Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

# A new quantum random number generator certified by value indefiniteness

José Manuel Agüero Trejo, Cristian S. Calude *

*School of Computer Science, University of Auckland, New Zealand*

ARTICLE INFO

*Article history:*
Received 12 June 2020
Received in revised form 12 August 2020
Accepted 13 August 2020
Available online xxxx

*Keywords:*
Quantum random number generator
Bi-immunity
Unpredictability
Normality

ABSTRACT

In this paper we propose a new ternary QRNG based on measuring located value indefinite observables with probabilities $1/4, 1/2, 1/4$ and prove that every sequence generated is maximally unpredictable, 3-bi-immune (a stronger form of bi-immunity), and its prefixes are Borel normal. The ternary quantum random digits produced by the QRNG are algorithmically transformed into quantum random bits using an alphabetic morphism which preserves all the above properties.

© 2020 Elsevier B.V. All rights reserved.

## 1. Introduction

Randomness is an important resource in science, statistics, cryptography, gambling, medicine, art and politics. Pseudo-random number generators (PRNGs) – computer algorithms designed to simulate randomness – have been the main, if not the only, sources of randomness for a long time, but their quality is weak. As early as 1951 von Neumann realised the danger of mistakenly believing that PRNGs produce "true" randomness [42]: "Anyone who attempts to generate random numbers by deterministic means is, of course, living in a state of sin." Problems with the poor quality PRNGs are well known: a classical example is the discovery in 2012 of a weakness in a worldwide-used encryption system which was traced to a PRNG [32].

With the development of algorithmic information theory [23,33,25] various classes of (algorithmic) random strings/sequences have been studied and von Neumann intuition was rigorously proved in a more general form: *mathematically there is no 'true" random string/sequence* [19].

The importance of high quality randomness – which is obvious in cryptography, where good randomness is vital to the security of data and communication, but is equally true in other areas ranging from statistics and information science to medicine, physics, politics and religion – has driven a recent surge of interest in developing "better than PRNG" random number generators, in particular, quantum random number generators (QRNGs) [22,28]. QRNGs are generally considered to be, by their very nature, "better than PRNGs" and are expected to "excel" precisely on properties of randomness where algorithmic PRNGs obviously fail: incomputability and inherent unpredictability. The formulation *"better than PRNGs"* can be read into two radically different ways: a) "better" than *some* PRNGs, b) "better" than *any* PRNGs. Of course, b) is the required property.

* Corresponding author.
*E-mail address:* cristian@cs.auckland.ac.nz (C.S. Calude).

https://doi.org/10.1016/j.tcs.2020.08.014
0304-3975/© 2020 Elsevier B.V. All rights reserved.

Please cite this article in press as: J.M. Agüero Trejo, C.S. Calude, A new quantum random number generator certified by value indefiniteness, Theoret. Comput. Sci. (2020), https://doi.org/10.1016/j.tcs.2020.08.014

To date only one class of QRNGs has been proved to satisfy b) [6,8,30]. This type of QRNG is based on a located form [3,5,9,10] of the Kochen-Specker Theorem [29], a result true only in Hilbert spaces of dimension *at least three*. These QRNGs – which locate and repeatedly measure a value-indefinite quantum observable – produce more than incomputable sequences (over alphabets with at least three letters); more precisely, they generate sequences having a form of algorithmic randomness called *bi-immunity* [25], that is, sequences for which no algorithm can compute more than finitely many exact values. The experimental analysis of 10 samples of $2^{30}$ binary strings generated with the implementation [30] of the QRNG proposed in [6,8] showed incomputability in a weak and not decisive manner. Some possible reasons include a problematic branch with probability zero used in the generalised beam splitter – recall, the Kochen-Specker Theorem is false in dimension 2 –, the not long enough length of samples, and, of course, imperfections in the implementation of the measuring protocol [2].

In this paper we improve the QRNG [6,8,30] and propose a new ternary QRNG based on measuring located value indefinite observables with probabilities $1/4, 1/2, 1/4$. *We prove that every sequence generated is maximally unpredictable, 3-bi-immune, and its prefixes are Borel normal.* The ternary quantum random digits produced by the QRNG are algorithmically transformed into quantum random bits using an alphabetic morphism which preserves all the above properties.

The paper is organised as follows. Section 2 includes the notation and main definitions. In Section 3 we present the main theoretical basis of the QRNG: localising value indefinite observables, and their unpredictability. Section 4 is devoted to the blueprint of the original QRNG based on Spin-1; in Section 5 we present the new QRNG. In Section 6 we prove the main properties of ternary sequences produced by the QRNG and in Section 7 we introduce the transformation from ternary to binary and prove that it preserves all properties proved in the previous section. The last section includes a summary and further questions.

