrow e^{i\frac{\pi}{2}}\left(e^{i\frac{\pi}{2}}\sqrt{\frac{1}{3}}\left\{\sqrt{\frac{3}{4}}\begin{pmatrix}0\\0\\1\end{pmatrix} + e^{i\frac{\pi}{2}}\sqrt{\frac{1}{4}}\left[e^{i\frac{\pi}{2}}\sqrt{\frac{1}{3}}\begin{pmatrix}0\\1\\0\end{pmatrix} + e^{i\frac{\pi}{2}}\sqrt{\frac{2}{3}}\begin{pmatrix}1\\0\\0\end{pmatrix}\right]\right\}\right. \\
&\qquad \left. + \sqrt{\frac{2}{3}}e^{i\frac{\pi}{2}}\left[\sqrt{\frac{2}{3}}\begin{pmatrix}0\\1\\0\end{pmatrix} + e^{i\frac{\pi}{2}}\sqrt{\frac{1}{3}}e^{i\frac{\pi}{2}}\begin{pmatrix}1\\0\\0\end{pmatrix}\right]\right) = |3\rangle, \\
|4\rangle &\longrightarrow e^{i\frac{\pi}{2}}e^{i\frac{\pi}{2}}\left(\sqrt{\frac{2}{3}}\left\{\sqrt{\frac{3}{4}}\begin{pmatrix}0\\0\\1\end{pmatrix} + e^{i\frac{\pi}{2}}\sqrt{\frac{1}{4}}\left[e^{i\frac{\pi}{2}}\sqrt{\frac{1}{3}}\begin{pmatrix}0\\1\\0\end{pmatrix} + \sqrt{\frac{2}{3}}e^{i\frac{\pi}{2}}\begin{pmatrix}1\\0\\0\end{pmatrix}\right]\right\}\right. \\
&\qquad \left. + e^{i\frac{\pi}{2}}\sqrt{\frac{1}{3}}e^{i\frac{\pi}{2}}\left[\sqrt{\frac{2}{3}}\begin{pmatrix}0\\1\\0\end{pmatrix} + e^{i\frac{\pi}{2}}\sqrt{\frac{1}{3}}e^{i\frac{\pi}{2}}\begin{pmatrix}1\\0\\0\end{pmatrix}\right]\right) = |2\rangle.
\end{aligned} \tag{7}$$

Beam splitter as an analogy of Ariadne's tread

How come can we quantum mechanically 'spread' a qutrit state of input into a coherent superposition of all qutrit states, and finally end up with a binary sequence—very much like two Hadamard unitary transformations first 'spread' a qubit, and then (up to a constant scalar factor) 'fold it back' into its original state? This is where the allegory of Ariadne's thread comes up in the configuration of a beam splitter. Consider a general quantum beam splitter with $m > 0$ nonzero inputs and $n > 0$ nonzero output ports. As long as the sum of probabilities of preparation and detection on both the respective input and the output ports adds up to one, a quantum realization is feasible[36–38]. Indeed, all that is necessary is that the input and the output state are tailored according to the probability amplitudes (phases do not count).

Considering this scenario, one may question: What happens to quantum unitarity, especially if $m \neq n$? For instance, with such a beam splitter, we could 'merge' two input ports into one output port ($n = m + 1 = 2$). Alternatively, one could 'split' a single input port into (a coherent superposition, resulting in) two output ports ($m = n + 1 = 2$). For example, the associated unitary three-dimensional matrix entries could be

$$U_{2\text{-to-}1} = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}, U_{1\text{-to-}2} = \begin{pmatrix} 0 & \cdot & \cdot \\ \frac{1}{\sqrt{2}} & \cdot & \cdot \\ \frac{1}{\sqrt{2}} & \cdot & \cdot \end{pmatrix}, \tag{8}$$

where, for $U_{2\text{-to-}1}$ (or $U_{1\text{-to-}2}$) the remaining rows (or columns) could fill up with unit vectors forming the orthonormal basis of a two-dimensional subspace orthogonal to $\begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$ (or its Hermitian conjugate).

