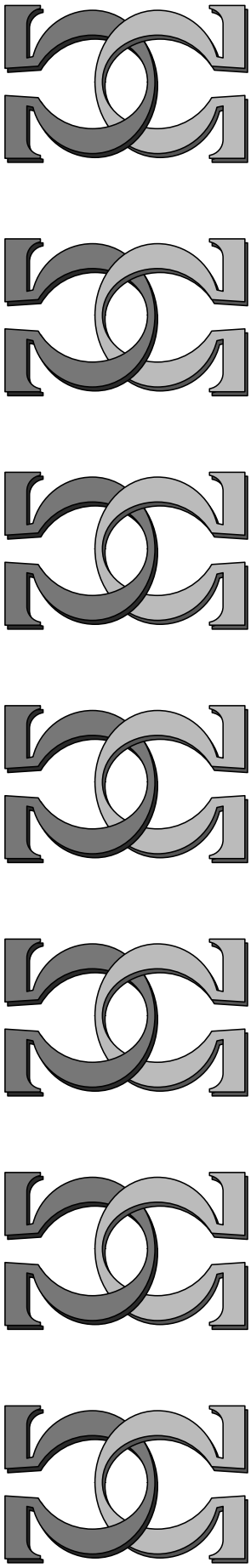

CDMTCS
Research
Report
Series

Kochen-Specker Theorem Revisited and Strong Incomputability of Quantum Randomness

A. A. Abbott[2], C. S. Calude[1,2], J. Conder[2], K. Svozil[2,3]

[1]Isaac Newton Institute for Mathematical Sciences, Cambridge, UK
[2]University of Auckland, NZ
[3]Vienna University of Technology, Austria

CDMTCS-422
July 2012

Centre for Discrete Mathematics and
Theoretical Computer Science

Kochen-Specker Theorem Revisited and Strong 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§

(Dated: September 17, 2012)

Abstract

We present a stronger variant of the Kochen-Specker theorem in which some quantum observables are identified to be *provably value indefinite*. This result is utilised for the construction and certification of a dichotomic quantum random number generator operating in a three-dimensional Hilbert space.

PACS numbers: 03.67.Lx, 05.40.-a, 03.65.Ta, 03.67.Ac, 03.65.Aa

Keywords: Kochen-Specker theorem, quantum value indefiniteness, quantum randomness, quantum indeterminism, random processes, quantum algorithms

* a.abbott@auckland.ac.nz

† cristian@cs.auckland.ac.nz; http://www.cs.auckland.ac.nz/~cristian

‡ jcon068@aucklanduni.ac.nz

§ svozil@tuwien.ac.at; http://tph.tuwien.ac.at/~svozil

I. LOCATED QUANTUM VALUE INDEFINITENESS

The Kochen-Specker theorem [1, 2] expresses the impossibility of a global truth value assignment to some particular (finite) collection of propositions under "mild" side conditions. In particular, the theorem requires that co-measurable (commuting) observables should behave quasi-classically (an assumption which leads to Gleason's theorem) and the outcomes of measurements of observables are independent of whatever other co-measurable observables are measured alongside them (non-contextuality assumption).

Thereby, the Kochen-Specker theorem does *not* explicitly identify certain particular observables which violate one or more of these prerequisites. Indeed, the Kochen-Specker theorem was not 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 applies to.

However, contemporary quantum random number 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 non-classicality than complementarity, *quantum value indefiniteness* being one of them.[3] 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[4] 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 utilised for that purpose.* Thus, one needs a different, in the sense of locatedness of violation of non-classicality, 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 communication presents such an argument, which will be utilised 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 non-located 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

We denote the set of natural numbers (in which we include 0) by $\mathbb{N} = \{0, 1, 2, \dots\}$, the positive integers by $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$, and the set of complex numbers by $\mathbb{C}$. We use the standard quantum mechanical bra-ket notation. That is, we denote vectors in the Hilbert space $\mathbb{C}^n$ by $|\cdot\rangle$. If we fix an orthonormal basis for $\mathbb{C}^n$ as $\{|a_1\rangle, \dots, |a_n\rangle\}$, then an arbitrary $|\psi\rangle \in \mathbb{C}^n$ can be written $|\psi\rangle = \sum_{i=1}^n c_i |a_i\rangle$ where $c_i \in \mathbb{C}$ for $1 \leq i \leq n$. If $|\phi\rangle = \sum_{i=1}^n d_i |a_i\rangle$ is another vector in $\mathbb{C}^n$, then the inner product of $|\psi\rangle$ and $|\phi\rangle$ is $\langle\phi|\psi\rangle = \sum_{i=1}^n c_i d_i^*$. The outer product $|\psi\rangle\langle\phi|$ is an $n \times n$ complex matrix where the entry at row i and column j is $(|\psi\rangle\langle\phi|)_{i,j} = c_i d_j^*$. We will have particular interest in the projection operators (represented by Hermitian matrices) projecting on to the linear space spanned by a non-zero vector $|\psi\rangle$, namely $P_\psi = \frac{|\psi\rangle\langle\psi|}{\langle\psi|\psi\rangle}$. 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.