## 2. Notation and definitions

The set of positive integers will be denoted by $\mathbb{N}$. Consider the alphabet $A_b = \{0, 1, \ldots, b-1\}$, where $b \geq 2$ is an integer; the elements of $A_b$ are to be considered the digits used in natural positional representations of numbers in the interval $[0, 1)$ at base $b$. By $A_b^*$ and $A_b^\omega$ we denote the sets of (finite) strings and (infinite) sequences over the alphabet $A_b$. Strings will be denoted by $x, y, u, w$; the length of the string $x = x_1x_2\ldots x_m$, $x_i \in A_b$, is denoted by $|x|_b = m$ (the subscript $b$ will be omitted if it is clear from the context); $A_b^m$ is the set of all strings of length $m$. Sequences will be denoted by $\mathbf{x} = x_1x_2\ldots$; the prefix of length $m$ of $\mathbf{x}$ is the string $\mathbf{x}(m) = x_1x_2\ldots x_m$. Strings will be ordered quasi-lexicographically according to the natural order $0 < 1 < 2 < \cdots < b-1$ on the alphabet $A_b$. For example, for $b = 2$, we have $0 < 1 < 00 < 01 < 10 < 11 < 000\ldots$. We assume knowledge of elementary computability theory over different size alphabets [19]. Sequences can be also viewed as $A_b$-valued functions defined on $\mathbb{N}$.

Let $\mathcal{B}(\mathbb{R})$ be the class of Borel sets in $\mathbb{R}$, that is, the smallest $\sigma$-algebra containing all opens sets. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space. A random variable $X : \Omega \to \mathbb{R}$ is a function such that for every $B \in \mathcal{B}(\mathbb{R})$ we have $\{w \in \Omega : X(w) \in B\} \in \mathcal{F}$. Furthermore, if for all $x, y \in \mathbb{R}$, $\mathbb{P}(X \leq x, Y \leq y) = \mathbb{P}(X \leq x)\mathbb{P}(Y \leq y)$, we say that $X, Y$ are independent random variables. By $\mathbb{E}(X) = \sum_x x\mathbb{P}(X = x)$ we denote the expectation of the random variable $X$ [14]. Let $u \in A_b^*$, $uA_b^\omega = \{\mathbf{x} \in A_b^\omega : \mathbf{x}(|u|) = u\}$ and consider the smallest $\sigma$-algebra $\mathcal{B}(A_b^\omega)$ generated by the family $(uA_b^\omega : u \in A_b^*)$. The *Lebesgue space (probability)* is the probability space $(A_b^\omega, \mathcal{B}(A_2^\omega), \mathbb{P})$ where $\mathbb{P}(uA_b^\omega) = b^{-|u|}$ [19].

In contrast to the bounds on probability distributions given by Bell Theorem [11,12] under the premise of locality, Kochen-Specker Theorem shows that, assuming non-contextuality,[1] the Hilbert-space structure of quantum mechanics makes it impossible to assign "classical" definite values to all possible quantum observables in a consistent manner. Since such a definite value is precisely a (deterministic) hidden variable specifying, in advance, the result of a measurement of an observable, the theorem shows that the outcomes of all quantum measurements on a system cannot be simultaneously pre-determined.

As is common in modern treatments of the Kochen-Specker Theorem [16,17,37] we focus on one-dimensional (rank-1) projection observables, and we denote the observable projecting onto the linear subspace spanned by a vector $|\psi\rangle$ as $P_\psi = \frac{|\psi\rangle\langle\psi|}{|\langle\psi|\psi\rangle|}$. We then fix a positive integer $n \geq 2$ and let $O \subseteq \{P_\psi : |\psi\rangle \in \mathbb{C}^n\}$ be a non-empty set of one-dimensional projection observables on the Hilbert space $\mathbb{C}^n$.

**Definition 1.** A set $C \subset O$ is a *context* of $O$ if $C$ has $n$ elements (i.e. $|C| = n$) and for all $P_\psi, P_\phi \in C$ with $P_\psi \neq P_\phi$, $\langle\psi|\phi\rangle = O$.

**Definition 2.** A *value assignment function* (on $O$) is a partial function $v : O \to \{0, 1\}$ assigning values to some (possibly all) observables in $O$. The partiality of the function $v$ means that $v(P)$ can be $0, 1$ or indefinite.

**Definition 3.** An observable $P \in O$ is *value definite* (under the assignment function $v$) if $v(P)$ is defined, i.e. it is 0 or 1; otherwise, it is *value indefinite* (under $v$). Similarly, we call $O$ *value definite* (under $v$) if every observable $P \in O$ is value definite.

[1] Informally, the property that the outcome of the measurement of a quantum observable is independent of how that value is eventually measured.

Please cite this article in press as: J.M. Agüero Trejo, C.S. Calude, A new quantum random number generator certified by value indefiniteness, Theoret. Comput. Sci. (2020), https://doi.org/10.1016/j.tcs.2020.08.014

## 3. Theoretical basis

In this section we present the main theoretical basis of the QRNG.

### 3.1. Localising value indefiniteness

Consider the following Kochen-Specker assumptions:

- **Admissibility:** Let $O$ be a set of one-dimensional projection observables on $\mathbb{C}^n$ and let $v : O \to \{0, 1\}$ be a value assignment function. Then $v$ is *admissible*[2] if for every context $C$ of $O$, we have that $\sum_{P \in C} v(P) = 1$, i.e. only one projection observable in a context can be assigned the value 1.
- **Non-contextuality of definite values**: The outcome obtained by measuring a value definite observable (a pre-existing physical property) is *non-contextual*, i.e. it does not depend on other compatible observables which may be measured alongside it.