Indeed, to obtain a binary sequence, one could 'post-process' the beam splitter arrangement in Fig. 5 by a beam splitter corresponding to the following real-valued unitary matrix:

$$U'_{2\text{-to-}1} = \frac{1}{\sqrt{2}}\begin{pmatrix} \sqrt{2} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{pmatrix}. \tag{9}$$

When the input state is $|a\rangle$, the resulting output state is $U'_{2\text{-to-}1}U|a\rangle$, with U and $U'_{2\text{-to-}1}$ defined in (6) and (9), respectively.

More explicitly,

$$\frac{1}{\sqrt{2}}\begin{pmatrix}\sqrt{2} & 0 & 0\\ 0 & 1 & 1\\ 0 & 1 & -1\end{pmatrix}\frac{1}{2}\begin{pmatrix}\sqrt{2} & \sqrt{2} & 0\\ 1 & -1 & \sqrt{2}\\ 1 & -1 & -\sqrt{2}\end{pmatrix}\begin{pmatrix}1\\0\\0\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\\0\end{pmatrix}.$$

A particle in state $|a\rangle$ will end up in either the first or second port with probability $\frac{1}{2}$ and be registered in the third port with probability 0.

Two questions arise: (i) The unitary quantum evolution—of the von Neumann type 'Vorgang' 2[44,45], referred to as 'process 2' by Everett[46]—that needs to be one-to-one, and it appears to be compromised. (ii) Can this problem be discussed in terms of value indefiniteness and partial value assignments?

The first question can be quickly addressed: The beam splitter examples discussed here show that concentration on a partial array of input and output ports cannot represent the whole picture. The full specification of a beam splitter in n dimensions has the same number n of input and output ports. The quantum evolution is incomplete if some input and output contexts are not considered. Because any unitary transformation can be represented by a bijective map of the vectors of one orthonormal basis—the input context—into the vectors of another orthonormal basis[34,35]—the output context. Suppose we also allow incomplete mappings of vectors from one context into some vectors of another context. This could not exclude mappings that are not one-to-one. Therefore, only the totality of those one-to-one vector transformations relating to two orthonormal bases forms a forward- and backward-reversible transformation.

The context-to-context unitary mapping can be viewed as a sort of 'rescrambling' of information contained in the channels or ports of the beam splitter[47,48]. Thereby, the 'latent' and 'omitted' ports act as Ariadne's thread that must be considered for reversibility. The situation resembles a zero-sum game encountered in entanglement swapping[49,50].

Although the results in this article have been proved in $\mathbb{C}^3$, they can easily be generalized to $\mathbb{C}^n$ with $n > 3$. Therefore, by 'merging' or 'folding' two or more observables of the context, represented by the orthogonal projection operators $E_2, \ldots, E_n$, we never leave the n-dimensional Hilbert space $\mathbb{C}^n$, because $E_{2,\ldots,n}\mathbb{C}^n$ is the $(n-1)$ -dimensional Hilbert space spanned by the vectors $|e_i\rangle$ that form $E_i = |e_i\rangle\langle e_i|$, with $i = 2, \ldots, n$. The vectors in $E_{2,\ldots,n}\mathbb{C}^n$ are orthogonal to the one-dimensional subspace $E_1\mathbb{C}^n$ spanned by $|e_1\rangle$, and the vectors $|e_1\rangle, \ldots, |e_1\rangle$ form an orthonormal basis.

Regarding the second question, we may say that value indefiniteness 'prevails' over value definiteness: whenever a value indefinite observable is involved, the 'merged' observables 'inherit' value indefiniteness.