B. Formal framework

We fix an $n \in \mathbb{N}^+$. Let $\mathcal{O} \neq \varnothing$ be an abstract set of observables, $\perp$ a symmetric relation on $\mathcal{O} \times \mathcal{O}$, and $\mathcal{C} \subseteq \{\{o_1, o_2, \dots o_n\} \mid o_i \in \mathcal{O} \text{ and } o_i \perp o_j \text{ for } i \neq j\}$ a set of contexts over $\mathcal{O}$. Let $v : \{(o, C) \mid o \in \mathcal{O}, C \in \mathcal{C} \text{ and } o \in C\} \xrightarrow{o} \{0, 1\}$ be a partial function, i.e. it may be

undefined for some values in its domain. We will call v an *assignment function*. 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 $v(o, C) \neq v(o', C')$.

Definition 1. 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.

Definition 2. The set $\mathcal{O}$ is *value definite* under v if every observable $o \in \mathcal{O}$ is value definite under v.

Definition 3. An observable $o \in \mathcal{O}$ is *non-contextual* 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.

Definition 4. The set of observables $\mathcal{O}$ is *non-contextual* under v if every observable $o \in \mathcal{O}$ which is not value indefinite (i.e. value definite in *some* context) is non-contextual under v. Otherwise, the set of observables $\mathcal{O}$ is *contextual*.

Definition 5. The set of observables $\mathcal{O}$ is *strongly contextual* under v if every observable $o \in \mathcal{O}$ is contextual under v.

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 will follow from Theorem 9.

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

which is value indefinite.

Definition 6. An assignment function v is *admissible* if the following hold for all $C \in \mathcal{C}$:

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

Example 7. As an example, let $n = 3$ and consider the set of observables $\mathcal{O} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ and contexts $\mathcal{C} = \{C_1 = \{0, 1, 2\}, C_2 = \{0, 3, 4\}, C_3 = \{0, 5, 6\}, C_4 = \{6, 7, 8\}\}$. This configuration is depicted by a Greechie[5] orthogonality diagram [6–8] in Fig. 1. Let our assignment function be defined as

$$v(0, C_1) = v(0, C_2) = v(6, C_4) = 1,$$

$$v(1, C_1) = v(2, C_1) = v(3, C_2) = v(4, C_2) = v(6, C_3) = v(7, C_4) = v(8, C_4) = 0,$$

and undefined elsewhere. Observables 0 and 6 are both contextual: although $v(0, C_1) = v(0, C_2) = 1$, observable 0 is value indefinite in C_3 since $v(0, C_3)$ is not defined; observable 6 is value definite but we have $v(6, C_3) \neq v(6, C_4)$. Observable 5 is value indefinite, since it appears only in C_3 and $v(5, C_3)$ is not defined. The other observables only appear in one context, in which they are all defined, and are thus non-contextual. This set $\mathcal{O}$ is neither value definite nor non-contextual. The function v is admissible, but the function v' specified exactly as v, except that it is defined for observable 5 in C_3 as $v'(5, C_3) = 0$, would not be admissible since the second condition for admissibility would not be satisfied in C_3.

This formal framework is presented for the purpose of our discussion of hidden variable theories in quantum mechanics. So far the framework is completely abstract, but, in order to discuss quantum mechanics, we need to remove some of this abstraction and specify some components. In particular, we consider quantum mechanical projection observables acting on a Hilbert space, and contexts are complete sets of compatible observables (i.e. sets of n orthogonal projectors; see below).

The assignment function v corresponds to the notion of a hidden variable: it specifies in advance the result obtained from the measurement of an observable. We do not concern ourselves with the mechanism of v, but rather with its possible existence subject to some

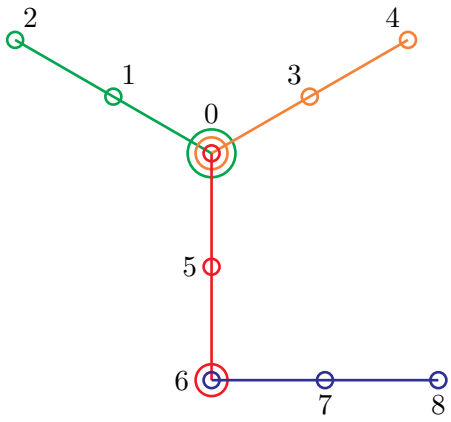

FIG. 1. (Color online) Greechie orthogonality diagram associated with the configuration of observables $\mathcal{C} = \{C_1 = \{0, 1, 2\}, C_2 = \{0, 3, 4\}, C_3 = \{0, 5, 6\}, C_4 = \{6, 7, 8\}\}$. Different contexts C_i are drawn in different colours.

constraints (specifically, the admissibility of v—we justify this more fully in Section III—requires that functions of the values associated with compatible observables satisfy the predictions of quantum theory). Our notion of value definiteness corresponds to the classical notion of determinism. An observable is value definite if v assigns it a definite value—i.e. we are able to predict in advance the value obtained via measurement. Non-contextuality, on the other hand, corresponds to the classical notion that the value obtained via measurement is independent of other compatible observables measured alongside it.

The notion of admissibility serves as an analogue to the notion of a *two-valued (dispersionless) measure* that is used in quantum logic [7–12], 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 [1, 2, 9, 11–14], as well as the stronger results which we will 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 Section III.

