Strong Kochen-Specker theorem and incomputability of quantum randomness

Alastair A. Abbott,[*] Cristian S. Calude,[†] and Jonathan Conder[‡]
Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand

Karl Svozil[§]
Institute for Theoretical Physics, Vienna University of Technology, Wiedner Hauptstrasse 8-10/136, 1040 Vienna, Austria
(Received 17 September 2012; published 17 December 2012)

The Kochen-Specker theorem shows the impossibility for a hidden variable theory to consistently assign values to certain (finite) sets of observables in a way that is noncontextual and consistent with quantum mechanics. If we require noncontextuality, the consequence is that many observables must not have pre-existing definite values. However, the Kochen-Specker theorem does not allow one to determine *which* observables must be value indefinite. In this paper we present an improvement on the Kochen-Specker theorem which allows one to actually locate observables which are *provably value indefinite*. Various technical and subtle aspects relating to this formal proof and its connection to quantum mechanics are discussed. This result is then utilized for the proposal and certification of a dichotomic quantum random number generator operating in a three-dimensional Hilbert space.

DOI: 10.1103/PhysRevA.86.062109 PACS number(s): 03.65.Ta, 03.67.Lx, 05.40.−a, 03.67.Ac

I. LOCATED QUANTUM VALUE INDEFINITENESS

While Bell's theorem [1] expresses the impossibly for a local hidden variable theory to give the same statistical results as quantum mechanics, the Kochen-Specker theorem [2,3] proves the impossibility for a hidden variable theory to even assign values to certain (finite) sets of observables in a way that is noncontextual and consistent with quantum mechanics. More precisely, it expresses a contradiction between the following presuppositions:

(P1) the set of observables in question [4] have pre-assigned definite values,

(P2) the outcomes of measurements of observables are noncontextual; that is, they are independent of whatever other comeasurable observables are measured alongside them, along with the requirement that the relationship between hidden variables associated with sets of comeasurable observables behave quasiclassically, as expected from quantum mechanics. This requirement means that, in any "complete" set of mutually comeasurable yes-no propositions (represented by mutually orthogonal projectors spanning the Hilbert space), exactly one proposition should be assigned the value "yes."

Thereby, the Kochen-Specker theorem does *not explicitly identify* certain particular observables which violate one or more of these presuppositions. Indeed, the Kochen-Specker theorem has not been designed to actually *locate* the particular observable(s) which would violate the assumptions. This is not seen as a deficiency of the theorem, because its content suffices for the many (mostly metaphysical) purposes it has been designed for and applied to.

In what follows we shall pursue a threefold agenda. First, we shall make explicit and formalize the physical notions involved; in particular, value (in)definiteness and contextuality. We shall thereby remain within the formalism of quantum logic, as outlined by Birkhoff and von Neumann [5,6], as well as by Kochen and Specker [7,8].

This enables us to specify exactly the actual *location of breakdown of classicality* within the set of Kochen-Specker observables; that is, we identify the observables for which classicality inadvertently renders complete contradictions, no matter what their (classical) outcome or value may be. In order to do this, we prove a modified version of the original Kochen-Specker theorem in which we obtain a contradiction between the presupposition (P2) and a crucially weaker version of (P1).

Second, we will clarify in what sense the Kochen-Specker and Bell-type theorems imply the violation of the noncontextuality assumption (P2). Formalization has become necessary because in the literature the term "contextuality" is often identified with violations of certain Bell-type inequalities on single quanta [9–12] in the absence of strict locality conditions [13].

We point out that, while from a purely logical point of view violation of the noncontextuality assumption (P2) is *sufficient* to interpret the Kochen-Specker theorem, it is by no means *necessary* for or implied by the Kochen-Specker theorem. Indeed, violation of the primary assumption of value definiteness (P1) presents a viable (albeit also not necessary, as other, more exotic, possibilities demonstrate; e.g., Ref. [14]) option to interpret the Kochen-Specker theorem.

Third, we shall also consider which collections of observables do not render Kochen-Specker contradictions. Restricting ourselves to these very limited collections would allow maintenance of assumptions (P1) and (P2) about quantized systems, but would also reduce the domain of conceivable observables dramatically.

The results presented can be interpreted as one natural consequence of, and advancement beyond, the Kochen-Specker theorem. They may be particularly important if we investigate the concrete "underpinning" of the Kochen-Specker theorem: exactly why and where a quantized system disobeys classicality.

Apart from foundational issues, there is also a concrete application which profits from such quantum information theoretic findings. Contemporary quantum random number

[*]a.abbott@auckland.ac.nz; http://www.cs.auckland.ac.nz/∼aabb009
[†]cristian@cs.auckland.ac.nz; http://www.cs.auckland.ac.nz/∼cristian
[‡]jonathan.conder@auckland.ac.nz
[§]svozil@tuwien.ac.at; http://tph.tuwien.ac.at/∼svozil

generators can no longer be based upon and certified by our conviction in the quantum postulate of *complementarity* alone. They should also be certified by strictly stronger forms of nonclassicality than complementarity, *quantum value indefiniteness* being one of them [15]. For these purposes, the Kochen-Specker theorem, as well as other Bell-type theorems, serve merely as *indications* that quantum value indefiniteness possibly "happens somewhere" because it cannot be excluded that particular individual quanta [15] could still be value definite.

Unfortunately, by their very design, these theorems cannot guarantee that a particular observable actually *is* value indefinite. One could, for instance, not exclude that a "demon" could act in such a way that all observables actually measured would be value definite, whereas other observables which are not measured would be value indefinite.

However, for quantum random number generators we need certification of value indefiniteness on the *particular observables utilized for that purpose*. Thus, one needs a different (in the sense of locatedness of violation of nonclassicality) stronger type of theorem than Kochen and Specker present; an argument that could (formally) *assure* that, if quantum mechanics is correct, the particular quantum observables used for the generation of random number sequences are *provably value indefinite,* hence the measured quantum sequences cannot refer to any consistent property of the measured quanta alone.

This article presents such an argument, which will be utilized for a dichotomic quantum random number generator operating in a three-dimensional Hilbert space. By now it should be clear that such a device would be strictly preferential to previous proposals using merely quantum complementarity or, in addition to that, some type of nonlocated violations of global value definiteness.

In what follows we shall first present the basic definitions, then state and prove the aforementioned result, and subsequently apply this result to the proposal of a quantum random number generator based on *located quantum value indefiniteness* which produces, as we prove, a strongly incomputable sequence of bits.

II. DEFINITIONS

A. Notation and formal framework

As usual we denote the set of complex numbers by $\mathbb{C}$ and use the standard quantum mechanical bra-ket notation; that is, we denote vectors in the Hilbert space $\mathbb{C}^n$ by $|\cdot\rangle$. We will have particular interest in the projection operators projecting onto the linear subspace spanned by a nonzero vector $|\psi\rangle$; namely $P_\psi = \frac{|\psi\rangle\langle\psi|}{\langle\psi|\psi\rangle}$; we will use this notation for projection operators throughout this paper. We briefly note that in this paper we only consider pure quantum states and will accordingly not explicitly specify quantum states as pure states as opposed to mixed states.

In order to discuss hidden variable theories precisely and without any of the ambiguity that is common in such discussion, we present an explicit formal framework in which we will work.

We fix a positive integer n. Let $\mathcal{O} \subseteq \{P_\psi \mid |\psi\rangle \in \mathbb{C}^n\}$ be a nonempty set of projection observables in the Hilbert space $\mathbb{C}^n$ and $\mathcal{C} \subseteq \{\{P_1, P_2, \ldots, P_n\} \mid P_i \in \mathcal{O} \text{ and } \langle i|j\rangle = 0 \text{ for } i \neq j\}$ a set of measurement contexts over $\mathcal{O}$. A context $C \in \mathcal{C}$ is thus a maximal set of compatible (i.e., they can be simultaneous measured) projection observables. Let $v : \{(o,C) \mid o \in \mathcal{O}, C \in \mathcal{C}, \text{ and } o \in C\} \stackrel{o}{\to} \{0,1\}$ be a partial function (i.e., it may be undefined for some values in its domain). For some $o,o' \in \mathcal{O}$ and $C,C' \in \mathcal{C}$ we say $v(o,C) = v(o',C')$ if $v(o,C)$, $v(o',C')$ are both defined and have equal values. If either $v(o,C)$ or $v(o',C')$ are not defined or they are both defined but have different values, then $v(o,C) \neq v(o',C')$. We will call v an *assignment function*, and it expresses the notion of a hidden variable: it specifies in advance the result obtained from the measurement of an observable.