Conclusions

We have proved that for every probability distribution (p_1, p_2, p_3) $(\sum_i p_i = 1 \text{ and } 0 \leq p_i < 1)$, one can construct a value indefinite quantum state which, by *every unitary measurement*, produces the outcomes with probabilities p_i.

Based on this result, the quantization of an algorithmic pre-processing binary method[25] and the quantum 'merging' technique, we have constructed quantum random generators based on measuring a three-dimensional value indefinite observable producing binary quantum random outputs with the same randomness qualities as the ternary ones; their outputs are maximally unpredictable[16]. The results can easily be generalized from $\mathbb{C}^3$ to $\mathbb{C}^n$ with $n > 3$.

Data availability

All data generated or analysed during this study are included in this published article.

Received: 8 February 2024; Accepted: 19 May 2024
Published online: 04 June 2024

References

1. Markoff, J. *Flaw Found in an Online Encryption Method*, (New York Times, published on Feb. 14, 2012), https://www.nytimes.com/2012/02/15/technology/researchers-find-flaw-in-an-online-encryption-method.html (2012).
2. Lenstra, A. K., Hughes, J. P., Augier, M., Bos, J. W., Kleinjung, T. & Wachter, C. *Ron was wrong, Whit is right*, Santa Barbara: IACR: 17, Cryptology ePrint Archive, Paper 2012/064, Cryptology ePrint Archive: 2012/064, https://eprint.iacr.org/2012/064.pdf (2012).
3. Quantique, SA., *What is the Q in QRNG? Random Number Generation. White Paper*, https://marketing.idquantique.com/acton/attachment/11868/f-0226/1/ (2020).
4. Calude, C. S. *Information and Randomness—An Algorithmic Perspective*. https://doi.org/10.1007/978-3-662-04978-5 (Springer, Berlin, 2002).
5. Pironio, S. *et al.* Random numbers certified by Bell's theorem. *Nature* **464**, 1021. https://doi.org/10.1038/nature09008 (2010).
6. Nonaka, M., Agüero, M., Kovalsky, M. & Hnilo, A. Testing randomness of series generated in an optical Bell's experiment. *Appl. Opt.* **62**, 3105. https://doi.org/10.1364/AO.477218 (2023).
7. Hayashi, M. & Koshiba, T. *Quantum Inform. Process.* **21**, 291. https://doi.org/10.1007/s11128-022-03639-x (2022).
8. Abbott, A. A., Calude, C. S., Conder, J. & Svozil, K. Strong Kochen–Specker theorem and incomputability of quantum randomness. *Phys. Rev. A* **86**, 062109. https://doi.org/10.1103/PhysRevA.86.062109 (2012).
9. Abbott, A. A., Calude, C. S. & Svozil, K. A variant of the Kochen–Specker theorem localising value indefiniteness. *J. Math. Phys.* **56**, 102201. https://doi.org/10.1063/1.4931658 (2015).
10. Kochen, S. & Specker, E. P. *J. Math. Mech.* **17**, 59. https://doi.org/10.1512/iumj.1968.17.17004 (1968).
11. Landsman, K. Randomness? What randomness. *Found. Phys.* **50**, 61. https://doi.org/10.1007/s10701-020-00318-8 (2020).
12. Budroni, C., Cabello, A., Gühne, O., Kleinmann, M. & Larsson, J.-A. Kochen–Specker contextuality. *Rev. Modern Phys.* **94**, 045007. https://doi.org/10.1103/RevModPhys.94.045007 (2022).

