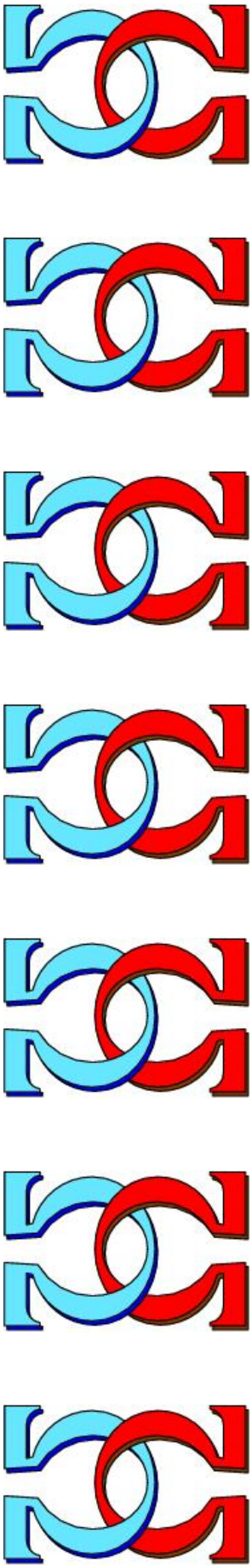


CDMTCS
Research
Report
Series

Binary Quantum Random Number Generator Based on Value Indefinite Observables

C. S. Calude[1] and K. Svozil[2]

[1]School of Computer Science, University of Auckland, New Zealand
[2]Institute for Theoretical Physics, TU Wien, Austria

CDMTCS-575
December 2023

Centre for Discrete Mathematics and
Theoretical Computer Science

Binary Quantum Random Number Generator Based on Value Indefinite Observables

Cristian S. Calude[1,*] and Karl Svozil[2,†]

[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*

(Dated: December 19, 2023)

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 a quantum random number generator based on measuring a three-dimensional value indefinite observable that generates binary quantum random outputs with the same randomness qualities as the ternary ones: its 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

I. INTRODUCTION

All known quantum random number generators, which rely on measuring value-indefinite observables [1–3] are three-dimensional. This is because the Kochen-Specker Theorem [4] and the Located Kochen-Specker Theorem [1, 5] are false in dimension two. In this article, we construct a quantum random generator based on measuring a three-dimensional value indefinite observable generating binary quantum random outputs with the same randomness qualities as the ternary ones; its outputs are maximally unpredictable [6]. Our results in $\mathbb{C}^3$ can easily be generalized to $\mathbb{C}^n$ with $n > 3$.

This is possible because if we fix a context C in $\mathbb{C}^n, n > 2$ and a value indefinite observable $E \in C$ (under a value assignment function v), then we can locate a value indefinite observable $G \in C$ such that $v(G) = \sum_{E' \in C \setminus \{E\}} v(E')$. Hence, the measurements of the observables E and G produce maximally unpredictable binary quantum random outputs.

II. NOMENCLATURE AND DEFINITIONS

By n, we denote a positive integer greater than 1. 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 $|\psi\rangle$.

In the following, we formalize hidden variables and the concept of value definiteness as in [5].

Fix $n > 1$. Consider $O \subseteq \{E_\psi \mid |\psi\rangle \in \mathbb{C}^n\}$, a nonempty set of one-dimensional projection observables on the Hilbert space $\mathbb{C}^n$. A set $C \subset O$ is a *context of* 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 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 [7–9] to model non-halting computations; they were used in quantum physics in [1]. A *value assignment function (on O)* is a partial two-valued function $v : O \to \{0,1\}$, assigning values to some (possibly all) observables in 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, that is, $v(E,C) = v(E)$.

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

Let O be a set of one-dimensional projection observables on $\mathbb{C}^n$, and let $v : O \to \{0,1\}$ be a value assignment function. Then, v is *admissible* if the following two conditions hold for every context C of 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 a $E \in C$ 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. However, if the value assignment on a particular set 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 would be incompatible with the definite values of other observables sharing a context with E. If

* cristian@cs.auckland.ac.nz; http://www.cs.auckland.ac.nz/~cristian
† svozil@tuwien.ac.at; http://tph.tuwien.ac.at/~svozil

$v(E)=1$, a measurement of every observable in a context C containing E must yield the outcome 1 for E. Consequently, to avoid contradiction, the outcome 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).

III. VALUE INDEFINITE OBSERVABLES

We proceed with the main result:

Fix a context C in $\mathbb{C}^n, n>2$. If an observable $E\in C$ is value indefinite under a value assignment function v, then there exists a value indefinite observable $G\in C$ such that $v(G)=\sum_{E'\in C\setminus\{E\}} v(E')$.