Formally we fix our framework as follows: with n fixed we consider the Hilbert space $\mathbb{C}^n$. The observables $\mathcal{O} \subseteq \{P_\psi \mid |\psi\rangle \in \mathbb{C}^n\}$ are projections onto one-dimensional linear subspaces of $\mathbb{C}^n$. These operators can be shown to commute exactly when the corresponding subspaces are orthogonal (or equal). Consequently, the relation $\perp$ on $\mathcal{O} \times \mathcal{O}$ is defined by: $P_\psi \perp P_\phi$

if and only if $|\psi\rangle$ is orthogonal to $|\phi\rangle$ (i.e. $\langle\psi|\phi\rangle = 0$). Therefore $P_\psi \perp P_\phi$ implies that P_ψ and P_ϕ are compatible, so contexts can be viewed as maximal sets of mutually compatible projection operators.

C. Kochen-Specker Theorem

The Kochen-Specker theorem [2] shows that if $n > 2$, then certain sets of observables in $\mathbb{C}^n$ cannot be both value definite and non-contextual under any admissible assignment function. This proves that it is impossible for all projection observables to be value definite and non-contextual. The Kochen-Specker theorem can be readily presented using the concepts developed above.

Theorem 8 (Kochen-Specker)**.** *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 non-contextual and value definite.*

D. Strong contextuality can not be guaranteed

How strong is the incompatibility between non-contextuality and value definiteness stated in the Kochen-Specker theorem? The theorem tells us that not every observable can be both non-contextual and value definite, but gives us no information as to 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 non-contextual.

Theorem 9. *Let $\mathcal{O}$ be a set of observables and $\mathcal{C} \subseteq \{\{o_1, o_2, \ldots o_n\} \mid o_i \in \mathcal{O}$ and $o_i \perp o_j$ for $i \neq j\}$ a set of contexts over $\mathcal{O}$. Then there exists an admissible assignment function v and an $o \in \mathcal{O}$ such that $v(o, C) = 1$ for every context $C \in \mathcal{C}$ with $o \in C$, and $\mathcal{O}$ is value definite under v.*

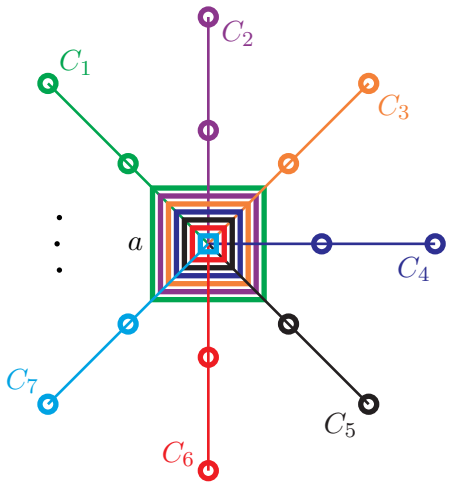

FIG. 2. (Color online) Greechie orthogonality diagram with an overlaid value assignment reflecting the proof of Theorem 9 associated with the configuration of contexts $S_a = \{C \mid C \in \mathcal{C} \text{ and } a \in C\} \subseteq \mathcal{C}$. Different contexts C_i are drawn in different colours.

Proof. Let $a \in \mathcal{O}$ be any observable, and 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. Define the assignment function v_a for $C \in S_a$ by

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

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 $\sum_{o \in C} v_a(o, C) = 1$. The function v_a is then admissible and assigns a definite value (namely 1) to the observable a (which was arbitrarily chosen) in a non-contextual 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 centre of the star, as depicted in Fig. 2.

The above proof actually shows that the following stronger statement is true:

Theorem 10. *For every observable $o \in \mathcal{O}$ there exists an admissible assignment function v_o under which $\mathcal{O}$ is value definite and o is non-contextual.*

Such a result should not be surprising in view of the predictions of quantum mechanics. Specifically, for a physical system prepared in an eigenstate of an observable o, the Born rule

predicts that the probability of measuring the corresponding eigenvalue is (non-contextually) 1. Nevertheless, it is important to place a bound on the degree of non-classicality [15, 16] that we can guarantee.

It turns out, however, 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 non-contextual. This finding is somewhat stronger than a similar result by Kochen and Specker [2, 7] derived from the (as Specker used to call them [17]) "bug"-type orthogonality diagrams (a sub-diagram 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 non-contextual, the other must be *value indefinite*. In light of Theorem 10, 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 sufficient for our purposes, and the larger values we found require significantly longer proofs.

Theorem 11. *Let $|a\rangle, |b\rangle \in \mathbb{C}^3$ be unit vectors such that $0 < |\langle a|b\rangle| \leq \frac{3}{\sqrt{14}}$. 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 non-contextual 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 $\{|a\rangle, |\psi\rangle, |\phi\rangle\}$,

TABLE I. Assignment table containing the representation of observable propositions (projectors), together with the contexts in which they appear. See Fig. 3 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	

and is understood to represent the corresponding projection observable P_φ. For brevity, we have omitted commas, brackets and normalisation constants from these vectors, and used the notation $\widetilde{n} = -n$ for $n \in \mathbb{N}$. 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 non-contextual 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. 3. We eventually obtain a contradiction, namely that $v(o, C_{24}) = 0$ for all $o \in C_{24}$ (the dotted line in Fig. 3). Therefore there does not exist such 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 $q = \sqrt{1-p^2}$. Then $(|b\rangle - |a\rangle\, p)\frac{1}{q}$ is a unit vector orthogonal to $|a\rangle$. Taking a cross