13. Agüero Trejo, J. M. & Calude, C. S. A new quantum random number generator certified by value indefiniteness. *Theor. Comput. Sci.* **862**, 3. https://doi.org/10.1016/j.tcs.2020.08.014 (2021).
14. Agüero Trejo, J. M. & Calude, C. S. Proceedings of the Royal Society A **479**, 1 https://doi.org/10.1098/rspa.2022.0543 (2023).
15. Svozil, K. Three criteria for quantum random-number generators based on beam splitters. *Phys. Rev. A* **79**, 054306 https://doi.org/10.1103/PhysRevA.79.054306 (2009).
16. Abbott, A. A., Calude, C. S. & Svozil, K. *Fields of Logic and Computation II*, inedited by L. D. Beklemishev, A. Blass, N. Dershowitz, B. Finkbeiner, and W. Schulte (Springer, Cham, Switzerland, 2015b), vol. 9300 of *Lecture Notes in Computer Science*, pp. 69–86, ISBN 978-3-319-23533-2, arXiv:1403.2738, https://doi.org/10.1007/978-3-319-23534-9_4.
17. Davis, M. *Computability and Unsolvability* (McGraw-Hill, New York, 1958).
18. Greechie, R. J. *J. Combinatorial Theor. Ser. A* **10**, 119. https://doi.org/10.1016/0097-3165(71)90015-X (1971).
19. Bretto, A. *Hypergraph Theory, Mathematical Engineering*. https://doi.org/10.1007/978-3-319-00080-0 (Springer, Cham, 2013).
20. Calude, C. S. & Svozil, K. Quantum randomness and value indefiniteness. *Adv. Sci. Lett.* **1**, 165. https://doi.org/10.1166/asl.2008.016 (2008).
21. Abbott, A. A., Calude, C. S. & Svozil, K. A non-probabilistic model of relativised predictability in physics. *Information* **6**, 773. https://doi.org/10.3390/info6040773 (2015).
22. Abbott, A. A., Calude, C. S., Dinneen, M. J. & Huang, N. Experimentally probing the algorithmic randomness and incomputability of quantum randomness. *Phys. Scripta* **94**, 045103. https://doi.org/10.1088/1402-4896/aaf36a (2019).
23. Kulikov, A., Jerger, M., Potočnik, A., Wallraff, A. & Fedorov, A. Realization of a quantum random generator certified with the Kochen–Specker theorem. *Phys. Rev. Lett.* **119**, 240501. https://doi.org/10.1103/PhysRevLett.119.240501 (2017).
24. Fedorov, A. *Binary Beam Splitters May Not Be Protected by Value Indefiniteness as Tertiary Ones* (2022), private communications.
25. Calude, C. S., Celine, K. F., Gao, Z., Jain, S., Staiger, L. & Stephan, F. *Theoret. Comput. Sci.* **894**, 31. https://doi.org/10.1016/j.tcs.2021.09.005 (2021).
26. Horn, R. A. & Johnson, C. R. *Matrix Analysis* (Cambridge University Press, New York, 2013).
27. Dokovic, D. Z. & Johnson, C. R. Unitarily achievable zero patterns and traces of words in A and A. *Linear Algebra Appl.* **421**, 63. https://doi.org/10.1016/j.laa.2006.03.002 (2007).
28. Cabello, A., Portillo, J. R., Solís, A. & Svozil, K. Minimal true-implies-false and true-implies-true sets of propositions in noncontextual hidden-variable theories. *Phys. Rev. A* **98**, 012106. https://doi.org/10.1103/PhysRevA.98.012106 (2018).
29. Lovász, L. On the Shannon capacity of a graph. *IEEE Trans. Inform. Theory* **25**, 1. https://doi.org/10.1109/TIT.1979.1055985 (1979).
30. Svozil, K. *Quantum, Probability, Logic: The Work and Influence of Itamar Pitowsky*, in edited by M. Hemmo and O. Shenker, vol. 1 of *Jerusalem Studies in Philosophy and History of Science (JSPS)*, pp. 521–544, ISBN 978-3-030-34316-3, arXiv:1812.08646, https://doi.org/10.1007/978-3-030-34316-3_24 (Springer International Publishing, Cham, 2020).