An observable $o \in C$ is *value definite* in the context C under v if $v(o,C)$ is defined. Otherwise o is *value indefinite* in C. If o is value definite in all contexts $C \in \mathcal{C}$ for which $o \in C$ then we simply say that o is value definite under v. Similarly, if o is value indefinite in all such contexts C then we say that o is value indefinite under v. The set $\mathcal{O}$ is *value definite* under v if every observable $o \in \mathcal{O}$ is value definite under v. This notion of value definiteness corresponds to the classical notion of determinism: an observable is value definite if v assigns it a definite value; that is, we are able to predict in advance the value obtained via measurement.

An observable $o \in \mathcal{O}$ is *noncontextual* under v if for all contexts $C,C' \in \mathcal{C}$ with $o \in C,C'$ we have $v(o,C) = v(o,C')$. Otherwise, v is *contextual*. Note that an observable which is value indefinite in a context is always contextual even if it takes the same value in every context in which it is value definite. On the other hand, if an observable is value definite in all contexts that it is in, it can be either contextual or not (and in the latter case its value is constant in all contexts containing it), depending on v. The set of observables $\mathcal{O}$ is *noncontextual* under v if every observable $o \in \mathcal{O}$ which is not value indefinite (i.e., value definite in *some* context) is noncontextual under v. Otherwise, the set of observables $\mathcal{O}$ is *contextual*. Furthermore, we say that the set of observables $\mathcal{O}$ is *strongly contextual* under v if every observable $o \in \mathcal{O}$ is contextual under v. Noncontextuality corresponds to the classical notion that the value obtained via measurement is independent of other compatible observables measured alongside it.

Every strongly contextual set of observables under v is contextual under v, provided that v is not undefined everywhere. However the converse implication is false, as we will discuss in Sec. II C.

If an observable o is noncontextual then it is value definite, but this is not true for sets of observables: $\mathcal{O}$ can be noncontextual but not value definite if it contains an observable which is value indefinite.

An assignment function v is *admissible* if the following hold for all $C \in \mathcal{C}$:

(i) if there exists an $o \in C$ with $v(o,C) = 1$, then $v(o',C) = 0$ for all $o' \in C \setminus \{o\}$,

(ii) if there exists an $o \in C$ such that $v(o',C) = 0$ for all $o' \in C \setminus \{o\}$, then $v(o,C) = 1$.

In the discussion of hidden variables, we do not concern ourselves with the mechanism of v, but rather with its possible existence subject to certain constraints (specifically, the admissibility of v—we justify this more fully in Sec. III—requires that functions of the values associated with compatible observables satisfy the predictions of quantum theory). The notion of admissibility serves as an analog to the notion of a

two-valued (dispersionless) measure that is used in quantum logic [16–21], the difference being that the definition is sound even when not all observables are value definite. This distinction is subtle but, nevertheless, will allow us to formulate known results such as the Kochen-Specker theorem [3] as well as the stronger results which we present in this paper. However, we stress that this is still a purely formal framework and that, in order to make a connection to physical reality, further assumptions must be made, specifically pertaining to the nature of measurement; we defer this connection to physical reality to Sec. III.

We briefly note that this formal framework could be presented in an even more more abstract setting without reference to Hilbert spaces, but for the sake of concreteness we avoid this here.

B. Kochen-Specker theorem

Using the framework developed, the Kochen-Specker theorem [3], which we outlined and discussed in the introduction, can be presented in the following more rigorous form: if $n > 2$ there exists a set of projection observables $\mathcal{O}$ on $\mathbb{C}^n$ and a set of contexts over $\mathcal{O}$ such that there is no admissible assignment function v under which $\mathcal{O}$ is both noncontextual and value definite. This proves that it is impossible for all projection observables to be value definite and noncontextual.

C. Strong contextuality cannot be guaranteed

How strong is the incompatibility between noncontextuality and value definiteness stated in the Kochen-Specker theorem? The theorem tells us that not every observable can be both noncontextual and value definite, but gives us no information regarding how far this incompatibility goes. Here we show that this incompatibility cannot be maximal: no set of observables is strongly contextual under every admissible value definite assignment function on it. In other words, for any set of contexts over any set of observables, there exists an admissible assignment function under which the set of observables is value definite and at least one observable is noncontextual.

More precisely, let $\mathcal{O}$ be a set of projection observables and $\mathcal{C}$ a set of contexts over $\mathcal{O}$. Then for every $a \in \mathcal{O}$ there exists an admissible assignment function v such that $v(a,C) = 1$ for every context $C \in \mathcal{C}$ with $o \in C$, and $\mathcal{O}$ is value definite under v. To see this, consider the set $S_a = \{C \mid C \in \mathcal{C} \text{ and } a \in C\} \subseteq \mathcal{C}$ of contexts in which a appears. If we define the assignment function v_a for $C \in S_a$ by

$$v_a(o,C) = \begin{cases} 1 & \text{for} \quad o = a \\ 0 & \text{for} \quad o \neq a. \end{cases}$$

It is clear this satisfies $\sum_{o \in C} v_a(o,C) = 1$, for all $C \in S_a$. For $C \in \mathcal{C} \setminus S_a$, the function v_a can be defined in any arbitrary contextual way to satisfy admissibility. The function v_a is then admissible and assigns a definite value (namely 1) to the observable a (which was arbitrarily chosen) in a noncontextual way [i.e., $v_a(a,C) = 1$ for all $C \in S_a$].

Note that the configuration of contexts $S_a = \{C \mid C \in \mathcal{C} \text{ and } a \in C\} \subseteq \mathcal{C}$ amounts to a "star-shaped" Greechie orthogonality diagram, with the common observable a at the center of the star, as depicted in Fig. 1.

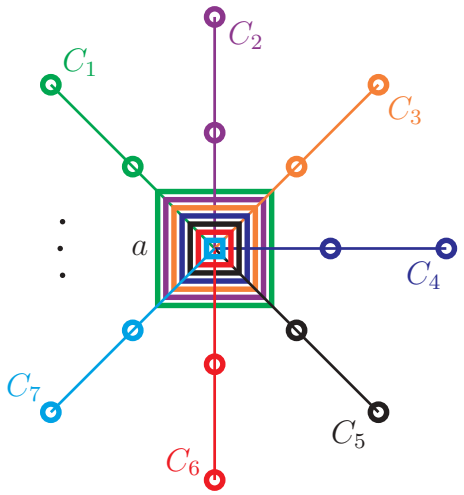

FIG. 1. (Color online) Greechie orthogonality diagram[a] of the contexts in S_a with an overlaid value assignment reflecting the argument against strong contextuality being guaranteed. Different contexts C_i are drawn in different colours, circles represent the value 0 and squares represent the value 1.

[a]Observables are represented by circles and squares, contexts by smooth line segments.

Indeed this should not be surprising in view of the predictions of quantum mechanics. Specifically, for a physical system prepared in the state $|\psi\rangle$, the Born rule predicts that measurement of the projection observable P_ψ should give the value 1 (noncontextually) with probability 1. Nevertheless, it is important to place a bound on the degree of nonclassicality [22,23] that we can guarantee. In fact, it is possible to go further than we have and define v_a to noncontextually assign the value 0 to each observable appearing on a "ray" of the star in Fig. 1. This is a consequence of the fact no two observables on differing "rays" are compatible.

However, in the following we show that one cannot go much further than this. Specifically, in what are the main theoretical results of the paper, we show that there are pairs of observables (belonging to different contexts) such that at most one of them can be assigned the value 1 by an admissible assignment function under which $\mathcal{O}$ is noncontextual. This finding is somewhat stronger than a similar result by Kochen and Specker [3,20] derived from the (as Specker used to call them [24]) "bug"-type orthogonality diagrams (a subdiagram of their diagram Γ_1), as not all observables are assumed to be value definite. Instead, an observable is only deduced to be value definite where the admissibility of v requires it to be so.