For a proof, fix a context C and assume that E is value indefinite under v, meaning that both $v(E)=0$ as well as $v(E)=1$ are (in)consistent with respect to admissibility.

First, we show that

$$\sum_{E'\in C\setminus\{E\}} E' \tag{1}$$

is value indefinite.

The following two cases arise:

(i) Suppose that

$$\sum_{E'\in C\setminus\{E\}} v(E')=0. \tag{2}$$

Then, due to Completeness (b), E needs to be assigned the value one, that is, $v(E)=1$. But this contradicts the assumption that $v(E)$ is undefined. Therefore, the equality (2) is false.

(ii) Suppose that

$$\sum_{E'\in C\setminus\{E\}} v(E')=1. \tag{3}$$

Then, due to Exclusivity (a), E needs to be assigned the value zero, that is, $v(E)=0$. Again, this contradicts the assumption that $v(E)$ is undefined. Therefore, the equality (3) is false.

Second, we show the existence of a value indefinite observable $G\neq E$ such that $v(G)=\sum_{E'\in C\setminus\{E\}} v(E')$. Indeed, if every $G\neq E$ would be value definite, then the sum (1) would be value definite too, a contradiction.

Note that, because of context independence, that is, the independence of the value assignment function from the context, if $v(E)=1$, a measurement of observable E in any context C containing E must yield the outcome 1. Consequently, to avoid contradiction with the Exclusivity criterion (a), the outcome of measurements for all of the other observables in all of these contexts containing E must be 0; hence, the remaining observables in all of the contexts containing E are value definite, with value 0.

Likewise, in $n>2$ dimensions, having fewer than $n-1$ observables—say, one to $n-2$ observables—with value 0 could still lead to undefined value assignments on the remaining $n-1$ to 2 observables. Hence, these remaining $n-1$ to 2 observables remain value indefinite. However, if there are $n-1$ observables with value assignment 0, then, due to Completeness criterion (b), the remaining observable is assigned value 1.

Note also that, by "merging" two or more observables of the context, represented by the orthogonal projection operators $E_2,\ldots,E_n$, we never left 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 $|e_1\rangle,\ldots,|e_1\rangle$ for an orthonormal basis.

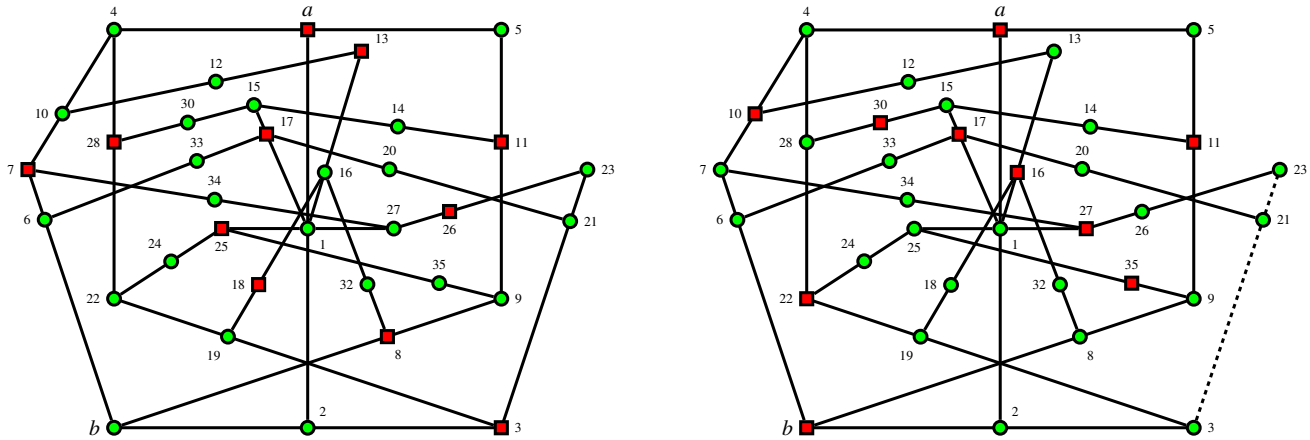
For the sake of an example, we shall delineate a hypergraph introduced in [5] and split it into segments serving as true-implies-false (TIFS) and true-implies-true (TITS) gadgets [10].

The hypergraph corresponding to the TIFS gadget in Figure 1 illustrates the orthogonality relations among vector labels of the elements of hyperedges [11], as detailed in [10, Table I]. By subsequently applying the admissibility rules [12, Fig. 24.2.a] a single consistent value assignment, as in Figure 1(a) 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 must be either 0 or undefined, that is, value indefinite.