31. Solís-Encina, A. & Portillo, J. R. *Orthogonal representation of graphs*, arXiv:1504.03662, https://doi.org/10.48550/arXiv.1504.03662 (2015).
32. Pavičić, M. & Megill, N. D. Vector generation of quantum contextual sets in even dimensional Hilbert spaces. *Entropy*. https://doi.org/10.3390/e20120928 (2018).
33. Svozil, K. & Tkadlec, J. *J. Math. Phys.* **37**, 5380. https://doi.org/10.1063/1.531710 (1996).
34. Schwinger, J. *Proceedings of the National Academy of Sciences (PNAS)* **46**, 570. https://doi.org/10.1073/pnas.46.4.570 (1960).
35. Joglekar, S. D. *Mathematical Physics: The Basics* (CRC Press, Boca Raton, Florida, 2007).
36. Reck, M. & Zeilinger, A. in *Quantum Interferometry*, edited by F. De Martini, G. Denardo, and A. Zeiliger (World Scientific, Singapore, 1994), pp. 170–177, proceedings of the Adriatico Workshop Adriatico Workshop, Trieste, Italy. https://doi.org/10.1142/2131 (1993).
37. Reck, M., Zeilinger, A., Bernstein, H. J. & Bertani, P. *Phys. Rev. Lett.* **73**, 58. https://doi.org/10.1103/PhysRevLett.73.58 (1994).
38. de Guise, H., Di Matteo, O. & Sánchez-Soto, L. L. Simple factorization of unitary transformations. *Phys. Rev. A* **97**, 022328. https://doi.org/10.1103/PhysRevA.97.022328 (2018).
39. Murnaghan, F. D. *The Unitary and Rotation Groups*, vol. 3 of *Lectures on Applied Mathematics* (Spartan Books, Washington, 1962).
40. Greenberger, D. M., Horne, M. A. & Zeilinger, A. *Phys. Today* **46**, 22. https://doi.org/10.1063/1.881360 (1993).
41. Zeilinger, A. *Am. J. Phys.* **49**, 882. https://doi.org/10.1119/1.12387 (1981).
42. Lai, H. M., Leung, A. F. & Wong, P. Y. Phase difference between the transmitted and the reflected optical fields of a symmetric dielectric plate. *Am. J. Phys.* **53**, 1103. https://doi.org/10.1119/1.14042 (1985).
43. Degiorgio, V. Phase shift between the transmitted and the reflected optical fields of a semireflecting lossless mirror. *Am. J. Phys.* **48**, 81. https://doi.org/10.1119/1.12238 (1980).
44. von Neumann, J. *Mathematische Grundlagen der Quantenmechanik* (Springer, Berlin, Heidelberg, 1996).
45. von Neumann, J. *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, 1955).
46. Everett, H. III. *Rev. Modern Phys.* **29**, 454. https://doi.org/10.1103/RevModPhys.29.454 (1957).
47. Schrödinger, E. *Naturwissenschaften* **23**, 823. https://doi.org/10.1007/BF01491914 (1935).
48. Zeilinger, A. *Found. Phys.* **29**, 631. https://doi.org/10.1023/A:1018820410908 (1999).
49. Bennett, C. H. *et al. Phys. Rev. Lett.* **70**, 1895. https://doi.org/10.1103/PhysRevLett.70.1895 (1993).
50. Peres, A. Delayed choice for entanglement swapping. *J. Mod. Opt.* **47**, 139. https://doi.org/10.1080/09500340008244032 (2000).

Acknowledgements

We thank J. M. Agüero Trejo for comments, which improved the presentation, and M. Reck for the Mathematica code producing the generalized beam-splitter setup for an arbitrary unitary transformation. The research of K. Svozil was funded in whole or in part by the Austrian Science Fund (FWF), Grant-DOI: 10.55776/I4579. For open access purposes, the author has applied a CC BY public copyright license to any author accepted manuscript version arising from this submission.

Author contributions

C.S.C. and K.S. have contributed equally to the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to K.S.

Reprints and permissions information is available at www.nature.com/reprints.