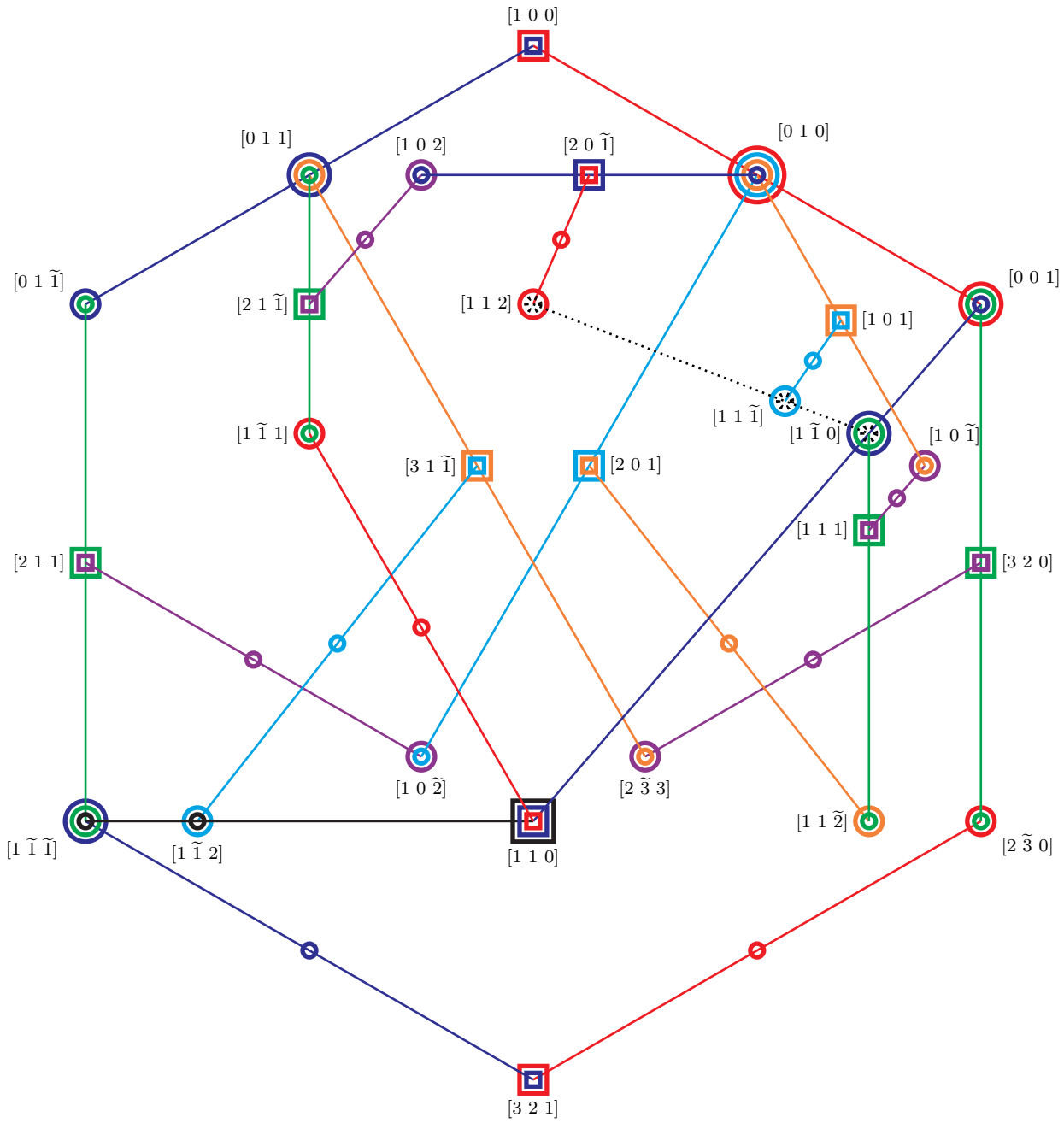

FIG. 3. (Color online) Greechie orthogonality diagram with an overlaid value assignment that can be used to visualise Table I. The circles and squares represent observables that will be given the values 0 and 1 respectively. They are joined by smooth lines which correspond to contexts, i.e. complete sets of compatible observables.

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 $z = \sqrt{1-x^2-y^2} \in \mathbb{R}$. 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, α is compatible with a because $\langle\alpha|a\rangle = 0$. Likewise, β is compatible with 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

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

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 non-contextual 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. 4. 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.

□

Corollary 12. *Let $|a\rangle, |b\rangle \in \mathbb{C}^3$ be unit vectors such that $\sqrt{\frac{5}{14}} \leq |\langle a|b\rangle| \leq \frac{3}{\sqrt{14}}$. Then there exists a set of projection observables $\mathcal{O}$ containing P_a and P_b, and a set of contexts $\mathcal{C}$ over*

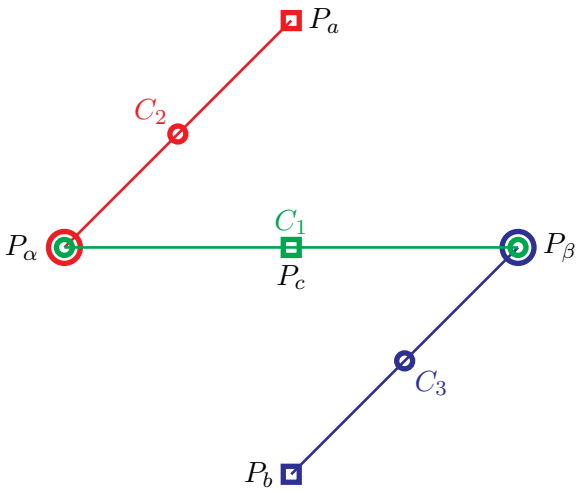

FIG. 4. (Color online) Greechie orthogonality diagram with an overlaid value assignment that illustrates the relationship between the contexts C_1, C_2 and C_3 in Theorem 11. The circles and squares represent observables that will be given the values 0 and 1 respectively. They are joined by smooth lines which represent contexts.