Conversely, the TITS gadget hypergraph in Figure 2 illustrates the orthogonality relations among vector labels of the elements of hyperedges [11], as detailed in [10, Table I]. Using the admissibility rules [12, Fig. 24.2.a] a single consistent value assignment, as in Figure 2(a) implies $v(a)=1$ and $v(b)=1$, in contrast with the value assignment when assuming $v(a)=1$ and $v(b)=0$.

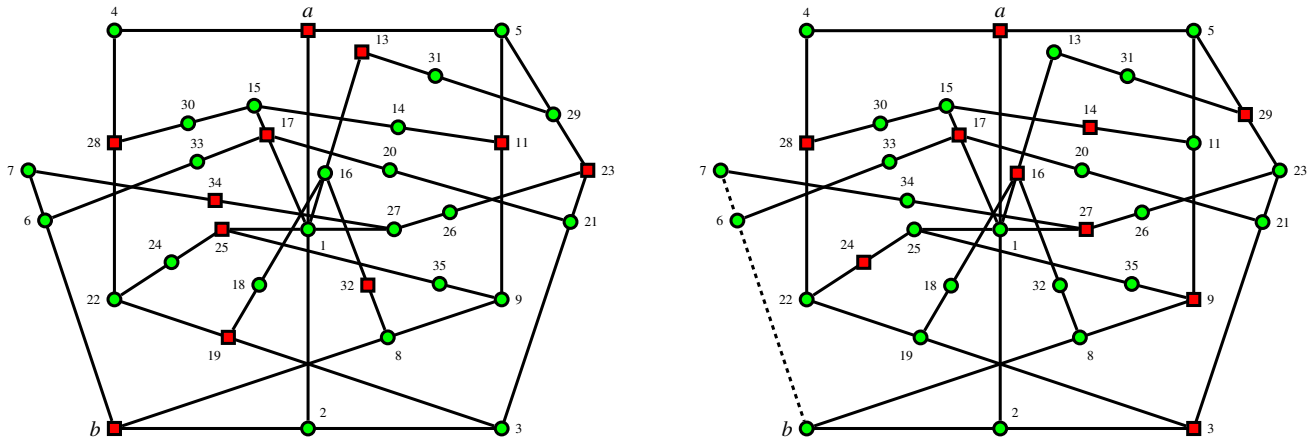
As before, for any such configuration of quantum observables, there exists no classical admissible value assignment v satisfying the constraint on the input and output ports $v(a)=1$ and $v(b)=0$, respectively. Consequently, if a has a preselected input state $v(a)=1$, then the value assignment $v(b)$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

Therefore, the concatenation of the two hypergraphs depicting TIFS and TITS gadgets, originally introduced by Abbott and the authors in [10], and shown in Figures 1 and 2 respectively, excludes both admissible value assignments of 0 and 1, rendering $v(b)$ undefined and thus the observable b value indefinite. Indeed, as in Figure 3 the penetration of admissible value assignments is rather limited: if the system is prepared



(a) (b)

FIG. 1. The TIFS gadget hypergraph for b given $v(a) = 1$, as well as the TITS gadget hypergraph for 3 given $v(a) = 1$, illustrates the orthogonality relations among vector labels of the elements of hyperedges [11] within a subset of quantum observables—also known as a faithful orthogonal representation [13] or coordinatization [14], as enumerated in [10, 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 $v(a) = 1$ and $v(b) = 0$ and applying the admissibility rules successively [12, Fig. 24.2.a]. (b) An inconsistent value assignment is obtained by assuming $v(a) = v(b) = 1$ 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 v with the constraint on the input and output ports $v(a) = v(b) = 1$ exists. Therefore, if a has a preselected input state $v(a) = 1$, then the value assignment $v(b)$ for the output state b has either to be 0 or needs to be undefined, that is, b is value indefinite.



(a) (b)

FIG. 2. The TITS gadget hypergraph for b given $v(a) = 1$, as well as the TIFS gadget hypergraph for 3 given $v(a) = 1$, which is partly reflection symmetric along the $\{a, 1, 2\}$ context to the TIFS gadget hypergraph in Figure 1, illustrates the orthogonality relations among vector labels of the elements of hyperedges [11] within a subset of quantum observables—also known as a faithful orthogonal representation [13] or coordinatization [14], as enumerated in [10, 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 $v(a) = 1$ and $v(b) = 1$ and applying the admissibility rules successively [12, Fig. 24.2.b]. (b) An inconsistent value assignment is obtained by assuming $v(a) = 1$ and $v(b) = 0$ 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 v exists with the constraint on the input and output ports $v(a) = 1$ and $v(b) = 0$. Therefore, if a has a preselected input state $v(a) = 1$, then the value assignment $v(b)$ For the output state, b has to be 1 or undefined; that is, b is an indefinite value.