This difference allows us to deduce an even stronger result, with particular relevance to quantum random number generators: there are pairs of observables such that, if one of them is assigned the value 1 by an admissible assignment function under which $\mathcal{O}$ is noncontextual, the other must be *value indefinite*. This is the best guarantee of located value indefiniteness one could hope for, and we will make use of it in our proposal for a quantum random number generator. The proof relies on the weaker result described above, so we demonstrate that first and deduce the main result as a corollary. Note that there are larger values than $\frac{3}{\sqrt{14}}$ for which these results are true. However, this number is more than

TABLE I. Assignment table containing the representation of observable propositions (projectors), together with the contexts in which they appear. See Fig. 2 for an illustration of these.

v	1, 2	3, 4	5, 6	7, 8	9, 10	11, 12	13	14, 15	16, 17	18, 19	20, 21	22, 23	24
1	1 0 0	1 0 0	**2 1 1**	2 1 1	**2 0 1**	2 0 1		1 1 0	**1 1 1**	1 1 1	**1 0 1**	1 0 1	
0	**0 1 0**	**0 1 1**	1 $\widetilde{1}$ $\widetilde{1}$	**1 0 $\widetilde{2}$**	1 0 $\widetilde{2}$	**1 1 $\widetilde{2}$**		**1 $\widetilde{1}$ 0**	1 $\widetilde{1}$ 0	**1 0 $\widetilde{1}$**	1 0 $\widetilde{1}$	**1 1 $\widetilde{1}$**	
0	**0 0 1**	**0 1 $\widetilde{1}$**	0 1 $\widetilde{1}$	2 $\widetilde{5}$ 1	0 1 0	1 $\widetilde{5}$ $\widetilde{2}$		0 0 1	1 1 $\widetilde{2}$	1 $\widetilde{2}$ 1	0 1 0	1 $\widetilde{2}$ $\widetilde{1}$	1 1 $\widetilde{1}$
													1 $\widetilde{1}$ 0
1	3 2 1	3 2 1	**3 2 0**	3 2 0	**3 1 $\widetilde{1}$**	3 1 $\widetilde{1}$	**1 1 0**	1 1 0	**2 1 $\widetilde{1}$**	2 1 $\widetilde{1}$	**2 0 $\widetilde{1}$**	2 0 $\widetilde{1}$	1 1 2
0	**2 $\widetilde{3}$ 0**	**1 $\widetilde{1}$ $\widetilde{1}$**	2 $\widetilde{3}$ 0	**2 $\widetilde{3}$ 3**	2 $\widetilde{3}$ 3	**1 $\widetilde{1}$ 2**	1 $\widetilde{1}$ 2	**1 $\widetilde{1}$ 1**	1 $\widetilde{1}$ 1	**1 0 2**	1 0 2	**1 1 2**	
0	3 2 $\widetilde{13}$	1 $\widetilde{4}$ 5	0 0 1	6 $\widetilde{9}$ $\widetilde{13}$	0 1 1	1 $\widetilde{7}$ $\widetilde{4}$	1 $\widetilde{1}$ $\widetilde{1}$	1 $\widetilde{1}$ $\widetilde{2}$	0 1 1	2 $\widetilde{5}$ $\widetilde{1}$	0 1 0	1 $\widetilde{5}$ 2	

sufficient for our purposes, and the larger values we found require significantly longer proofs.

Theorem 1. Let $|a\rangle, |b\rangle \in \mathbb{C}^3$ be unit vectors such that $0 < |\langle a|b\rangle| \leqslant \frac{3}{\sqrt{14}}$. Then there exists a set of projection observables $\mathcal{O}$ containing P_a and P_b, and a set of contexts $\mathcal{C}$ over $\mathcal{O}$, such that there is no admissible assignment function under which $\mathcal{O}$ is noncontextual and P_a, P_b have the value 1.

Proof. We first show that the theorem holds under the equality $|\langle a|b\rangle| = \frac{3}{\sqrt{14}}$, and then, by means of a reduction to the case of equality, show it also holds for $0 < |\langle a|b\rangle| < \frac{3}{\sqrt{14}}$.

By choosing the basis appropriately, without loss of generality we may assume that $|a\rangle \equiv (1,0,0)$ and $|b\rangle \equiv \frac{1}{\sqrt{14}}(3,2,1)$. Let $|\psi\rangle = (0,1,0)$ and $|\phi\rangle = (0,0,1)$.

In Table I we define 24 contexts $C_1, C_2, \ldots, C_{24}$, which are numbered by the column headings. Each row vector $|\varphi\rangle$ in the table is defined relative to the afore-chosen basis $\{|a\rangle, |\psi\rangle, |\phi\rangle\}$ and is understood to represent the corresponding projection observable P_φ. For brevity, we have omitted commas, brackets, and normalization constants from these vectors, and have used the notation $\widetilde{n} = -n$.

As an example, $C_1 = \{P_a, P_\psi, P_\phi\}$.

Now let $\mathcal{C} = \{C_1, C_2, \ldots, C_{24}\}$ and $\mathcal{O} = \bigcup_{i=1}^{24} C_i$. Suppose there exists an admissible assignment function v under which $\mathcal{O}$ is noncontextual and $v(P_a, C_1) = v(P_b, C_2) = 1$. By continual application of the admissibility requirements, one can show that v assigns certain values to all the observables in Table I. This argument proceeds through the table from left to right, where the value assigned to each observable is noted in the leftmost column. For example, in the first step we conclude that $v(P_\psi, C_1) = v(P_\phi, C_1) = 0$. An observable whose value is determined by the others in the column is marked in bold, provided that the value given will be used later on. This argument is also illustrated in Fig. 2. We eventually obtain a contradiction, namely that $v(o, C_{24}) = 0$ for all $o \in C_{24}$ (the dotted line in Fig. 2). Therefore there does not exist such an admissible assignment function v.

We now show that if $0 < |\langle a|b\rangle| < \frac{3}{\sqrt{14}}$ and P_a and P_b both have the value 1, then there is a third observable P_c which must also have the value 1 and satisfies $|\langle a|c\rangle| = \frac{3}{\sqrt{14}}$. The above proof then applies to again show no admissible v exists satisfying the requirements.

By scaling $|b\rangle$ by a phase factor if necessary, we may assume that $\langle a|b\rangle \in \mathbb{R}$. Let $p = \langle a|b\rangle$ and $q = (1 - p^2)^{1/2}$. Then $(|b\rangle - |a\rangle p)\frac{1}{q}$ is a unit vector orthogonal to $|a\rangle$. Taking a cross product, the set $\{|a\rangle, (|b\rangle - |a\rangle p)\frac{1}{q}, |a\rangle \times (|b\rangle - |a\rangle p)\frac{1}{q}\}$ forms an orthonormal basis for $\mathbb{C}^3$. Relative to this basis, $|a\rangle \equiv (1,0,0)$ and $|b\rangle \equiv (p,q,0)$. Set $x = \frac{3}{\sqrt{14}}$, so that $p^2 < x^2$. Then

$$\frac{p^2(1-x^2)}{q^2x^2} = \frac{p^2 - p^2x^2}{q^2x^2} < \frac{x^2 - p^2x^2}{q^2x^2} = \frac{(1-p^2)x^2}{q^2x^2} = 1.$$

Now set $y = \frac{p(1-x^2)}{qx}$, so that

$$y^2 = \frac{p^2(1-x^2)}{q^2x^2}(1-x^2) < 1 - x^2.$$

Then we can set $z = (1 - x^2 - y^2)^{1/2} \in \mathbb{R}$. This choice of z makes $|c\rangle \equiv (x,y,z)$ a unit vector in $\mathbb{R}^3$. Taking cross products, we define

$$|\alpha\rangle = |a\rangle \times |c\rangle \equiv (1,0,0) \times (x,y,z) = (0, -z, y),$$

$$|\beta\rangle = |b\rangle \times |c\rangle \equiv (p,q,0) \times (x,y,z) = (qz, -pz, py - qx),$$

so that $\langle\alpha|\beta\rangle = (0, -z, y) \cdot (qz, -pz, py - qx) = pz^2 + py^2 - qxy = p(z^2 + y^2) - p(1 - x^2) = 0$. Therefore $\{|\alpha\rangle, |\beta\rangle, |c\rangle\}$ is an orthogonal basis for $\mathbb{C}^3$. This implies that the projection observables P_α, P_β, and P_c associated with the subspaces of $\mathbb{C}^3$ spanned by $|\alpha\rangle$, $|\beta\rangle$, and $|c\rangle$ are mutually compatible; that is, $C_{25} = \{P_\alpha, P_\beta, P_c\}$ is a context. Moreover, P_α is compatible with P_a because $\langle\alpha|a\rangle = 0$. Likewise, P_β is compatible with P_b. Hence there exist contexts C_{26} and C_{27} such that $P_\alpha, P_a \in C_{27}$ and $P_\beta, P_b \in C_{27}$.

Define unit vectors $|\psi\rangle \equiv (0, 2y - z, y + 2z)\frac{\sqrt{14}}{5}$ and $|\phi\rangle \equiv (0, y + 2z, z - 2y)\frac{\sqrt{14}}{5}$. Then it is easily checked that $\{|a\rangle, |\psi\rangle, |\phi\rangle\}$ is an orthonormal basis for $\mathbb{C}^3$. Note that

$$\begin{aligned}(|a\rangle 3 + |\psi\rangle 2 + |\phi\rangle)\tfrac{1}{\sqrt{14}} &\equiv \left(\tfrac{3}{\sqrt{14}}, (4y - 2z + y + 2z)\tfrac{1}{5}, (2y + 4z + z - 2y)\tfrac{1}{5}\right) \\ &= (x, y, z) \equiv |c\rangle,\end{aligned}$$

so $|c\rangle \equiv (3, 2, 1)\frac{1}{\sqrt{14}}$ relative to the basis $\{|a\rangle, |\psi\rangle, |\phi\rangle\}$.