$\mathcal{O}$, such that there is no admissible assignment function under which $\mathcal{O}$ is non-contextual, 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 $q = \sqrt{1-p^2}$. 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 $p^2 \geq \frac{5}{14}$ and hence

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

From Theorem 11 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 non-contextual and a, b (a, 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 non-contextual, $v(P_a, C_1) = 1$ 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 non-contextuality, 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 12, 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 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.

Definition 13. Let v be a value assignment function. We say that v is a *faithful* representation of a realisation 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 Section 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 non-contextuality 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, [18]), 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 realism and instead require the non-contextuality of any pre-determined properties.

Non-contextuality assumption. The set of observables $\mathcal{O}$ is non-contextual.

While from the Kochen-Specker theorem and Theorem 9 it is mathematically conceivable that only some observables are forced to be value indefinite, while others remain both non-

contextual and value definite, this is a difficult stance to argue physically in favour of due to overall uniformity and symmetry. Regardless, if we can guarantee that one observable a is value definite, with the value 1 (e.g. by preparing the system in an eigenstate of a with eigenvalue 1), Corollary 12 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 [19, pp. 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[20] [(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 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 for which the system is an eigenstate of. Quantum theory is thus based on the notion that a physical state is "completely characterised 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 [19, pp. 778]. The theory then presents a probabilistic framework to express behaviour in other contexts. A reasonable assumption based on this principle is the:

Eigenstate assumption. Let $|\psi\rangle$ be a (normalised) quantum state and v a faithful assignment function. Then $v(o, C) = 1$ and $v(o', C) = 0$ for the projection observables $o = |\psi\rangle\langle\psi|$ and $o' \perp o$, and any context $C \in \mathcal{C}$ with $o, o' \in C$.

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

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. Further, 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 begin by stating the following well known fact about projection operators.

Fact 14. *Let* $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ *be an orthonormal basis for* $\mathbb{C}^n$*. Then* $\sum_{i=1}^{n} |\psi_i\rangle\langle\psi_i| = \mathbf{1}$*.*

Lemma 15. *Let* $C = \{o_1, \ldots, o_n\}$ *be a context of projection observables,* v *a faithful assignment function and* $v(o_1, C) = 1$*. Then* $v(o_i, C) = 0$ *for all* $2 \leq i \leq n$*.*

Proof. Since o_1 and o_i are compatible (physically co-measurable), if we measure them both, the system will collapse into the eigenstate of o_1, corresponding to the eigenvalue 1. Since this final state would also be an eigenstate of o_i, it follows from Fact 14 that this state corresponds to the eigenvalue 0 of o_i and hence $v(o_i, C) = 0$. □

Lemma 16. *Let* $C = \{o_1, \ldots, o_n\}$ *be a context of projection observables and* v *a faithful assignment function. Suppose that for* $2 \leq i \leq n$ *we have* $v(o_i, C) = 0$*. Then we must have* $v(o_1, C) = 1$*.*

Proof. Since o_2,...,o_n are all compatible, if we measure them all the system will collapse into a simultaneous eigenstate of each of these operators corresponding, in every case, to the eigenvalue 0. Since this final state is also an eigenstate of o_1, it follows from Fact 14 that this state corresponds to the eigenvalue 1 of o_1 and hence $v(o_1, C) = 1$. □

Theorem 17. *A faithful assignment function* v *must be admissible.*

Proof. The proof follows directly from the previous two Lemmata. □

This theorem justifies our definition of an admissible v. Indeed, admissibility of v is the direct generalisation of the "sum rule" used in proofs of the Kochen-Specker theorem [2, 21] to the case where value definiteness is not assumed. In our proof of Theorem 17 we are particularly careful in using our assumptions to show that admissibility is required if simple relations of projection observables are to be satisfied.

Corollary 18. *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 $\sqrt{\frac{5}{14}} \leq |\langle\psi|\phi\rangle| \leq \frac{3}{\sqrt{14}}$. Then, assuming non-contextuality, 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 12 and Theorem 17 it follows that P_ϕ must be value indefinite. □

IV. A RANDOM NUMBER GENERATOR

From our assumptions of non-contextuality along with our physical assumptions in the preceding section, we arrived at the key result of Corollary 18, which allows us to identify particular observables which must be value indefinite. This guarantee of indefiniteness, which both the Bell [18] 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) [22–28] 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 18 to prove that such a device will produce strongly incomputable sequences of bits—a strong, explicit certification of the QRNG.