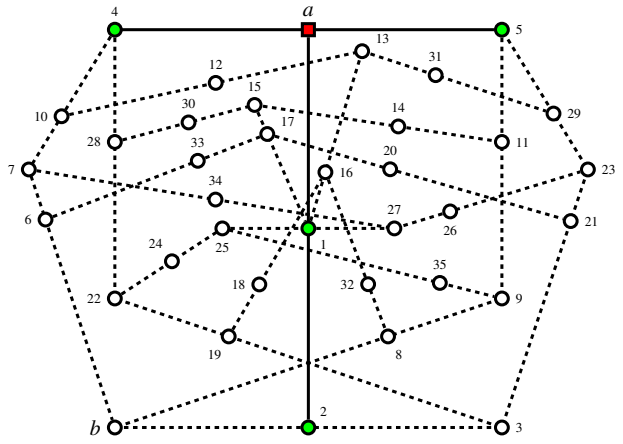


FIG. 3. Concatenated hypergraph from the hypergraphs depicting TIFS and TITS gadgets shown in Figures 1 and 2, respectively. Admissibility merely allows "star-shaped" value definite observables along the two contexts $\{a,1,2\}$ and $\{a,4,5\}$ if the system is prepared in state a.

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 all contexts $\{b,2,3\}$, $\{b,6,7\}$, and $\{b,8,9\}$, in which b is an element, have at least one more element which is value indefinite. This is because the set of observables $O=\{a,b,1,\ldots,35\}$ is not unital [15], 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 $v(a)=1$ [12, 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 Figures 1 and 2 as TITS and TIFS gadgets for 3 given $v(a)=1$, respectively. Therefore, $v(3)$ is undefined, and the obsevable 3 is value indefinite.

IV. A CONSTRUCTION OF A BINARY QUANTUM RANDOM NUMBER GENERATORS BASED ON VALUE INDEFINITE OBSERVABLES

A. Quantum versus classical models

A quantum realization of the construction in Figures 1, 2 and 3 can be obtained from the faithful orthogonal representation of the elements of the hyperedges as vectors. One such representation was already given in [10, 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 $|a\rangle$, 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, 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 is value-definite with a value of $v(2)=0$. 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 $E_{2,3}$:

$$\begin{aligned}E_{2,3}&=E_2+E_3=|2\rangle\langle 2|+|3\rangle\langle 3|\\ &=\frac{1}{2}\begin{pmatrix}1&-\frac{1}{\sqrt{2}}&-\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}&\frac{3}{2}&-\frac{1}{2}\\ -\frac{1}{\sqrt{2}}&-\frac{1}{2}&\frac{3}{2}\end{pmatrix}.\end{aligned}\tag{4}$$

This is a particular case of (1). 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 Figure 3 because some elements of O are assigned the value 0 for all two-valued states [12, Table 24.1], hence not separable [4, 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.

B. Beam splitter realizations

Figure 4 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 [10, Table I] $|a\rangle = (1,0,0)^T$, $|b\rangle = \left(\frac{1}{\sqrt{2}},\frac{1}{2},\frac{1}{2}\right)^T$, $|2\rangle = \left(0,\frac{1}{\sqrt{2}},-\frac{1}{\sqrt{2}}\right)^T$, $|3\rangle = \left(\frac{1}{\sqrt{2}},-\frac{1}{2},-\frac{1}{2}\right)$, $|4\rangle = (0,0,1)^T$, and $|5\rangle = (0,1,0)^T$ identifying the generic label x with a (ket) vector $|x\rangle$ was used to compute the respective unitary transformation matrix [16, 17] that transforms the input state a into the output state b, the input state 4 into the output state 2, and the input state 5 into the output state 3:

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

This unitary matrix realizes a beam splitter [18–21] using the parametrization of the unitary group [22]. 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.