Now let $\mathcal{C} = \{C_1, C_2, \ldots, C_{27}\}$ and $\mathcal{O} = \bigcup_{i=1}^{27} C_i$. Suppose there exists an admissible assignment function v under which $\mathcal{O}$ is noncontextual and $v(P_a, C_{26}) = v(P_b, C_{27}) = 1$. Since v is admissible, it follows that $v(P_\alpha, C_{26}) = v(P_\beta, C_{27}) = 0$. Therefore $v(P_\alpha, C_{25}) = v(P_\beta, C_{25}) = 0$, so by admissibility $v(P_c, C_{25}) = 1$. This deduction is illustrated in Fig. 3. However, by interpreting the observables in Table I as being defined relative to the basis $\{|a\rangle, |\psi\rangle, |\phi\rangle\}$, it is immediately clear that again no such admissible function v exists. ■

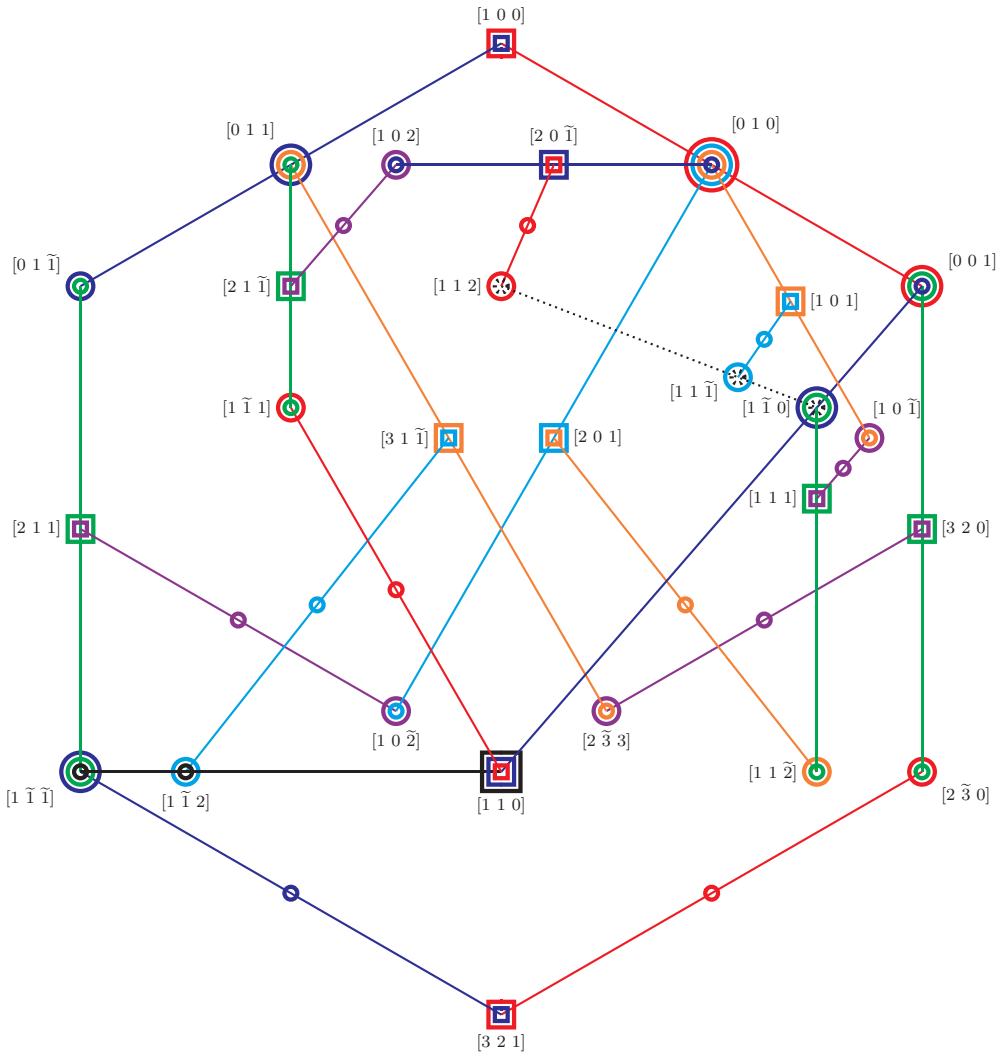

FIG. 2. (Color online) Greechie orthogonality diagram with an overlaid value assignment that can be used to visualize Table I. The circles and squares represent observables that will be given the values 0 and 1, respectively. They are joined by smooth lines which correspond to contexts (i.e., complete sets of compatible observables).

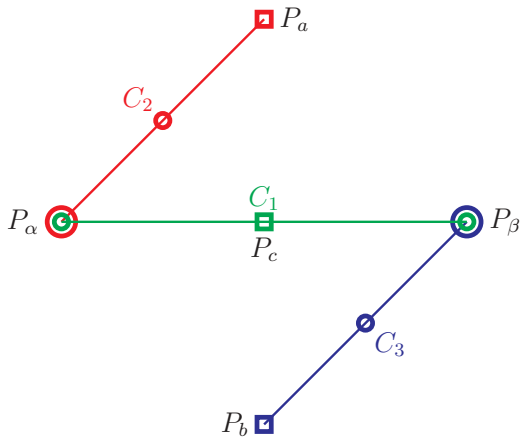

FIG. 3. (Color online) Greechie orthogonality diagram with an overlaid value assignment that illustrates the relationship between the contexts C_1, C_2, and C_3 in Theorem 1. The circles and squares represent observables that will be given the values 0 and 1, respectively. They are joined by smooth lines which represent contexts.

Corollary 2. Let $|a\rangle, |b\rangle \in \mathbb{C}^3$ be unit vectors such that $\sqrt{5/14} \leqslant |\langle a|b\rangle| \leqslant \frac{3}{\sqrt{14}}$. Then there exists a set of projection observables $\mathcal{O}$ containing P_a and P_b and a set of contexts $\mathcal{C}$ over $\mathcal{O}$, such that there is no admissible assignment function under which $\mathcal{O}$ is noncontextual, P_a has the value 1 and P_b is value definite.

Proof. Again scale $|b\rangle$ so that $\langle a|b\rangle \in \mathbb{R}$. Let $p = \langle a|b\rangle$ and $q = (1 - p^2)^{1/2}$. As above we construct an orthonormal basis in which $|a\rangle \equiv (1, 0, 0)$ and $|b\rangle \equiv (p, q, 0)$. Define $|\alpha\rangle \equiv (0, 1, 0)$, $|\beta\rangle \equiv (0, 0, 1)$, and $|c\rangle \equiv (q, -p, 0)$. Then $\{|a\rangle, |\alpha\rangle, |\beta\rangle\}$ and $\{|b\rangle, |c\rangle, |\beta\rangle\}$ are orthonormal bases for $\mathbb{C}^3$, so we can define the contexts $C_1 = \{P_a, P_\alpha, P_\beta\}$ and $C_2 = \{P_b, P_c, P_\beta\}$. Note that $p^2 \geqslant \frac{5}{14}$ and hence

$$\langle a|c\rangle = q = \sqrt{1 - p^2} \leqslant \sqrt{1 - \tfrac{5}{14}} = \tfrac{3}{\sqrt{14}}.$$

From Theorem 1 it follows that there are sets of observables $\mathcal{O}_b$, $\mathcal{O}_c$ and contexts $\mathcal{C}_b$, $\mathcal{C}_c$ such that there is no admissible assignment function under which $\mathcal{O}_b$ ($\mathcal{O}_c$) is noncontextual and P_a, P_b (P_a, P_c) have the value 1. We combine these sets

to give $\mathcal{O} = \mathcal{O}_b \cup \mathcal{O}_c \cup \{P_\alpha, P_\beta\}$ and $\mathcal{C} = \mathcal{C}_b \cup \mathcal{C}_c \cup \{C_1, C_2\}$. Suppose there exists an admissible assignment function v under which $\mathcal{O}$ is noncontextual, $v(P_a, C_1) = 1$ and P_b is value definite. Then $v(P_b, C_2) \neq 1$ by the definition of $\mathcal{O}_b$, so $v(P_b, C_2) = 0$. Since $v(P_a, C_1) = 1$ and v is admissible, $v(P_\beta, C_1) = 0$ and hence $v(P_\beta, C_2) = 0$ as well. So by admissibility $v(P_c, C_2) = 1$, which is impossible by the definition of $\mathcal{O}_c$. Therefore there does not exist such a function v. ■

The difference between the above result and the Kochen-Specker theorem is subtle but critical. The Kochen-Specker theorem, under the assumption of noncontextuality, only finds a contradiction with the hypothesis that *all* observables are value definite—it does not allow any specific observable to be proven value indefinite. Corollary 2, however, allows just this—*specific value indefinite observables can be identified*. While we delay the physical interpretation of this result until the following section, we mention that it applies to measurements of an observable on a physical system in an eigenstate of a different observable.