The fundamental result is:

**Theorem 1** *(Kochen-Specker [29]). Let $n \geq 3$. Then there exists a (finite) set of one-dimensional projection observables $O$ on the Hilbert space $\mathbb{C}^n$ such that there is no value assignment function $v$ satisfying the following three conditions: i) $O$ is value definite under $v$, ii) $v$ is admissible, iii) $v$ is non-contextual.*

Kochen-Specker Theorem shows that, in agreement with quantum mechanics, not every observable can be both non-contextual and value definite, but it does not describe the extent of this incompatibility. In fact, it has been shown that for any sets 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. That is, the incompatibility between the Kochen-Specker assumptions is not maximal, hence not all observables need to be value indefinite.

Why are value indefinite observables important? One reason is that *measuring one such observable may produce a random outcome*. But, to measure a value indefinite observable we have to "effectively find" one, not just know that such an observable exists as Kochen-Specker Theorem assures. Essentially, to answer the above question in the affirmative, we need a constructive form of the Kochen-Specker Theorem allowing to localise a value indefiniteness observable. Motivated by Einstein, Podolsky and Rosen definition of *physical reality* [26, p. 777]:

> If, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists a *definite value* prior to observation corresponding to this physical quantity.

we make the following assumption:

- **Eigenstate principle**: If a quantum system is prepared in the state $|\psi\rangle$, then the projection observable $P_\psi$ is value definite.

In detail, if a quantum system is prepared in an arbitrary state $|\psi\rangle \in \mathbb{C}^n$, then the measurement of the observable $P_\psi$ should yield the outcome 1, hence, if $P_\psi \in O$, then $v(P_\psi) = 1$.

**Theorem 2** *(Localised Kochen-Specker [3,7,10]). Assume a quantum system prepared in the state $|\psi\rangle$ in a dimension $n \geq 3$ Hilbert space $\mathbf{C}^n$, and let $|\phi\rangle$ be any state neither orthogonal nor parallel to $|\psi\rangle$ ($0 < |\langle\psi|\phi\rangle| < 1$). If the following three conditions are satisfied: i) admissibility, ii) non-contextuality and iii) eigenstate principle, then the projection observable $P_\psi$ is value indefinite.*

From Theorem 2 we deduce that, given a system prepared in state $|\psi\rangle$, a one-dimensional projection observable can only be value definite if it is an eigenstate of that observable. Furthermore, for any diagonalisable observable $O$ with spectral decomposition $O = \sum_{i=1}^{n} \lambda_i P_{\lambda_i}$, where $\lambda_i$ denotes each distinct eigenvalue with corresponding eigenstate $|\lambda_i\rangle$, $O$ has a predetermined measurement outcome if and only if each projector in its spectral decomposition has a predetermined measurement outcome. Thus, we can generalise our previous result to the outcome of the measurement of an observable with non-degenerate spectra. Such generalisation is of particular importance for applying this result to elements of physical reality where a measurement is assumed to yield a meaningful result that describes a physical attribute; thus, utilising the value assignment function to represent the realisation of a given state whenever the corresponding observable is value definite. The latter can be observed as follows.

Let $C = \{P_1, \ldots, P_n\}$ be a context of projection observables and let $v$ be a value assignment function such that $v(P_1) = 1$ under $C$. Since a context is a maximal set of compatible projection observables it follows that, if any pair $(P_1, P_i)$ is

[2] In agreement with quantum mechanics predictions.

Please cite this article in press as: J.M. Agüero Trejo, C.S. Calude, A new quantum random number generator certified by value indefiniteness, Theoret. Comput. Sci. (2020), https://doi.org/10.1016/j.tcs.2020.08.014

measured, then the system will collapse into the eigenstate $|\phi\rangle$ of the projection observable $P_1$ with eigenvalue 1. It follows that, as all observables in $C$ are physically co-measurable and $\sum_{j=1}^{n} P_j = 1$, we deduce that $|\phi\rangle$ is an eigenstate of $P_i$ with corresponding eigenvalue 0; that is, $v(P_i) = 0$. Similarly, if $v(P_i) = 0$ for $i \neq 1$, then $v(P_1) = 1$. Hence, the admissibility of $v$ serves as a generalisation of the sum rule that corresponds to the physical interpretation of the measurement process.

Finally, we can answer the question 'how "large" or "typical" is the set of value indefinite observables?'

**Theorem 3** *([7]). The set of value indefinite observables has constructive Lebesgue measure one, that is, almost all observables are value indefinite.*

Theorem 2 paved the way to construct a class of QRNGs based on measuring value indefinite observables. How "good" is such a QRNG? The answer will use the following

- **epr principle**: If a repetition of measurements of an observable generates a computable sequence, then these observables are value definite.