A. Random number generator design

The QRNG setup is shown in Fig. 5. Spin-1 particles are prepared in the $\mathsf{S}_z = 0$ 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 $\mathsf{S}_x = 0$ projector

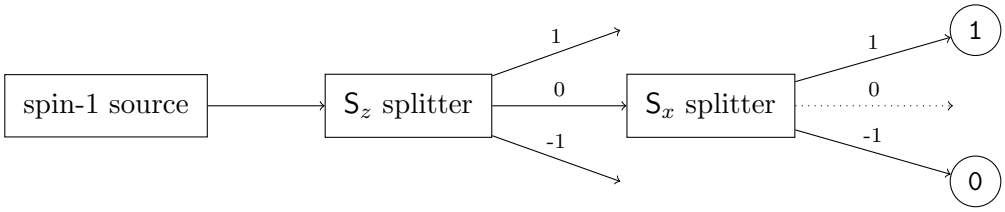

FIG. 5. Experimental setup of a configuration of quantum observables rendering random bits certified by quantum value indefiniteness.

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 $\mathsf{S}_x = \pm 1$ outcomes can be assigned 0 and 1 respectively. Further, since $\langle \mathsf{S}_z = 0 | \mathsf{S}_x = \pm 1 \rangle = 1/\sqrt{2}$, it follows from Corollary 18 that neither of the $\mathsf{S}_x = \pm 1$ outcomes can have 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'—i.e. 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 [29] 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. As 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 [30]) is a symptom of randomness: however, there exist computable uniformly distributed sequences, e.g. Champernowne sequence [29] 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 [31], 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 like [23, 32] or websites [33, 34], 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; but, 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 18. 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 sub-sequence 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:

Theorem 19. *Assume Non-contextuality, 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 [35] 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 $\mathsf{S}(\theta, \phi)$, where θ and ϕ are the polar and azimuthal angles respectively, and we thus have $\mathsf{S}_x = \mathsf{S}(\pi/2, 0)$ and $\mathsf{S}_z = \mathsf{S}(0, 0)$. Explicitly, this operator is represented in matrix form as

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

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 18, we see that the QRNG will provide bits by measurement of $\mathsf{S}(\theta, \phi)$ that are certified by value indefiniteness whenever $\sqrt{\frac{5}{14}} \leq |\langle \mathsf{S}_z = 0 | \mathsf{S}(\theta,\phi) = \pm 1\rangle| \leq \frac{3}{\sqrt{14}}$. This inequality is, from equation (2), readily seen to be satisfied for angles $\frac{\pi}{3} \leq \theta \leq \frac{2\pi}{3}$. 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 $\sqrt{\frac{5}{14}} \leq \langle \mathsf{S}_z = 0 | \mathsf{S}(\theta, \phi) = \pm 1 \rangle \leq \frac{3}{\sqrt{14}}$ is indeed being realised. 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. GENERALISED 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 generalised beam-splitters [36–38]. Generalised 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 parameterize U_n [39]. 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), realise 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 realise 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 generalised beam-splitters, the associated normalised row eigenvectors

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

have to be "stacked" on top of one another [36], 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 [36, 40–42], without loss of generality we can represent an arbitrary $U(2)$ matrix realised 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 realise 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 [36].

In our specific case, we have

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

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-splitter operating on beams i and j (beams 1,2,3 correspond to $\mathsf{S}_z = +1, 0, -1$ 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. 6.

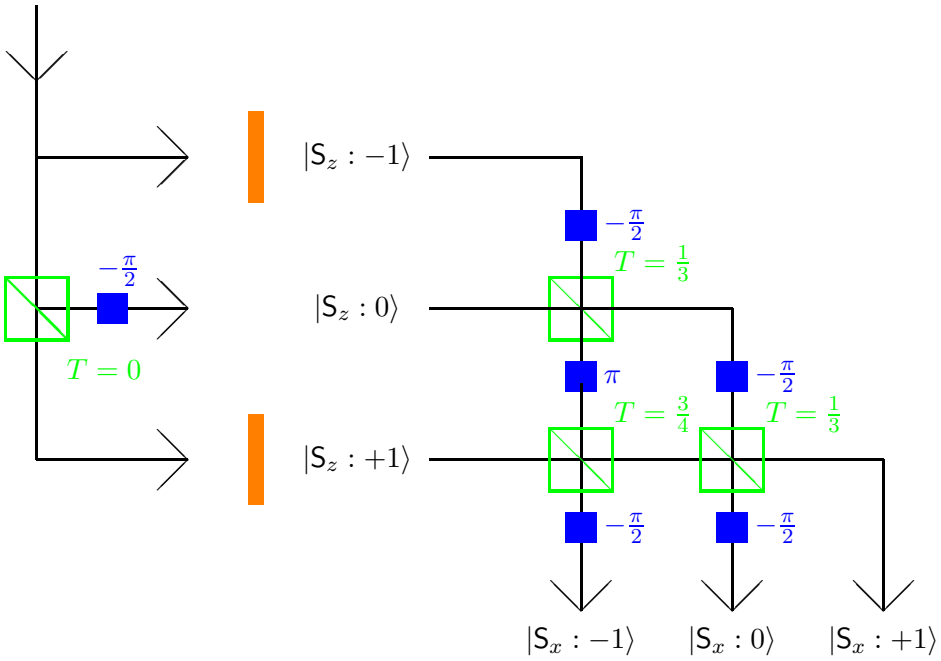

FIG. 6. (Color online) Configuration of a random number generator with a preparation and a measurement stage, including filters blocking $|\mathsf{S}_z:-1\rangle$ and $|\mathsf{S}_z:+1\rangle$. (For ideal beam-splitters, these filters would not be required.) The measurement stage (right array) realises 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 generalised beam-splitters..