III. PHYSICAL INTERPRETATION

In order to make operational use of the results of the previous section we connect the formal entities with measurement outcomes. In the process of doing this, we make explicit the assumptions that our results rely on.

A. The role of measurement

An inherent assumption in the attempt to attribute physical meaning to the Kochen-Specker theorem (as well as the other theorems we have proved), and one which we shall also make, is that measurement is actually a physically meaningful process. In particular, we assume:

Measurement assumption. Measurement yields a physically meaningful and unique result.

This may seem rather self-evident, but it is not true of interpretations of quantum mechanics such as the many-worlds interpretation, where measurement is just a process by which the apparatus or experimenter becomes entangled with the state being "measured." In such an interpretation it does not make sense to talk about the unique "result" of a measurement, let alone any definite values which one may pre-associate with them.

To establish the relationship between the quantum system of interest and the function v assigning definite values in advance, we need to restrict ourselves to assignment functions which agree with quantum mechanics. Specifically, definite values prescribed by the function should be just that; they must guarantee the result of a measurement.

Let v be a value assignment function. We say that v is a *faithful* representation of a realization r_ψ of a state $|\psi\rangle$ if a measurement of observable o in the context C on the physical state r_ψ yields the result $v(o, C)$ whenever o has a definite value under v.

Usually, it is implicitly assumed that a value assignment function is faithful—if it is not then it has no real relation to the physical system that it is meant to model and is of little interest. Nonetheless, since we intend to make all assumptions explicit here, we will make clear that we are referring to faithful assignment functions when necessary. Of course, an assignment function which is defined nowhere meets this condition, but this complete indefiniteness does not fully capture our knowledge of a quantum system; we should at least be able to predict the outcomes of *some* measurements. We discuss this issue of when to assign definite values in Sec. III C.

B. Value indefiniteness

The Kochen-Specker theorem leaves two possibilities: either we give up the idea that every observable should be simultaneously value definite, or we allow observables to be defined contextually. Of course, some combination of both options is also possible. Here we opt to assume noncontextuality of observables for which the outcome is predetermined and thus give up the historic notion of complete determinism (classical omniscience).

This assumption might be in contradiction to that of physicists who, in the tradition of the realist Bell (see the oft-quoted text [1]), tend to opt for contextuality. The option for contextuality saves realistic omniscience and "contextual value definiteness" at the price of introducing a more general dependence of at least some potential observables on the measurement context. In what follows we make no attempt to save realistic omniscience and instead require the noncontextuality of any predetermined properties.

Noncontextuality assumption. The set of observables $\mathcal{O}$ is noncontextual.

While from the Kochen-Specker theorem and our discussion of strong contextuality it is mathematically conceivable that only some observables are forced to be value indefinite, while others remain both noncontextual and value definite, this would be a rather strange scenario due to the overall uniformity and symmetry of these arguments. Regardless, if we can guarantee that one observable P_a is value definite, with the value 1 (e.g., by preparing the system in an eigenstate of P_a with eigenvalue 1), Corollary 2 gives us some observables that must be value indefinite.

C. Predictability implies value definiteness

A more subtle assumption relates to the question of when we should consider a physical observable to have a definite value associated with it, and the connection between these definite values and probability. Einstein, Podolsky, and Rosen (EPR), in their seminal paper on the EPR paradox as it is now known, said ([25], p. 777):

> If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality[1] [(e.p.r.)] corresponding to this physical quantity.

From the physicist's point of view, the ability to predict the value of an observable with certainty seems sufficient to posit the existence of a definite value associated with that observable. However, the identification that EPR make between

[1]An element of physical reality corresponds to the notion of a definite value, possibly contextual, as outlined in this paper.

certainty and probability one is less sound. Mathematically, the statement is simply not true: for infinite measure spaces probability zero events not only can, but must occur—every point has probability 0 under the Lebesgue measure. With a frequentist view of probability, the two notions cannot be united even for finite spaces. One can only say an event is certain if its complement is the empty set.

With the formalism of quantum mechanics entirely based on probability spaces, what then can we say about any definite values in physical reality? A deterministic theory is based on a description of a state which is complete in that it specifies definite values for all observables. The state in quantum theory, however, is given as a wave function, which in turn is determined by the operators of which the system is an eigenstate. Quantum theory is thus based on the notion that a physical state is "completely characterized by the wave function," which is an eigenstate of some operator and is determined for any context containing the said operator; as EPR note, the "physical quantity" corresponding to that operator has "with certainty" the corresponding eigenvalue ([25], p. 778). The theory then presents a probabilistic framework to express behavior in other contexts. A reasonable assumption based on this principle is the following:

Eigenstate assumption. Let $|\psi\rangle$ be a (normalized) quantum state and v be a faithful assignment function. Then $v(P_\psi, C) = 1$ and $v(P_\phi, C) = 0$ for any context $C \in \mathcal{C}$ with $P_\psi, P_\phi \in C$.

While this is a reasonable condition under which to assign an initial set of definite values, its use is restricted to contexts containing the "preparation" observable. In order to extend this, we must more carefully formulate the notion of being able to predict the value of an observable with certainty.

Let us consider a system which we prepare, measure, rinse, and repeat ad infinitum. Let $\mathbf{x} = x_1 x_2 \ldots$ denote the infinite sequence produced by concatenating the outputs of these measurements. Fix a set of observables $\mathcal{O}$ and contexts $\mathcal{C}$ and let o_i, C_i denote the observable and corresponding context of the ith measurement. We can predict with certainty the value of each measurement if there exists a computable function $f : \mathbf{N} \times \mathcal{O} \times \mathcal{C} \to \{0,1\}$ such that, for every i, $f(i, o_i, C_i) = x_i$. Why do we require that f be computable? Since we must with every measurement obtain a result, there is guaranteed to be some function giving $\mathbf{x}$ from the measurements, but if it is not computable then this function offers no method to predict the values. Why do we formulate this for infinite sequences? The notion of computability, and thus concrete predictability, only makes sense for infinite sequences; it is clear that any technique which allows prediction of every measurement with certainty must also do so when the measurements are continued ad infinitum.

The last assumption is the following:

Elements of physical reality (e.p.r.) assumption. If there exists a computable function $f : \mathbf{N} \times \mathcal{O} \times \mathcal{C} \to \{0,1\}$ such that for every i $f(i, o_i, C_i) = x_i$, then there is a definite value associated with o_i at each step [i.e., $v_i(o_i, C_i) = f(i, o_i, C_i)$].

We note that the assumption above does not postulate the existence of an effective way to find or to compute the computable function f: such a function simply exists. This is visible in classical hidden-variable-type theories such as statistical mechanics for thermodynamics, where we can hardly claim to be able to even describe fully the momentum and position of each particle in a gas, but it is sufficient to know that we *can* do so and that these hidden variables exist in the sense that they allow us, in principle, to predict the outcome of any measurement in advance. Furthermore, we follow EPR in noting that this is certainly only a sufficient condition for definite values to be present; it is by no means necessary.

D. Connection to quantum theory

The final step is to justify our requirement of the admissibility of the assignment function.

We first note the following: Let $C = \{P_1, \ldots, P_n\}$ be a context of projection observables, v a faithful assignment function and $v(P_1, C) = 1$. Since P_1 and P_i $(i \neq 1)$ are compatible (physically comeasurable), if we measure them both, the system will collapse into the eigenstate of P_1 corresponding to the eigenvalue 1. Since this final state would also be an eigenstate of P_i, it follows from the fact that $\sum_{j=1}^{n} P_j = \mathbf{1}$ that this state corresponds to the eigenvalue 0 of P_i and hence $v(P_i, C) = 0$. Hence we conclude that $v(P_i, C) = 0$ for all $2 \leqslant i \leqslant n$. By a similar argument, we see that if instead $v(P_i, C) = 0$ for $2 \leqslant i \leqslant n$ we must have $v(P_1, C) = 1$.

From these facts it follows directly that a faithful assignment function v must be admissible, thus justifying our definition of an admissible v. Indeed, admissibility of v is the direct generalization of the "sum rule" used in proofs of the Kochen-Specker theorem [3,26] to the case where value definiteness is not assumed. In our deduction of the requirement of admissibility we are particularly careful in using our assumptions to show that admissibility is required if simple relations of projection observables are to be satisfied.