Assume the Eigenstate and epr principles. An infinite repetition of the experiment measuring a quantum value indefinite observable always generates an incomputable infinite sequence $x_1 x_2 \ldots$. In fact, a stronger result is true as we will show in Section 6.1. Informally, a sequence $\mathbf{x}$ is bi-immune if no algorithm can generate infinitely many correct values of its elements (pairs, $(i, x_i)$). The formal definition is as follows. A sequence $\mathbf{x} \in A_b^\omega$ $(b \geq 2)$ is *bi-immune* if there is no partially computable function $\varphi$ from $\mathbb{N}$ to $A_b$ having an infinite domain $\mathrm{dom}(\varphi)$ with the property that $\varphi(i) = x_i$ for all $i \in \mathrm{dom}(\varphi)$ [13]). In the binary case we have:

**Theorem 4** *([3]). Assume the Eigenstate and epr principles. An infinite repetition of the experiment measuring a quantum value indefinite observable in $\mathbb{C}^2$ always generates a bi-immune sequence $\mathbf{x} \in A_2^\omega$.*

### 3.2. Value definiteness and unpredictability

Since probability spaces lie at the core of quantum mechanics, we can describe quantum behaviour in different contexts by utilising the probabilistic framework that the theoretical notion of the wave function characterisation provides; here, physical attributes correspond to projection operators and their corresponding eigenvalues. However, the use of the *eigenstate assumption* is restricted to contexts that contain the observable $P_\psi$, where $|\psi\rangle$ is the state in which the system was prepared. For this reason, formalising the notion of predictability with respect to the value that corresponds to a given observable is required.

Consider a system that continuously repeats the process of state preparation and measurement, as in [3]. Let $\mathbf{x} = x_1 x_2 \ldots$ denote the infinite sequence produced by concatenating the outputs of the measurement performed at each iteration. Let $\mathcal{O}, \mathcal{C}$ be a fixed set of observables and contexts, respectively, with $O_i, C_i$ denoting the observable and the corresponding context for the $i$-th measurement. We say that a measurement outcome is predictable if there exists a *computable function* $f : \mathbb{N} \times \mathcal{O} \times \mathcal{C} \to \{0, 1\}$ such that, for every iteration $i$ we have that $f(i, O_i, C_i) = x_i$. Note that if every value of a sequence of measurement results is predictable, then the computability of $f$ ensures that there is some function that outputs the values $x_i$ of $\mathbf{x}$ corresponding to each iteration. However, an incomputable $f$ provides no way of obtaining each term of the sequence and therefore offers no method of prediction [40]. Finally, following [3], if such function exists, we assume there is a definite value associated with the sequence of observables used for computing each term of the function output; that is $f(i, O_i, C_i) = v_i(O_i, C_i)$.

Theorem 4 proves this form of unpredictability, but leaves the possibility of finitely many exceptions. An even stronger result, which removes this possibility, was obtained by using a non-probabilistic model for unpredictability [8,9]. To this aim we consider an *experiment* $E$ producing a single bit $x \in \{0, 1\}$; with a particular trial of $E$ we associate the parameter $\lambda$ (the state of the universe) which fully describes the trial; $\lambda$ can be viewed as a resource from which one can extract finite information from in order to predict the outcome of the experiment $E$. The trials of $E$ generate a succession of events of the form "$E$ is prepared, performed, the result recorded, $E$ is reset", iterated finitely many times in an algorithmic fashion.

An *extractor* is a physical device selecting a finite amount of information from $\lambda$ without altering the experiment $E$; it produces a finite string of bits $\langle\lambda\rangle$. A *predictor* for $E$ is an algorithm $P_E$ which *halts* on every input and *produces* **0** or **1** or **prediction withheld**. The predictor $P_E$ can use as input the information $\langle\lambda\rangle$, but must be *passive,* that is, it must not disturb or interact with $E$ in any way.

A predictor $P_E$ provides a *correct prediction* using the extractor $\langle\,\rangle$ for an instantiation of $E$ with parameter $\lambda$ if, when taking as input $\langle\lambda\rangle$, it outputs 0 or 1 (i.e. it does not refrain from making a prediction) and the output is equal to $x$, the result of the experiment. Fix an extractor $\langle\,\rangle$; the predictor $P_E$ is $k, \langle\,\rangle$-*correct* if there exists an $n \geq k$ such that when $E$ is repeated $n$ times with associated parameters $\lambda_1, \ldots, \lambda_n$ producing the outputs $x_1, x_2, \ldots, x_n$, $P_E$ outputs the sequence $P_E(\langle\lambda_1\rangle), P_E(\langle\lambda_2\rangle), \ldots, P_E(\langle\lambda_n\rangle)$ with the following two properties: (i) no prediction in the sequence is incorrect, and (ii) in the sequence there are $k$ correct predictions. The confidence we have in a $k, \langle\,\rangle$-correct predictor increases as $k \to \infty$. If $P_E$ is $k, \langle\,\rangle$-correct for all $k$, then $P_E$ never makes an incorrect prediction and the number of correct predictions can be made arbitrarily large by repeating $E$ enough times.

Please cite this article in press as: J.M. Agüero Trejo, C.S. Calude, A new quantum random number generator certified by value indefiniteness, Theoret. Comput. Sci. (2020), https://doi.org/10.1016/j.tcs.2020.08.014

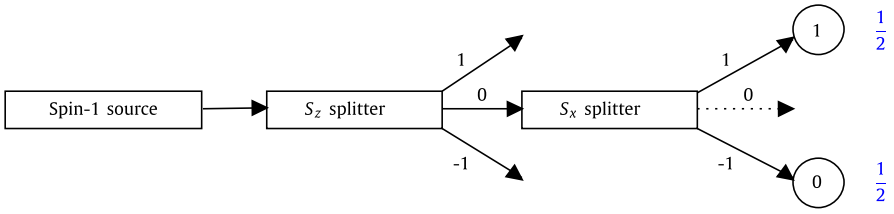


**Fig. 1.** QRNG setup proposed in [3]; the values $\frac{1}{2}, \frac{1}{2}$ (in blue) correspond to the outcome probabilities. (For interpretation of the colours in the figure(s), the reader is referred to the web version of this article.)