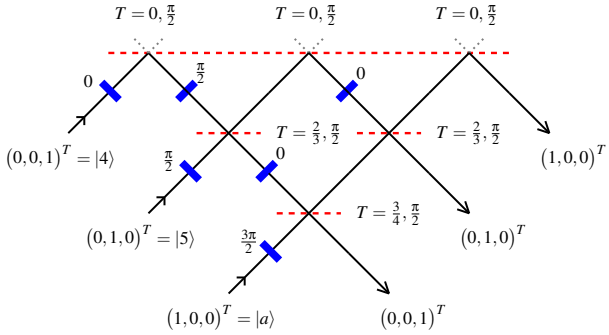


FIG. 4. A triangular array of quantum mechanical beam splitters is a realization of the input or preparation context $\{a,4,5\}$ and the output or measurement context $\{b,2,3\}$ in terms of the vector coordinatization [10, Table I] $a \equiv (1,0,0)^T$, $b \equiv \left(\frac{1}{\sqrt{2}},\frac{1}{2},\frac{1}{2}\right)^T$, $2 \equiv \left(0,\frac{1}{\sqrt{2}},-\frac{1}{\sqrt{2}}\right)^T$, $3 \equiv \left(\frac{1}{\sqrt{2}},-\frac{1}{2},-\frac{1}{2}\right)^T$, $4 \equiv (0,0,1)^T$, and $5 \equiv (0,1,0)^T$.

The output wave function, given the input wave function, is the coherent superposition (summation) of the contributions of all the possible forward passes from the input port(s) towards 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 [23]. 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 [24], whereby, for a symmetric lossless dielectric plate [25], the reflected and transmitted parts are $\pi/2$ out of phase [23, 26].

The relations (6) present a computation of the effects on the input ports of the beam splitter in Figure 4 by successive applications of phase shifts and beam mixings.

$$\begin{aligned} |a\rangle &\longrightarrow e^{i\frac{3\pi}{2}}\left\{e^{i\frac{\pi}{2}}\sqrt{\frac{1}{4}}\begin{pmatrix}0\\0\\1\end{pmatrix} + \sqrt{\frac{3}{4}}\left[e^{i\frac{\pi}{2}}\sqrt{\frac{1}{3}}\begin{pmatrix}0\\1\\0\end{pmatrix} + \sqrt{\frac{2}{3}}e^{i\frac{\pi}{2}}\begin{pmatrix}1\\0\\0\end{pmatrix}\right]\right\} = |b\rangle, \\ |5\rangle &\longrightarrow e^{i\frac{\pi}{2}}\left(e^{i\frac{\pi}{2}}\sqrt{\frac{1}{3}}\left\{\sqrt{\frac{3}{4}}\begin{pmatrix}0\\0\\1\end{pmatrix} + e^{i\frac{\pi}{2}}\sqrt{\frac{1}{4}}\left[e^{i\frac{\pi}{2}}\sqrt{\frac{1}{3}}\begin{pmatrix}0\\1\\0\end{pmatrix} + e^{i\frac{\pi}{2}}\sqrt{\frac{2}{3}}\begin{pmatrix}1\\0\\0\end{pmatrix}\right]\right\}\right. \\ &\qquad \left. + \sqrt{\frac{2}{3}}e^{i\frac{\pi}{2}}\left[\sqrt{\frac{2}{3}}\begin{pmatrix}0\\1\\0\end{pmatrix} + e^{i\frac{\pi}{2}}\sqrt{\frac{1}{3}}e^{i\frac{\pi}{2}}\begin{pmatrix}1\\0\\0\end{pmatrix}\right]\right) = |3\rangle, \\ |4\rangle &\longrightarrow e^{i\frac{\pi}{2}}e^{i\frac{\pi}{2}}\left(\sqrt{\frac{2}{3}}\left\{\sqrt{\frac{3}{4}}\begin{pmatrix}0\\0\\1\end{pmatrix} + e^{i\frac{\pi}{2}}\sqrt{\frac{1}{4}}\left[e^{i\frac{\pi}{2}}\sqrt{\frac{1}{3}}\begin{pmatrix}0\\1\\0\end{pmatrix} + \sqrt{\frac{2}{3}}e^{i\frac{\pi}{2}}\begin{pmatrix}1\\0\\0\end{pmatrix}\right]\right\}\right. \\ &\qquad \left. + e^{i\frac{\pi}{2}}\sqrt{\frac{1}{3}}e^{i\frac{\pi}{2}}\left[\sqrt{\frac{2}{3}}\begin{pmatrix}0\\1\\0\end{pmatrix} + e^{i\frac{\pi}{2}}\sqrt{\frac{1}{3}}e^{i\frac{\pi}{2}}\begin{pmatrix}1\\0\\0\end{pmatrix}\right]\right) = |2\rangle. \end{aligned} \tag{6}$$

V. CERTIFICATION

In this section, we prove that the quality of randomness produced by the quantum random number generators described by the value definite observables and the unitary matrices in Equations (5) and subsequently (13) are the same as the quality of the quantum random number generators in [2, 3]: Every sequence generated is maximally unpredictable: no algorithm can predict a single bit of the sequence.