As a consequence, we get the following useful form of Corollary 2 which we will utilize in the remainder of the paper.

Corollary 3. Let $|\psi\rangle \in \mathbb{C}^3$ be a quantum state describing a system. Also let $|\phi\rangle \in \mathbb{C}^3$ be any other state which satisfies $\sqrt{5/14} \leqslant |\langle\psi|\phi\rangle| \leqslant \frac{3}{\sqrt{14}}$. Then, assuming noncontextuality, P_ϕ cannot be assigned a definite value by a faithful assignment function.

Proof. From the eigenstate assumption, P_ψ must be assigned the value 1. By Corollary 2 and the requirement for a faithful assignment function to be admissible, it follows that P_ϕ must be value indefinite. ■

IV. A RANDOM NUMBER GENERATOR

From our assumptions of noncontextuality along with our physical assumptions in the preceding section, we arrived at the key result of Corollary 3, which allows us to identify particular observables which must be value indefinite. This guarantee of indefiniteness, which both the Bell [1] and Kochen-Specker theorems cannot yield, adds extra conviction to the widely accepted (but not proven) unpredictability of the result of quantum measurements. Since quantum random number generators (QRNGs) [27–33] depend entirely on this, it seems clear we should make use of this extra certification in their design. In this section we present such a design of a QRNG and use Corollary 3 to prove that such a device will produce strongly incomputable sequences of bits—a strong, explicit certification of the QRNG.

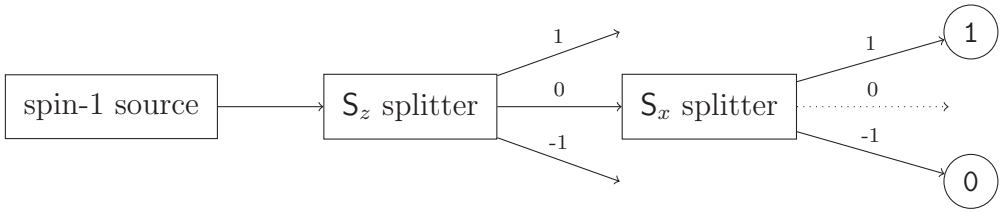

FIG. 4. Experimental setup of a configuration of quantum observables rendering random bits certified by quantum value indefiniteness.

A. Random number generator design

The QRNG setup is shown in Fig. 4. Spin-1 particles are prepared in the $S_z = 0$ state (thus, by the eigenstate assumption, this operator has a definite value), and then the S_x operator is measured. Since the preparation state is an eigenstate of the $S_x = 0$ projector with eigenvalue 0, this outcome has a definite value and cannot be obtained. Thus, while the setup uses spin-1 particles, the outcomes are dichotomic and the $S_x = \pm 1$ outcomes can be assigned 0 and 1, respectively. Furthermore, since $\langle S_z = 0 | S_x = \pm 1\rangle = 1/\sqrt{2}$, it follows from Corollary 3 that neither of the $S_x = \pm 1$ outcomes can have a pre-assigned definite value.

While this design is very simple, it has the two key properties we need from such a QRNG: it produces bits certified by value indefiniteness, and it produces the bits 0 and 1 independently and with 50:50 probability.

B. Certification via value indefiniteness

Consider the QRNG described in the previous section, and let us consider that we run it repeatedly "to infinity;" that is, we use it repeatedly to generate bits and concatenate them together to produce, in the limit, the binary sequence $\mathbf{x} = x_1 x_2 \ldots x_n \ldots$. Here we consider the sequence $\mathbf{x}$ produced in such a manner and show that, under our assumptions, it is guaranteed to be *incomputable*. Note that we are using the measurement assumption here, since we must assume that $\mathbf{x}$ is actually produced (not that, for example, all infinite sequences are generated in different universes).

Before presenting our argument we note that Martin-Löf's theorem in algorithmic information theory [34] shows that *there are no pure, true, or perfect random sequences*: there are patterns in every sequence, a deterministic provable fact which is much stronger than the typical highly probable results (facts true with probability one) proved in probability theory. Because we cannot speak about pure, true or perfect randomness we have no option but to study degrees and symptoms of randomness: some sequences are more random than others. Uniform distribution within a sequence (Borel normality [35]) is a symptom of randomness; however, there exist computable uniformly distributed sequences (e.g., the Champernowne sequence [34]), which are far from being random in any meaningful way. Unpredictability is another symptom; (strong) incomputability is one mathematical way to express it. Uniform distribution and unpredictability are independent; while the lack of uniform distribution can be easily mitigated by procedures à la von Neumann [36], transforming a computable sequence into an incomputable one is a much more difficult problem.

Quantum randomness is usually qualified in terms of the probability distribution of the source. This only allows for probabilistic claims about the outcomes of individual measurements. For example, with probability one any sequence of quantum random bits is incomputable; such a statement is weaker than saying that the sequence is provably incomputable. Nevertheless, claims made in different articles, even recent ones such as Refs. [28,37] or web sites [38,39], according to which "perfect randomness can be obtained via quantum experiments," are only of this statistical nature. Here we are able to prove the guaranteed incomputability of quantum randomness; however, due to Martin-Löf's theorem, even this result cannot be called "perfect randomness."

For the sake of contradiction let us assume that $\mathbf{x}$ as described above is computable. Then, by definition, there must exist a Turing machine T (and thus a computable function) that can be associated with $\mathbf{x}$ allowing us to predict with certainty every value x_i. From the e.p.r. assumption, it follows that each observable o_i is value definite and $v_i(o_i, C) = x_i$. This contradicts the implications of Corollary 3. Thus we conclude that $\mathbf{x}$ must be incomputable.

This proof can easily show the stronger claim: that $\mathbf{x}$ is *bi-immune*; that is, no infinite subsequence of $\mathbf{x}$ is computable. This can easily by seen by the same argument: if there was a computable subsequence then we could assign definite values to the observables giving rise to this subsequence, contradicting our assumption of value indefiniteness everywhere.

We have proved:

Assume the noncontextuality, measurement, eigenstate and e.p.r. assumptions. Then there exits a QRNG which generates a bi-immune binary sequence.

We further note that this result is more general than that proved in Ref. [40] and does not require any assumption about the uniformity of the bits produced.

C. Experimental robustness

Before we proceed to describe an explicit realisation of the QRNG described above, we wish to briefly make a couple of points on the robustness of this certification by value indefiniteness to experimental imperfections.

We can describe the measurement context more generally by the spin observable $S(\theta,\phi)$, where θ and ϕ are the polar and azimuthal angles, respectively, and we thus have $S_x = S(\pi/2,0)$ and $S_z = S(0,0)$. Explicitly, this operator is represented in matrix form as

$$S(\theta,\phi) = \begin{pmatrix} \cos(\theta) & \frac{e^{-i\phi}\sin(\theta)}{\sqrt{2}} & 0 \\ \frac{e^{i\phi}\sin(\theta)}{\sqrt{2}} & 0 & \frac{e^{-i\phi}\sin(\theta)}{\sqrt{2}} \\ 0 & \frac{e^{i\phi}\sin(\theta)}{\sqrt{2}} & -\cos(\theta) \end{pmatrix}. \quad (1)$$

Misalignment and imperfection in the experimental setup will, in general, lead to angles θ and ϕ differing slightly from $\pi/2$ and 0, respectively. While a change in ϕ only induces a phase shift and does not alter the probability of measuring any particular eigenvalue, a change in θ will alter the probabilities of detection. However, a detailed calculation shows that

$$|\langle \mathsf{S}_z = 0|\mathsf{S}(\theta,\phi) = \pm 1\rangle| = \sin\theta/\sqrt{2}, \tag{2}$$

and the difference in probabilities of measuring a bit as 0 or 1 is not affected by such a change in θ. This is in distinct contrast to setups based on single beam splitters, in which misalignment introduces bias into the distribution of bits.

From Corollary 3, we see that the QRNG will provide bits by measurement of $\mathsf{S}(\theta,\phi)$ that are certified by value indefiniteness whenever $\sqrt{5/14} \leqslant |\langle \mathsf{S}_z = 0|\mathsf{S}(\theta,\phi) = \pm 1\rangle| \leqslant \frac{3}{\sqrt{14}}$. This inequality is, from Eq. (2), readily seen to be satisfied for angles $\frac{\pi}{3} \leqslant \theta \leqslant \frac{2\pi}{3}$. This has the important consequence of protecting against inevitable experimental misalignment: even in the presence of relatively significant misalignment, the device would produce bits which are certified by value indefiniteness. Otherwise, if the certification only held for the ideal case of $\frac{\pi}{2}$, any experimental imperfections would render this theoretical result inapplicable to any real experiment.