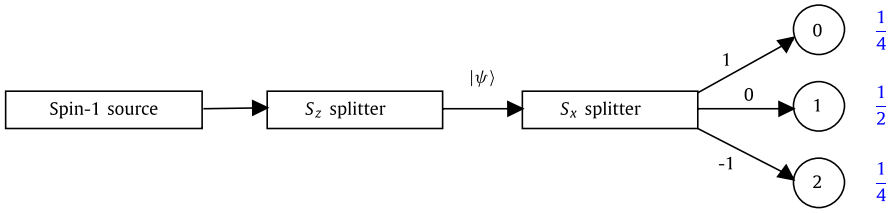


**Fig. 2.** Blueprint for a new QRNG; the values $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$ (in blue) correspond to the outcome probabilities of setups prepared in the state $|\psi\rangle = |\pm 1\rangle$.

If $P_E$ is not $k, \langle\rangle$-correct for all $k$, then we cannot exclude the possibility that any correct prediction $P_E$ makes is simply due to chance. Hence, we say that the outcome $x$ of a single trial of the experiment $E$ performed with parameter $\lambda$ is *predictable* (with certainty) if there exist an extractor $\langle\rangle$ and a predictor $P_E$ which is $k, \langle\rangle$-correct for all $k$, and $P_E(\langle\lambda\rangle) = x$.

Consider an experiment $E$ performed in dimension $n \geq 3$ Hilbert space in which a quantum system is prepared in a state $|\psi\rangle$ and a value indefinite observable $P_\phi$ is measured producing a single bit $x$.

**Theorem 5** *([8,9]). Assume the epr and Eigenstate principles. Let* $\mathbf{x}$ *be an infinite sequence obtained by measuring a quantum value indefinite observable in* $\mathbb{C}^2$ *in an infinite repetition of the experiment E. Then no single bit* $x_i$ *can be predicted.*

## 4. A QNRG based on localised value indefiniteness

A blueprint for a QRNG based on Theorem 2 was proposed in [3] using a generalised beam splitter and a physical realisation with superconducting transmon qutrits was given in [30]. As Theorems 1 and 2 are true *only* in Hilbert spaces of dimension $n \geq 3$, any QRNG based on them produces sequences over alphabets with at least three elements. As a consequence, a QRNG using the classical beam splitter is not certified by these theorems.

*The QRNG operates in a succession of events of the form "preparation, measurement, reset", iterated indefinitely many times in an algorithmic fashion*, [3]. Let $\mathbf{x} = x_1 x_2 \ldots$ denote the infinite sequence produced by concatenating the consecutive outputs of infinitely many events as described above.

From Theorem 2 a system prepared on an arbitrary state $|\psi\rangle$ must have a definite value associated to the operator $P_\psi$. Hence, for spin-1 particles prepared in the state $S_z = 0$, this operator is value definite. As the possible outcomes of an observable $O$ correspond to the eigenvalues $o$ of the projectors that describe the spectral decomposition $O = \sum_o o P_o$, we deduce that the state $|S_z = 0\rangle$ is an eigenstate of the projector $S_x = 0$, i.e. $|0\rangle\langle 0|$, with eigenvalue 0; so, the probability of obtaining this outcome is 0. For this reason, $S_x = \pm 1$ are the only results we need to consider for now. Furthermore, we have that $\langle S_z | S_x \rangle = \langle 0 | \pm 1 \rangle = \frac{1}{\sqrt{2}}$; so, by the previous results, it is not possible to assign a definite value to $S_x = \pm 1$.

To date, *this QRNG is the only example of a random generator provably better than any PRNG.*

An experimental study [4] of the realisation [30] of this QRNG has used various tests to compare it with arguably the best PRNGs. While the analysis failed to observe a strong advantage of the quantum random sequences due to incomputability, the results are informative: some of the test results are ambiguous and require further study, others highlight difficulties that can guide the development of future tests of algorithmic randomness and incomputability, and, more importantly, ideas for improvement of the design of QRNG based on Theorem 2 have emerged. One such idea, developed in the following section, is to eliminate the problematic branch $S_x = 0$ in Fig. 1 which has probability zero. Why problematic? In standard measure-theoretic formulation of probability [27] it is possible for a non-empty event to have probability zero, hence, events of probability zero are not necessarily impossible.

## 5. A new QRNG based on localised value indefiniteness

To address the above problem we propose a new QRNG setup, based on the blueprint, with a different state preparation, see Fig. 2.