Suppose we prepare a quantized system in a state $|a\rangle = (1,0,0)^T$ which is value definite with respect to any context containing the observable $|a\rangle\langle a| = \mathrm{diag}(1,0,0)$. This system is then 'analyzed' in terms of the spin-1 operator in the x-direction S_x, and its associated unit eigenvectors (through its spectral decomposition) form the unitary operator given by the unitary matrix [3]:

$$U_x = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & -\sqrt{2} & 1 \end{pmatrix}. \tag{7}$$

Then, as discussed earlier, U_x can be represented by a beam splitter.

Note that, as $|a\rangle$ is not in the context formed by the row vectors of U_x, it is not value definite with respect to S_1. By forming the scalar product between $|a\rangle$ and the row vectors of U_x, and by taking the (absolute) square, we obtain a ternary quantum random number generator producing ternary digits with the probability distribution $\left(\frac{1}{4},\frac{1}{2},\frac{1}{4}\right)$, see [3].

The computable alphabetic morphism $\varphi\colon \{0,1,2\} \to \{0,1\}$

$$\varphi(x) = \begin{cases} 0, & \text{if } x = 0, \\ 1, & \text{if } x = 1, \\ 0, & \text{if } x = 2, \end{cases} \tag{8}$$

transforms by sequential concatenation ternary strings and sequences into binary ones and preserves maximal unpredictability for the probability distribution $\frac{1}{4},\frac{1}{2},\frac{1}{4}$; see [27] and Section 7 in [2].

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 (8) results in the 'merging' or 'folding' 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 5. Thereby, the unitary matrix U'

$$U' = \frac{1}{2\sqrt{2}}\begin{pmatrix} 1+\sqrt{2} & \sqrt{2} & 1-\sqrt{2} \\ 1-\sqrt{2} & \sqrt{2} & 1+\sqrt{2} \\ \sqrt{2} & -2 & \sqrt{2} \end{pmatrix} \tag{9}$$

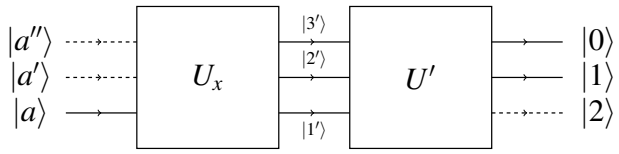


FIG. 5. A horizontal schema of two beam splitters U_x and U' in serial composition$U'U_x$, with the 'input' state prepared in $|a\rangle$, and two 'active output' ports in states $|0\rangle$ and $|1\rangle$.

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

$$U'U_x = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & \sqrt{2} \end{pmatrix}. \tag{10}$$

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 $|a\rangle$, this output state $U_x|a\rangle$ corresponds to a value-indefinite observable. Subsequently, it is 'merged' 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 [28, 29], two unitary matrices are unitary equivalent if their eigenvalues coincide. In our case, both U_x in (7) as well as $U'U_x$ in (9) have one eigenvalue -1, and a double eigenvalue 1. More explicitly, the matrix

$$V = \begin{pmatrix} \frac{1}{2\sqrt{3}}\sqrt{2-\sqrt{2+\sqrt{3}}} & \frac{1}{2\sqrt{3}}\sqrt{2+\sqrt{2+\sqrt{3}}} & \sqrt{\frac{2}{3}} \\ -\frac{1}{\sqrt{6}}\sqrt{2-\sqrt{2+\sqrt{3}}} & -\frac{1}{\sqrt{6}}\sqrt{2+\sqrt{2+\sqrt{3}}} & \frac{1}{\sqrt{3}} \\ \frac{1}{2}\sqrt{2+\sqrt{2+\sqrt{3}}} & -\frac{1}{2}\sqrt{2-\sqrt{2+\sqrt{3}}} & 0 \end{pmatrix} \tag{11}$$

satisfies the equality $V^T U_x V = U'U_x$: this proves that the matrix U_x defined in (7) is unitarily equivalent to the matrix combination $U'U_x$ in (10).

Using the invariance results in [3], we deduce that the quantum random number generator described in the section generates maximally unpredictable binary random digits.

VI. 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 input 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 [18–21]. 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 instance, the associated unitary three-dimensional matrix entries could be

$$U_{2\text{-to-}1} = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}, \; U_{1\text{-to-}2} = \begin{pmatrix} 0 & \cdot & \cdot \\ \frac{1}{\sqrt{2}} & \cdot & \cdot \\ \frac{1}{\sqrt{2}} & \cdot & \cdot \end{pmatrix}, \qquad (12)$$

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 Figure 4 by a beam splitter corresponding to the following real-valued unitary matrix:

$$U'_{2\text{-to-}1} = \frac{1}{\sqrt{2}} \begin{pmatrix} \sqrt{2} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{pmatrix}. \qquad (13)$$

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 Equations (10) and (13), 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 [30, 31], referred to as 'process 2' by Everett [32]—that needs to be one-to-one, appears to be compromised. (ii) Moreover, what happens in such a situation concerning 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 is the same number n of input and output ports. The quantum evolution is incomplete if some input and output contexts are not considered. 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 [16, 17]—the output context. Incomplete mappings of vectors from one context into some vectors of another context may not be one-to-one and thus represent a unitary transformation; only the totality of those vectors forms a forward- and backward-reversible transformation.