Furthermore, calculation shows that $\langle \mathsf{S}_z = 0|\mathsf{S}(\theta,\phi) = 0\rangle = \cos\theta$, and since $\langle \mathsf{S}_z = 0|\mathsf{S}(\theta,\phi) = 0\rangle = 0$ only when $\theta = \frac{\pi}{2}$, a third detector measuring the $|\mathsf{S}(\theta,\phi) = 0\rangle$ outcome could be employed to monitor the degree of misalignment present in the system. The number of counts at this detector would allow quantification of the angle θ and provide an experimental method to test that the condition of $\sqrt{5/14} \leqslant \langle \mathsf{S}_z = 0|\mathsf{S}(\theta,\phi) = \pm 1\rangle \leqslant \frac{3}{\sqrt{14}}$ is indeed being realized. Without monitoring this third outcome, one could not determine from the $|\mathsf{S}(\theta,\phi) = \pm 1\rangle$ counts alone if this is indeed the case.

V. GENERALIZED BEAM SPLITTER QUANTUM RANDOM NUMBER GENERATOR

In this section we describe a physical realisation of the QRNG described in the previous section. Since it is not particularly feasible to directly use spin-1 particles in a QRNG with an acceptably high bit rate, the realisation we present uses photons and is expressed in terms of generalized beam splitters [41–43]. Generalized beam splitters are based on the possibility to (de)compose an arbitrary unitary transformation U_n in n-dimensional Hilbert space into two-dimensional transformations U_2 of two-dimensional subspaces thereof; a possibility that can be used to parametrize U_n [44]. In more physical terms, they amount to serial stacks of phase shifters and beam splitters in the form of an interferometer with n input and output ports, beam splitter such that the beam splitters affect only two (sub)paths which, together with the phase shifters (affecting single paths at any one time), realize the associated transformations in $U(2)$. These components can be conveniently arranged into "triangle form" with n in- and out-bound beam paths.

For the sake of an explicit demonstration, consider an orthonormal cartesian standard basis $|1\rangle \equiv (1,0,0)$, $|0\rangle \equiv (0,1,0)$, and $|-1\rangle \equiv (0,0,1)$. Then, in order to realize observables such as the spin state observables $S(\theta,\phi)$ and, in particular, spin states measured along the x axis; that is, for $\theta = \frac{\pi}{2}$ and $\phi = 0$,

$$\mathsf{S}_x = \mathsf{S}\left(\frac{\pi}{2},0\right) = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & 0 \end{pmatrix}, \tag{3}$$

in terms of generalized beam splitters, the associated normalized row eigenvectors

$$\begin{aligned} |\mathsf{S}_x : +1\rangle &\equiv \frac{1}{2}(1,\sqrt{2},1), \\ |\mathsf{S}_x : 0\rangle &\equiv \frac{1}{\sqrt{2}}(1,0,-1), \\ |\mathsf{S}_x : -1\rangle &\equiv \frac{1}{2}(1,-\sqrt{2},1), \end{aligned} \tag{4}$$

have to be "stacked" on top of one another [41], thereby forming a unitary matrix U_x which corresponds to the spin-state operator S_x for spin-state measurements along the x axis; more explicitly,

$$\mathsf{U}_x = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & -\sqrt{2} & 1 \end{pmatrix}. \tag{5}$$

While many variations on the unitary matrix to represent a beam splitter exist [41,45–47], without loss of generality we can represent an arbitrary $U(2)$ matrix realized by a beam splitter and external phase shift as

$$\begin{pmatrix} \sqrt{T} & ie^{i\phi}\sqrt{R} \\ i\sqrt{R} & e^{i\phi}\sqrt{T} \end{pmatrix}, \tag{6}$$

where ϕ represents the phase of an external phase shifter on the second input port, and $T, R \in [0,1]$ are the transmittance and reflectance of the beam splitter, respectively (with $R + T = 1$). The beam-splitter arrangement to realize U_x can be found by transforming U_x into the identity matrix I_3 by successive right multiplication by adjoints of $U(2)$ matrices of the above form—each one making an individual off-diagonal element equal to zero—followed by a final set of phase shifters [41].

In our specific case, we have

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & -i \end{pmatrix}\begin{pmatrix} \sqrt{\frac{1}{3}} & \sqrt{\frac{2}{3}} & 0 \\ i\sqrt{\frac{2}{3}} & -i\sqrt{\frac{1}{3}} & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} \sqrt{\frac{3}{4}} & 0 & -i\sqrt{\frac{1}{3}} \\ 0 & 1 & 0 \\ i\sqrt{\frac{1}{4}} & 0 & -\sqrt{\frac{3}{4}} \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{\frac{1}{3}} & \sqrt{\frac{2}{3}} \\ 0 & i\sqrt{\frac{2}{3}} & -i\sqrt{\frac{1}{3}} \end{pmatrix} = \mathsf{U}_x. \tag{7}$$

This corresponds to three beam splitters with transmittances $T_{3,2} = T_{2,1} = \frac{1}{3}$, $T_{3,1} = \frac{3}{4}$, and phases $\phi_{3,2} = \phi_{2,1} = -\pi/2$, $\phi_{3,1} = \pi$, where $T_{i,j}$ and $\phi_{i,j}$ are the parameters for the beam

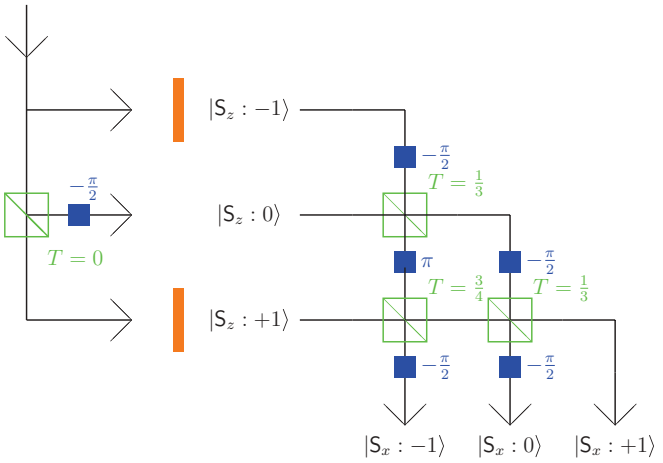

FIG. 5. (Color online) Configuration of a random number generator with a preparation and a measurement stage, including filters blocking $|S_z:-1\rangle$ and $|S_z:+1\rangle$. (For ideal beam splitters, these filters would not be required.) The measurement stage (right array) realizes a unitary quantum gate U_x, corresponding to the projectors onto the S_x state observables for spin-state measurements along the x axis, in terms of generalized beam splitters.

splitter operating on beams i and j (beams 1, 2, 3 correspond to $S_z = +1, 0, -1$, respectively). Two final phase shifts of $-\pi/2$ are needed on beams 2 and 3. The physical realisation of U_x is depicted in Fig. 5.

This setup is equivalent to the spin-1 setup for which we are guaranteed value indefiniteness under the conditions discussed in the previous section. Even in the case of non-perfectly configured beam splitters, as long as the observable corresponding to the unitary transformation implemented by the beam splitters has eigenstates $|a = \pm 1\rangle$ (corresponding to output ports 1 and 3) which fall within the bounds $\sqrt{5/14} \leqslant \langle S_z = 0|a = \pm 1\rangle \leqslant \frac{3}{\sqrt{14}}$ then the QRNG will still be protected by value indefiniteness. As discussed in the previous section, this allows for a considerable amount of error (more than would be desirable with respect to deviation from 50 : 50 bias) under which value indefiniteness is still guaranteed.

VI. MONITORING VALUE INDEFINITENESS

The rendition of value indefiniteness requires a quantized system with at least three mutually exclusive outcomes, corresponding to an associated Hilbert-space dimension equal to the number of these outcomes—a direct consequence of the Kochen-Specker theorem.

Of course, if one is willing to accept physical value indefiniteness based purely on formal Hilbert-space models of quantum mechanics [5], there is no further need of empirical evidence. In this line of thinking, Theorem 1, and hence the quantum value indefiniteness resulting from it via Corollary 2, needs no more empirical corroboration than the arithmetic fact that, in Peano arithmetic with standard addition, one plus one equals two.

QRNGs which monitor Bell-inequality violation simultaneously with bit generation have been proposed in the literature [28,48]. Given the nontrivial assumptions used in the proof of Theorem 1—in particular, the mutual physical coexistence of complementary observables—should our QRNG be monitored in this way too, in addition to value indefiniteness certification?

First, we stress that, in contrast with our proposed QRNG, the aforementioned devices require an initial random seed and hence operate as a secure randomness *expander*, rather than *generator*: The quality of randomness produced by such a device depends crucially upon the quality of randomness of the seed.