Please cite this article in press as: J.M. Agüero Trejo, C.S. Calude, A new quantum random number generator certified by value indefiniteness, Theoret. Comput. Sci. (2020), https://doi.org/10.1016/j.tcs.2020.08.014

### 5.1. A generalised spin observable

The property *spin* (**S**) is the intrinsic angular momentum characteristic of elementary particles. By deriving the spin state operator $S_x$ we can control the effect of the preparation state $|S_z\rangle$ on the outcome probabilities. We refer to the eigenvalue $s$ of $\mathbf{S}^2$ as the spin (quantum) number [36,41]. For a spin-1 particle, the eigenvalues of $S_z$ are $1, 0, -1$, thus introducing an orthonormal Cartesian standard basis $\{|1\rangle, |0\rangle, |-1\rangle\}$ defined by $S_z|m\rangle = \hbar m|m\rangle$ it follows that

$$S_z = \hbar \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

From $S_\pm|m\rangle = \sqrt{s(s+1) - m(m\pm 1)}\,|m\pm 1\rangle$ we obtain the raising and lowering operators for $s = 1$

$$S_+|m\rangle = \hbar\sqrt{2 - m(m+1)}\,|m+1\rangle,$$

$$S_-|m\rangle = \hbar\sqrt{2 - m(m-1)}\,|m-1\rangle.$$

Consequently, we have

$$S_+ = \begin{pmatrix} \langle 1|S_+|1\rangle & \langle 1|S_+|0\rangle & \langle 1|S_+|-1\rangle \\ \langle 0|S_+|1\rangle & \langle 0|S_+|0\rangle & \langle 0|S_+|-1\rangle \\ \langle -1|S_+|1\rangle & \langle -1|S_+|0\rangle & \langle -1|S_+|-1\rangle \end{pmatrix} = \sqrt{2}\hbar \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

$$S_- = \begin{pmatrix} \langle 1|S_-|1\rangle & \langle 1|S_-|0\rangle & \langle 1|S_-|-1\rangle \\ \langle 0|S_-|1\rangle & \langle 0|S_-|0\rangle & \langle 0|S_-|-1\rangle \\ \langle -1|S_-|1\rangle & \langle -1|S_-|0\rangle & \langle -1|S_-|-1\rangle \end{pmatrix} = \sqrt{2}\hbar \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Furthermore, since $S_\pm = S_x \pm iSy$, we get $S_x = \frac{1}{2}(S_+ + S_-)$ and $S_y = \frac{1}{2i}(S_- - S_+)$, it follows that

$$S_x = \frac{1}{\sqrt{2}}\hbar \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},\ S_y = \frac{1}{\sqrt{2}}\hbar \begin{pmatrix} 0 & -i & 0 \\ i & 0 & -i \\ 0 & i & 0 \end{pmatrix}.$$

Thus, the generalised Pauli matrices for a spin-1 particle are given by $\mathbf{S} = (S_x, S_y, S_z) = \hbar\boldsymbol{\sigma}$:

$$\sigma_x = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},\ \sigma_y = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & -i & 0 \\ i & 0 & -i \\ 0 & i & 0 \end{pmatrix},\ \sigma_z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

We can now consider the description of spin states that point in arbitrary directions specified by the unit vector $\mathbf{u} = (u_x, u_y, u_z) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$, where $\theta, \phi$ are the polar and azimuthal angles; we then define the spin observable operator **S** as a triplet of operators $\mathbf{S} = (S_x, S_y, S_z) = \hbar\boldsymbol{\sigma}$. Then, by adopting units in which $\hbar$ is numerically equal to unity, in order to reduce the amount of numerical clutter, we obtain the generalised spin observable operator that describes the measurement context:

$$S(\theta,\phi) = \mathbf{u}\cdot\mathbf{S} = \begin{pmatrix} u_z & \frac{u_x - iu_y}{\sqrt{2}} & 0 \\ \frac{u_x + iu_y}{\sqrt{2}} & 0 & \frac{u_x - iu_y}{\sqrt{2}} \\ 0 & \frac{u_x + iu_y}{\sqrt{2}} & -u_z \end{pmatrix},$$

that is,

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

Note that $S_z$ is given by $S(0,0)$ and $S_x$ by $S(\frac{\pi}{2}, 0)$.

Please cite this article in press as: J.M. Agüero Trejo, C.S. Calude, A new quantum random number generator certified by value indefiniteness, Theoret. Comput. Sci. (2020), https://doi.org/10.1016/j.tcs.2020.08.014

### 5.2. State preparation and outcome probabilities

By considering the orthonormal Cartesian standard basis $|1\rangle = (1,0,0)$, $|0\rangle = (0,1,0)$ and $|-1\rangle = (0,0,1)$ we can obtain the eigenvalues $\{-1,0,1\}$ of $S_x$ by solving the equation

$$det(S_x - I\lambda) = \begin{vmatrix} -\lambda & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & -\lambda & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\lambda \end{vmatrix} = 0,$$

that is, $-\lambda(\lambda^2 - \frac{1}{2}) + \frac{1}{2}\lambda = 0$. Consequently we have:

$$\begin{aligned} &S_x|S_x:1\rangle = |S_x:1\rangle \implies |S_x:+1\rangle = \tfrac{1}{2}(1,\sqrt{2},1), \\ &S_x|S_x:0\rangle = 0 \implies |S_x:0\rangle = \tfrac{1}{\sqrt{2}}(1,0,-1), \\ &S_x|S_x:-1\rangle = -|S_x:-1\rangle \implies |S_x:+1\rangle = \tfrac{1}{2}(1,-\sqrt{2},1). \end{aligned}$$