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 $|a=\pm1\rangle$ (corresponding to output ports 1 and 3) which fall within the bounds $\sqrt{\frac{5}{14}} \leq \langle \mathsf{S}_z=0|a=\pm1\rangle \leq \frac{3}{\sqrt{14}}$ 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 quantised 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 [43], there is no further need of empirical evidence. In this line of thinking, Theorem 11, and hence the quantum value indefiniteness resulting from it via Corollary 12, 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 [23, 44]. Given the non-trivial assumptions used in the proof of Theorem 11—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 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.

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

Thirdly, in the case that our QRNG is treated as an untrusted-device, as is common in cryptography (due to the users 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[45] and thus gives some indication of non-classicality 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 non-classical outcomes typically encountered in empirical realisations of Greenberger-Horne-Zeilinger type arguments [46, 47], as, at least ideally, they do not involve any statistics, but require a violation of local realism at every triple of outcomes.

To summarise, we have presented a formal conceptualisation 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 one can be guaranteed to be, but how far does this value indefiniteness go? We conjecture that *only a single* observable in the Hilbert space can be assigned the value one.

ACKNOWLEDGEMENTS

We are grateful to Kohtaro Tadaki for insightful comments which improved the paper. We thank Michael Reck for the code producing the generalised 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. Calude's contribution was done in part during his tenure as Visiting Fellow of the Isaac Newton Institute for Mathematical Sciences (June–July 2012). Conder has been supported in part by a University of Auckland Summer Scholarship (2012). Svozil's contribution was done in part during his visiting honorary appointment at the University of Auckland (February–March 2012), and

a visiting professorship at the University of Cagliari (May–July 2012).

---

[1] Ernst Specker, "Die Logik nicht gleichzeitig entscheidbarer Aussagen," Dialectica **14**, 239–246 (1960), http://arxiv.org/abs/1103.4537.

[2] Simon Kochen and Ernst P. Specker, "The problem of hidden variables in quantum mechanics," Journal of Mathematics and Mechanics (now Indiana University Mathematics Journal) **17**, 59–87 (1967).

[3] Note that there exist models of complementarity such as automaton logic or generalised urn models which are value definite [48].

[4] In the Bell-type cases all observables, and in the Kochen-Specker case "many" observables.

[5] Observables are represented by circles, contexts by smooth line segments.

[6] J. R. Greechie, "Orthomodular lattices admitting no states," Journal of Combinatorial Theory **10**, 119–132 (1971).

[7] Pavel Pták and Sylvia Pulmannová, *Orthomodular Structures as Quantum Logics* (Kluwer Academic Publishers, Dordrecht, 1991).

[8] Karl Svozil and Josef Tkadlec, "Greechie diagrams, nonexistence of measures in quantum logics and Kochen–Specker type constructions," Journal of Mathematical Physics **37**, 5380–5401 (1996).

[9] Neal Zierler and Michael Schlessinger, "Boolean embeddings of orthomodular sets and quantum logic," Duke Mathematical Journal **32**, 251–262 (1965).

[10] Gudrun Kalmbach, *Measures and Hilbert Lattices* (World Scientific, Singapore, 1986).

[11] Václav Alda, "On 0-1 measures for projectors I," Aplikace matematiky (Applications of Mathematics) **25**, 373–374 (1980).

[12] Václav Alda, "On 0-1 measures for projectors II," Aplikace matematiky (Applications of Mathematics) **26**, 57–58 (1981).

[13] Franz Kamber, "Die Struktur des Aussagenkalküls in einer physikalischen Theorie," Nachrichten der Akademie der Wissenschaften in Göttingen, Mathematisch-Physikalische Klasse **10**, 103–124 (1964).

[14] Franz Kamber, "Zweiwertige Wahrscheinlichkeitsfunktionen auf orthokomplementären Verbänden," Mathematische Annalen **158**, 158–196 (1965).

[15] Avshalom C. Elitzur, Sandu Popescu, and Daniel Rohrlich, "Quantum nonlocality for each pair in an ensemble," Physics Letters A **162**, 25–28 (1992).

[16] Karl Svozil, "How much contextuality?" Natural Computing **11**, 261–265 (2012), arXiv:1103.3980.

[17] Ernst Specker, (1999), private communication to K. Svozil.

[18] John S. Bell, "On the problem of hidden variables in quantum mechanics," Reviews of Modern Physics **38**, 447–452 (1966).

[19] Albert Einstein, Boris Podolsky, and Nathan Rosen, "Can quantum-mechanical description of physical reality be considered complete?" Physical Review **47**, 777–780 (1935).

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

[21] Asher Peres, "Generalized Kochen-Specker theorem," Foundations of Physics **26**, 807–812 (1996), arXiv:quant-ph/9510018.

[22] Osung Kwon, Young-Wook Cho, and Yoon-Ho Kim, "Quantum random number generator using photon-number path entanglement," Applied Optics **48**, 1774–1778 (2009).

[23] 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, "Random numbers certified by Bell's theorem," Nature **464**, 1021–1024 (2010).

[24] André Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden, "Optical quantum random number generator," Journal of Modern Optics **47**, 595–598 (2000).