Second, violation of Bell-inequalities alone is a purely statistical phenomenon and only indicates nonclassical correlations: in no way does it necessitate a Hilbert-space structure and hence it cannot give the certification of (strong) incomputability that our proposal does via value indefiniteness.

Third, in the case that our QRNG is treated as an untrusted device, as is common in cryptography (due to the user's inability to verify the device's workings), the set up could be modified to test such inequalities. This is the scenario in which monitoring inequality violation has most to offer, since violation of Bell inequalities can be derived from Kochen-Specker–type arguments[2] and thus gives some indication of nonclassicality in the absence of trust in the device, even if it cannot guarantee incomputability. An even better monitoring method—which might necessitate a revision of our current QRNG set up—may use the type of nonclassical outcomes typically encountered in empirical realizations of Greenberger-Horne-Zeilinger type arguments [49,50] because, at least ideally, they do not involve any statistics but require a violation of local realism at every triple of outcomes.

To summarize, we have presented a formal conceptualization of *value (in)definiteness* and proven that there always exists an admissible assignment function making a *single* observable value definite; one cannot hope to prove *all* observables are value indefinite. We also showed that, in an extension of the Kochen-Specker theorem, after preparing a pure state in three-dimensional Hilbert space, certain precisely identified observables are *provably value indefinite.*

We have applied these results to a proposal to generate bit sequences by a quantum random number generator. Any such sequence is, as we showed, then "certified by" quantum value indefiniteness (in the sense of the Bell, Greenberger-Horne-Zeilinger, and Kochen-Specker theorems) to produce a strongly incomputable sequence of bits.

To what extent we can guarantee value indefiniteness remains an open question. We know that not all observables can be value indefinite, and at least those in the star-shaped setup of Fig. 1 can be guaranteed to be, but how far does this value indefiniteness go? We conjecture that this is as far as one can go; that *only a single* observable in the Hilbert space can be assigned the value one, and only those orthogonal to the said observable can be assigned the value 0—any other observables must, under the assumption of noncontextuality be value indefinite.

[2]Such violations are often referred to as "proofs of the Kochen-Specker theorem," or "proofs of quantum contextuality" [9–12,52].

ACKNOWLEDGMENTS

We are grateful to Kohtaro Tadaki for insightful comments which improved the paper, as well as the anonymous referees who provided helpful comments. We thank Michael Reck for the code producing the generalized beam-splitter setup for an arbitrary unitary transformation. Abbott, Calude, and Svozil have been supported in part by Marie Curie FP7-PEOPLE-2010-IRSES Grant RANPHYS. Conder has been supported in part by a University of Auckland Summer Scholarship.

[1] John S. Bell, Rev. Mod. Phys. **38**, 447 (1966).
[2] Ernst Specker, Dialectica **14**, 239 (1960).
[3] Simon Kochen and Ernst P. Specker, J. Math. Mech. (now Indiana University Math. J.) **17**, 59 (1967).
[4] Due to complementarity, not all may be all simultaneously comeasurable (i.e., formally, commuting).
[5] John von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, 1955).
[6] Garrett Birkhoff and John von Neumann, Ann. Math. **37**, 823 (1936).
[7] Simon Kochen and Ernst P. Specker, in *Symposium on the Theory of Models, Proceedings of the 1963 International Symposium at Berkeley* (North Holland, Amsterdam, 1965), pp. 177–189.
[8] Simon Kochen and Ernst P. Specker, in *Proceedings of the 1964 International Congress for Logic, Methodology, and Philosophy of Science, Jerusalem* (North Holland, Amsterdam, 1965), pp. 45–57.
[9] Y. Hasegawa, R. Loidl, G. Badurek, M. Baron, and H. Rauch, Phys. Rev. Lett. **97**, 230401 (2006).
[10] H. Bartosik, J. Klepp, C. Schmitzer, S. Sponar, A. Cabello, H. Rauch, and Y. Hasegawa, Phys. Rev. Lett. **103**, 040403 (2009).
[11] G. Kirchmair, F. Zähringer, R. Gerritsma, M. Kleinmann, O. Gühne, A. Cabello, R. Blatt, and C. F. Roos, Nature (London) **460**, 494 (2009).
[12] Elias Amselem, Magnus Rådmark, Mohamed Bourennane, and Adán Cabello, Phys. Rev. Lett. **103**, 160405 (2009).
[13] Adán Cabello, Phys. Rev. Lett. **101**, 210401 (2008).
[14] Itamar Pitowsky, Phys. Rev. Lett. **48**, 1299 (1982).
[15] Note that there exist models of complementarity such as automaton logic or generalized urn models which are value definite [51].
[16] Neal Zierler and Michael Schlessinger, Duke Math. J. **32**, 251 (1965).
[17] Gudrun Kalmbach, *Measures and Hilbert Lattices* (World Scientific, Singapore, 1986).
[18] Václav Alda, Aplikace Matematiky (Applications of Mathematics) **25**, 373 (1980).
[19] Václav Alda, Aplikace Matematiky (Applications of Mathematics) **26**, 57 (1981).
[20] Pavel Pták and Sylvia Pulmannová, *Orthomodular Structures as Quantum Logics* (Kluwer Academic Publishers, Dordrecht, 1991).
[21] Karl Svozil and Josef Tkadlec, J. Math. Phys. **37**, 5380 (1996).
[22] Avshalom C. Elitzur, Sandu Popescu, and Daniel Rohrlich, Phys. Lett. A **162**, 25 (1992).
[23] Karl Svozil, Nat. Comput. **11**, 261 (2012).
[24] Ernst Specker (private communication).
[25] Albert Einstein, Boris Podolsky, and Nathan Rosen, Phys. Rev. **47**, 777 (1935).
[26] Asher Peres, Found. Phys. **26**, 807 (1996).
[27] Osung Kwon, Young-Wook Cho, and Yoon-Ho Kim, Appl. Opt. **48**, 1774 (2009).
[28] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature (London) **464**, 1021 (2010).
[29] André Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden, J. Mod. Opt. **47**, 595 (2000).
[30] Karl Svozil, Phys. Rev. A **79**, 054306 (2009).
[31] Michael A. Wayne, Evan R. Jeffrey, Gleb M. Akselrod, and Paul G. Kwiat, J. Mod. Opt. **56**, 516 (2009).
[32] M. Stipčević and B. Medved Rogina, Rev. Sci. Instrum. **78**, 045104 (2007).
[33] Hai-Qiang Ma, Yuejian Xie, and Ling-An Wu, Appl. Opt. **44**, 7760 (2005).
[34] Cristian Calude, *Information and Randomness—An Algorithmic Perspective*, 2nd ed. (Springer, Berlin, 2002).
[35] Émile Borel, Rendiconti del Circolo Matematico di Palermo (1884–1940) **27**, 247 (1909).
[36] Alastair A. Abbott and Cristian S. Calude, Computability **1**, 59 (2012).
[37] Zeeya Merali, Nat. News (2010).
[38] ID Quantique SA, *QUANTIS. Quantum Number Generator* (idQuantique, Geneva, Switzerland, 2001–2009).
[39] ANU Quantum Optics, *ANU. Quantum Random Number Generator* (ANU Quantum Optics, Australian National University, 2012) http://photonics.anu.edu.au/qoptics/Research/qrng.php accessed on July 9th, 2012.
[40] Cristian S. Calude and Karl Svozil, Adv. Sci. Lett. **1**, 165 (2008).
[41] M. Reck, Anton Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).
[42] Marek Zukowski, Anton Zeilinger, and Michael A. Horne, Phys. Rev. A **55**, 2564 (1997).
[43] Karl Svozil, J. Phys. A: Math. Gen. **38**, 5781 (2005).
[44] F. D. Murnaghan, *The Unitary and Rotation Groups* (Spartan Books, Washington, DC, 1962).
[45] A. Zeilinger, Am. J. Phys. **49**, 882 (1981).
[46] R. A. Campos, B. E. A. Saleh, and M. C. Teich, Phys. Rev. A **40**, 1371 (1989).
[47] Daniel M. Greenberger, Mike A. Horne, and Anton Zeilinger, Phys. Today **46**, 22 (1993).
[48] Umesh Vazirani and Thomas Vidick, Philos. Trans. R. Soc., A **370**, 3432 (2012).
[49] Dik Bouwmeester, Jian-Wei Pan, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999).
[50] Jian-Wei Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger, Nature (London) **403**, 515 (2000).
[51] Karl Svozil, Int. J. Theor. Phys. **44**, 745 (2005).
[52] Radek Lapkiewicz, Peizhe Li, Christoph Schaeff, Nathan K. Langford, Sven Ramelow, Marcin Wieśniak, and Anton Zeilinger, Nature (London) **474**, 490 (2011).