We are now able to form the unitary matrix $U_x$ corresponding to the spin state operator $S_x$

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

The fact that $U_x$ can be decomposed into two-dimensional transformations [24] enables the physical realisation of the unitary operator by a lossless beam splitter [38,43] leading to the implementation of a QRNG, as in [30], with the new outcome probabilities. For simplicity we adopt the following convention:

$$\begin{aligned} &|1_x\rangle = |S_x:+1\rangle = \tfrac{1}{2}|1\rangle + \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{2}|-1\rangle, \\ &|0_x\rangle = |S_x:0\rangle = \tfrac{1}{\sqrt{2}}|1\rangle - \tfrac{1}{\sqrt{2}}|-1\rangle, \\ &|-1_x\rangle = |S_x:+1\rangle = \tfrac{1}{2}|1\rangle - \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{2}|-1\rangle. \end{aligned}$$

Consider the probability distribution $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$. We can identify a possible corresponding state preparation $|\psi\rangle$ by solving the following system of equations:

$$\begin{aligned} &|\tfrac{1}{2}x + \tfrac{1}{\sqrt{2}}y + \tfrac{1}{2}z| = \tfrac{1}{2}, \\ &|\tfrac{1}{\sqrt{2}}x - \tfrac{1}{\sqrt{2}}z| = \tfrac{1}{\sqrt{2}}, \\ &|\tfrac{1}{2}x - \tfrac{1}{\sqrt{2}}y + \tfrac{1}{2}z| = \tfrac{1}{2}, \end{aligned}$$

where $x = \langle 1|\psi\rangle$, $y = \langle 0|\psi\rangle$, $z = \langle -1|\psi\rangle$. Setting $y = 0, z = 1 - x$ satisfies such constrains and provides $|1\rangle, |-1\rangle$ and $\frac{|+\rangle - |-\rangle}{\sqrt{2}}$ as preparation state candidates. Since $|1\rangle$ and $|-1\rangle$ are eigenstates of $S_z$ they represent a natural choice for our QRNG construction. We ensure the validity of these states by first noting that

$$\begin{aligned} &\langle 1_x|1\rangle = \tfrac{1}{2}, \ \langle 1_x|-1\rangle = \tfrac{1}{2}, \\ &\langle 0_x|1\rangle = \tfrac{1}{\sqrt{2}}, \ \langle 0_x|-1\rangle = \tfrac{-1}{\sqrt{2}}, \\ &\langle -1_x|1\rangle = \tfrac{1}{2}, \ \langle -1_x|-1\rangle = \tfrac{1}{2}. \end{aligned}$$

Thus, for $|\psi\rangle = |\pm 1\rangle$ we have

$$\langle 1_x|\psi\rangle = \frac{1}{2}, \ \langle 0_x|\psi\rangle = \pm\frac{1}{\sqrt{2}}, \ \langle -1_x|\psi\rangle = \frac{1}{2}.$$

Hence, by the third postulate of quantum mechanics, we obtain the following probabilities:

$$\begin{aligned} &p(S_{x,1}) = |\langle 1_x|\psi\rangle|^2 = \tfrac{1}{4}, \\ &p(S_{x,0}) = |\langle 0_x|\psi\rangle|^2 = \tfrac{1}{2}, \\ &p(S_{x,-1}) = |\langle -1_x|\psi\rangle|^2 = \tfrac{1}{4}. \end{aligned}$$

From these results it is clear that the preparation states $|1\rangle$ and $|-1\rangle$ for obtaining the outcome probabilities $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$ satisfy the requirements of Theorem 2. Furthermore, as only the preparation state $|S_z\rangle$ is modified, the unitary matrix $U_x$ remains unaltered. Thus, enabling the physical realisation of this QRNG.

Please cite this article in press as: J.M. Agüero Trejo, C.S. Calude, A new quantum random number generator certified by value indefiniteness, Theoret. Comput. Sci. (2020), https://doi.org/10.1016/j.tcs.2020.08.014

*In what follows by QRNG will mean the QRNG constructed in this section.*

## 6. Ternary quantum random sequences

In this section we study the main properties of quantum random sequences produced by the proposed QRNG: 3-bi-immunity, unpredictability and Borel normality.

### 6.1. Ternary 3-bi-immunity

Theorem 4 holds true also for ternary quantum random sequences, but a stronger result is true. Informally, a sequence $\mathbf{x} \in A_b^\omega$ is $b$-bi-immune if for every $a \in A_b$, no algorithm can generate infinitely many pairs $(i, x_i = a)$ or $(i, x_i \neq a)$. Formally, following [20], we say that a sequence $\mathbf{x} \in A_b^\omega$ is *$b$-bi-immune* if for every $a \in A_b$ the support $\mathbf{x}^{-1}(a) = \{i \in \mathbb{N} \mid x_i = a\}$ is bi-immune in the sense of computability theory [39], i.e. the set and its complement contain no infinite computable subset. Obviously, $b$-bi-immunity is stronger than bi-immunity which is stronger than incomputability.