One can view the context-to-context unitary mapping as a sort of 'rescrambling' of information contained in the channels or ports of the beam splitter [33, 34]. Thereby, the 'latent' and 'omitted' ports act as Ariadne's thread that must be considered for reversibility. The situation is similar to a zero-sum game encountered in entanglement swapping.

VII. CONCLUSIONS

We have shown that if an observable $E \in C$ (in $\mathbb{C}^n, n > 2$) is value indefinite under a value assignment function v, then we can locate a value indefinite observable $G \in C$ such that $v(G) = \sum_{E' \in C \setminus \{E\}} v(E')$. This yields a quantum mechanical justification for the algebraic post-processing transforming ternary quantum random digits into binary ones [2, 3, 27].

It also sheds new light on a question [35] about the 'effective two-dimensionality' of a setup introduced earlier [1] in which one output has probability zero, that might potentially endanger the principle of three- and higher-dimensionality of quantum random number generators [36]. The difference between the quantum random number generator in the 2012 article [1], which generates binary output directly, and the more recent one [3] that generates manifestly tertiary output (which needs post-processing) is the input state. Whereas the former uses the input state $(0,1,0)^T$, the latter uses another (orthogonal) state $|a\rangle = (1,0,0)^T$. In both instances, the 'internal' beam splitter machinery operates in three-dimensional Hilbert space.

Furthermore, the outputs of the binary quantum random number generators based on value-indefinite observables have the same randomness qualities as the ternary ones; that is, they are maximally unpredictable [6]. Our results in $\mathbb{C}^3$ can easily be generalized to $\mathbb{C}^n$ with $n > 3$.

ACKNOWLEDGMENTS

We thank Michael Reck for the code producing the generalised 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), Project No. I 4579-N.

[1] A. A. Abbott, C. S. Calude, J. Conder, and K. Svozil, Physical Review A **86**, 062109 (2012), arXiv:1207.2029, URL https://doi.org/10.1103/PhysRevA.86.062109.

[2] J. M. Agüero Trejo and C. S. Calude, Theoretical Computer Science **862**, 3 (2021), ISSN 03043975, URL linkinghub.elsevier.com/retrieve/pii/S0304397520304679.

[3] J. M. Agüero Trejo and C. S. Calude, Proc. R. Soc. A **479**, 1 (2023), URL https://doi.org/10.1098/rspa.2022.0543.

[4] S. Kochen and E. P. Specker, Journal of Mathematics and Mechanics (now Indiana University Mathematics Journal) **17**, 59 (1967), ISSN 0022-2518, URL https://doi.org/10.1512/iumj.1968.17.17004.

[5] A. A. Abbott, C. S. Calude, and K. Svozil, Journal of Mathematical Physics **56**, 102201 (2015), arXiv:1503.01985, URL https://doi.org/10.1063/1.4931658.

[6] A. A. Abbott, C. S. Calude, and K. Svozil, in *Fields of Logic and Computation II*, edited by L. D. Beklemishev, A. Blass, N. Dershowitz, B. Finkbeiner, and W. Schulte (Springer, Cham, Heidelberg, New York, Dordrecht, London, 2015), vol. 9300 of *Lecture Notes in Computer Science*, pp. 69–86, ISBN 978-3-319-23533-2, arXiv:1403.2738, URL https://doi.org/10.1007/978-3-319-23534-9_4.

[7] S. C. Kleene, Mathematische Annalen **112**, 727 (1936), ISSN 1432-1807, URL https://doi.org/10.1007/BF01565439.

[8] A. Church, American Journal of Mathematics **58**, 345 (1936), URL https://doi.org/10.2307/2371045.

[9] A. M. Turing, Proceedings of the London Mathematical Society, Series 2 **42, 43**, 230 (1936-7 and 1937), URL https://doi.org/10.1112/plms/s2-42.1.230, https://doi.org/10.1112/plms/s2-43.6.544.

[10] A. Cabello, J. R. Portillo, A. Solís, and K. Svozil, Physical Review A **98**, 012106 (2018), arXiv:1805.00796, URL https://doi.org/10.1103/PhysRevA.98.012106.