[25] Karl Svozil, "Three criteria for quantum random-number generators based on beam splitters," Physical Review A **79**, 054306 (2009), arXiv:quant-ph/0903.2744.

[26] Michael A. Wayne, Evan R. Jeffrey, Gleb M. Akselrod, and Paul G. Kwiat, "Photon arrival time quantum random number generation," Journal of Modern Optics **56**, 516–516 (2009).

[27] M. Stipčević and B. Medved Rogina, "Quantum random number generator based on photonic emission in semiconductors," Review of Scientific Instruments **78**, 045104 (2007).

[28] Hai-Qiang Ma, Yuejian Xie, and Ling-An Wu, "Random number generation based on the time of arrival of single photons," Applied Optics **44**, 7760–7763 (2005).

[29] Cristian Calude, *Information and Randomness—An Algorithmic Perspective*, 2nd ed. (Springer, Berlin, 2002).

[30] Émile Borel, "Les probabilités dénombrables et leurs applications arithmétiques," Rendiconti del Circolo Matematico di Palermo (1884 - 1940) **27**, 247–271 (1909).

[31] Alastair A. Abbott and Cristian S. Calude, CDMTCS-392.

[32] Zeeya Merali, "A truth test for randomness," Nature News (2010), 10.1038/news.2010.181, published online. URL: http://dx.doi.org/10.1038/news.2010.181.

[33] ID Quantique SA, *QUANTIS. Quantum number generator* (idQuantique, Geneva, Switzerland, 2001-2009).

[34] ANU Quantum Optics, *ANU. Quantum random number generator* (ANU Quantum Optics, Australian National University, 2012) uRL `http://photonics.anu.edu.au/qoptics/Research/qrng.php` accessed on July 9th, 2012.

[35] Cristian S. Calude and Karl Svozil, "Quantum randomness and value indefiniteness," Advanced Science Letters **1**, 165–168 (2008), eprint arXiv:quant-ph/0611029, arXiv:quant-ph/0611029.

[36] M. Reck, Anton Zeilinger, H. J. Bernstein, and P. Bertani, "Experimental realization of any discrete unitary operator," Physical Review Letters **73**, 58–61 (1994).

[37] Marek Zukowski, Anton Zeilinger, and Michael A. Horne, "Realizable higher-dimensional two-particle entanglements via multiport beam splitters," Physical Review A **55**, 2564–2579 (1997).

[38] Karl Svozil, "Noncontextuality in multipartite entanglement," J. Phys. A: Math. Gen. **38**, 5781–5798 (2005), quant-ph/0401113.

[39] F. D. Murnaghan, *The Unitary and Rotation Groups* (Spartan Books, Washington, D.C., 1962).

[40] A. Zeilinger, "General properties of lossless beam splitters in interferometry," American Journal of Physics **49**, 882–883 (1981).

[41] R. A. Campos, B. E. A. Saleh, and M. C. Teich, "Quantum-mechanical lossless beam splitter: $SU(2)$ symmetry and photon statistics," Physical Review A **40**, 1371–1384 (1989).

[42] Daniel M. Greenberger, Mike A. Horne, and Anton Zeilinger, "Multiparticle interferometry and the superposition principle," Physics Today **46**, 22–29 (1993).

[43] John von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, NJ, 1955).

[44] Umesh Vazirani and Thomas Vidick, "Certifiable quantum dice," Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences **370**, 3432–3448 (2012), arXiv:1111.6054.

[45] Such violations are often referred to as "proofs of the Kochen-Specker theorem," or "proofs of quantum contextuality" [49–53].

[46] Dik Bouwmeester, Jian-Wei Pan, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger, "Observation of three-photon greenberger-horne-zeilinger entanglement," Physical Review Letters **82**, 1345–1349 (1999).

[47] Jian-Wei Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger, "Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement," Nature **403**, 515–519 (2000).

[48] Karl Svozil, "Logical equivalence between generalized urn models and finite automata," International Journal of Theoretical Physics **44**, 745–754 (2005), quant-ph/0209136.

[49] Yuji Hasegawa, Rudolf Loidl, Gerald Badurek, Matthias Baron, and Helmut Rauch, "Quantum contextuality in a single-neutron optical experiment," Physical Review Letters **97**, 230401 (2006).

[50] H. Bartosik, J. Klepp, C. Schmitzer, S. Sponar, A. Cabello, H. Rauch, and Y. Hasegawa, "Experimental test of quantum contextuality in neutron interferometry," Physical Review Letters **103**, 040403 (2009), arXiv:0904.4576.

[51] G. Kirchmair, F. Zähringer, R. Gerritsma, M. Kleinmann, O. Gühne, A. Cabello, R. Blatt, and C. F. Roos, "State-independent experimental test of quantum contextuality," Nature **460**, 494–497 (2009), arXiv:0904.1655.

[52] Elias Amselem, Magnus Rådmark, Mohamed Bourennane, and Adán Cabello, "State-independent quantum contextuality with single photons," Physical Review Letters **103**, 160405 (2009).

[53] Radek Lapkiewicz, Peizhe Li, Christoph Schaeff, Nathan K. Langford, Sven Ramelow, Marcin Wieśniak, and Anton Zeilinger, "Experimental non-classicality of an indivisible quantum system," Nature **474**, 490–493 (2011).