[11] L. Lovász, IEEE Transactions on Information Theory **25**, 1 (1979), ISSN 0018-9448, URL https://doi.org/10.1109/TIT.1979.1055985.

[12] K. Svozil, in *Quantum, Probability, Logic: The Work and Influence of Itamar Pitowsky*, edited by M. Hemmo and O. Shenker (Springer International Publishing, Cham, 2020), vol. 1 of *Jerusalem Studies in Philosophy and History of Science (JSPS)*, pp. 521–544, ISBN 978-3-030-34316-3, arXiv:1812.08646, URL https://doi.org/10.1007/978-3-030-34316-3_24.

[13] A. Solís-Encina and J. R. Portillo, *Orthogonal representation of graphs* (2015), arXiv:1504.03662, URL https://doi.org/10.48550/arXiv.1504.03662.

[14] M. Pavičić and N. D. Megill, Entropy **20** (2018), ISSN 1099-4300, program code at https://puh.srce.hr/s/Qegixzz2BdjYwFL, accessed on June 12th, 2020, arXiv:1905.01567, URL https://doi.org/10.3390/e20120928.

[15] K. Svozil and J. Tkadlec, Journal of Mathematical Physics **37**, 5380 (1996), URL https://doi.org/10.1063/1.531710.

[16] J. Schwinger, Proceedings of the National Academy of Sciences (PNAS) **46**, 570 (1960), URL https://doi.org/10.1073/pnas.46.4.570.

[17] S. D. Joglekar, *Mathematical Physics: The Basics* (CRC Press, Boca Raton, Florida, 2007).

[18] M. Reck and A. Zeilinger, 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, 02–05 March 1993, URL https://doi.org/10.1142/2131.

[19] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Physical Review Letters **73**, 58 (1994), URL https://doi.org/10.1103/PhysRevLett.73.58.

[20] M. Reck (1994-1996), mathematica program.

[21] H. de Guise, O. Di Matteo, and L. L. Sánchez-Soto, Physical Review A **97** (2018), ISSN 2469-9934, arXiv:1708.00735, URL http://dx.doi.org/10.1103/PhysRevA.97.022328.

[22] F. D. Murnaghan, *The Unitary and Rotation Groups*, vol. 3 of *Lectures on Applied Mathematics* (Spartan Books, Washington, D.C., 1962).

[23] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Physics Today **46**, 22 (1993), URL https://doi.org/10.1063/1.881360.

[24] A. Zeilinger, American Journal of Physics **49**, 882 (1981), URL https://doi.org/10.1119/1.12387.

[25] H. M. Lai, A. F. Leung, and P. Y. Wong, American Journal of Physics **53**, 1103 (1985), ISSN 1943-2909, URL http://dx.doi.org/10.1119/1.14042.

[26] V. Degiorgio, American Journal of Physics **48**, 81 (1980), ISSN 1943-2909, URL http://dx.doi.org/10.1119/1.12238.

[27] C. S. Calude, K. F. Celine, Z. Gao, S. Jain, L. Staiger, and F. Stephan, Theoretical Computer Science **894**, 31 (2021), URL https://doi.org/10.1016/j.tcs.2021.09.005.

[28] R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, New York, NY, 1985, 2013), 2nd ed., ISBN 9780521839402,9780521548236,9781139785884, URL https://www.cambridge.org/9780521548236.

[29] D. Z. Dokovic and C. R. Johnson, Linear Algebra and its Applications **421**, 63 (2007), ISSN 0024-3795, URL http://dx.doi.org/10.1016/j.laa.2006.03.002.

[30] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Springer, Berlin, Heidelberg, 1932, 1996), 2nd ed., ISBN 978-3-642-61409-5,978-3-540-59207-5,978-3-642-64828-1, English translation in [31], URL https://doi.org/10.1007/978-3-642-61409-5.

[31] J. von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, NJ, 1955), ISBN 9780691028934, German original in [30], URL http://press.princeton.edu/titles/2113.html.

[32] H. Everett III, Reviews of Modern Physics **29**, 454 (1957), URL https://doi.org/10.1103/RevModPhys.29.454.

[33] E. Schrödinger, Naturwissenschaften **23**, 823 (1935), URL https://doi.org/10.1007/BF01491914.

[34] A. Zeilinger, Foundations of Physics **29**, 631 (1999), URL https://doi.org/10.1023/A:1018820410908.

[35] A. Fedorov, *Binary beam splitters may not be protected by value indefiniteness as tertiary ones* (2022), private communications.

[36] K. Svozil, Physical Review A **79**, 054306 (pages 3) (2009), arXiv:quant-ph/0903.2744, URL https://doi.org/10.1103/PhysRevA.79.054306.