Consider a ternary sequence $\mathbf{x} = x_1 x_2 \ldots \in A_3^\omega$ generated by the QRNG. Then, for every $a \in A_3$ the set $\mathbf{x}^{-1}(a) = \{i \in \mathbb{N} \mid x_i = a\}$ and its complement contain no infinite computable subset because otherwise a definite value would need to be assigned to the observables corresponding to the measurement outputs contradicting the construction of the QRNG (Theorem 2). We have:

**Theorem 6.** *Assume the Eigenstate and epr principles. Then, every sequence generated by the QRNG is 3-bi-immune.*

It is seen that the particular dimension 3 plays no role, so a stronger form of Theorem 4 is true:

**Theorem 7.** *Assume the Eigenstate and epr principles. An infinite repetition of the experiment measuring a quantum value indefinite observable in $\mathbb{C}^b$ always generates a $b$-bi-immune sequence $\mathbf{x} \in A_b^\omega$.*

### 6.2. Ternary unpredictability

It is easy to check that the proof of Theorem 5 works not only for the binary case, but for an arbitrary alphabet $A_b$, $b \geq 2$. In particular we have

**Theorem 8.** *Assume the epr and Eigenstate principles. Let $\mathbf{x}$ be an infinite sequence obtained by measuring a quantum value indefinite observable in $\mathbb{C}^b$ in an infinite repetition of the experiment $E$. Then no single bit $x_i$ can be predicted.*

**Corollary 1.** *Assume the epr and Eigenstate principles. Then, no single digit of every sequence $\mathbf{x} \in A_3^\omega$ generated by the QRNG can be predicted.*

## 7. Binary quantum random sequences

As in most applications one needs binary random strings, in this section we propose an algorithm to transform ternary sequences into binary ones and, as in Section 6, we study their bi-immunity, unpredictability and Borel normality.

### 7.1. From ternary to binary sequences

We give a simple algorithm to transform a ternary sequence into a binary sequence. The method is an alphabetic morphism $\varphi\colon A_3 \to A_2$

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

which can be extended sequentially for strings, $\mathbf{y}(n) = \varphi(\mathbf{x}(n)) = \varphi(x_1)\varphi(x_2)\ldots\varphi(x_n)$ and sequences $\mathbf{y} = \varphi(\mathbf{x}) = \varphi(x_1)\varphi(x_2)\ldots\varphi(x_n)\ldots$.

### 7.2. Binary 2-bi-immunity

To prove 2-bi-immunity we use Theorem 6 and the following:

**Theorem 9** *([20]). Consider $b \geq 3$ and an alphabetic morphism $\varphi$ of $A_b$ onto $A_{b-1}$. Then for every $b$-bi-immune sequence $\mathbf{x} \in A_b^\omega$, the sequence $\varphi(\mathbf{x}) \in A_{b-1}^\omega$ is $(b-1)$-bi-immune.*

Please cite this article in press as: J.M. Agüero Trejo, C.S. Calude, A new quantum random number generator certified by value indefiniteness, Theoret. Comput. Sci. (2020), https://doi.org/10.1016/j.tcs.2020.08.014

**Corollary 2.** *The alphabetic morphism $\varphi$ defined by (1) converts a 3-bi-immune sequence into a 2-bi-immune sequence.*

### 7.3. Binary unpredictability

**Theorem 10.** *Assume the epr and Eigenstate principles. Let $\mathbf{y} = \varphi(\mathbf{x})$, where $\mathbf{x} \in A_3^\omega$ is a ternary sequence generated by the QRNG and $\varphi$ is the alphabetic morphism defined in (1). Then, no single bit of $\mathbf{y} \in A_2^\omega$ can be predicted.*

**Proof.** Let $\mathbf{y}$ be a sequence as in the statement above. Fix an extractor $\langle\rangle$, and assume for the sake of contradiction that there exists a predictor $P_E$ for $\mathbf{y}$ which is $k, \langle\rangle$-correct for all $k \geq 1$. Since $P_E$ *never* makes an incorrect prediction, each of its predictions is correct with certainty, so the algorithm $P_E$ correctly and deterministically predicts the bits of $\mathbf{y}$, contradicting Corollary 2. A more physical explanation of this mathematical conclusion comes from the epr principle: $P_E$ predictions correspond to a value definite property of the system measured, i.e. the QRNG, which contradicts Theorem 4. □

### 7.4. Uniform distribution and Borel normality

Recall that for $b \geq 2$, $A_b = \{0, 1, 2, \ldots, b-1\}$. Fix now an integer $m > 1$ and consider the alphabet $A_b^m = \{a_1, \ldots, a_{b^m}\}$ of all strings $x \in A_b^*$ with $|x|_b = m$, ordered lexicographically. A string $x \in A_b^*$ will be denoted by $x^m$ when we emphasise that it belongs to $(A_b^m)^*$. Take for example $A_2 = \{0, 1\}, m = 2, A_2^2 = \{00, 01, 10, 11\}$; the string $x = 0010101110 \in A_2^*$ will be denoted by $x^2 = (00)(10)(10)(11)(10)$ when considered in $A_2^2$. Clearly, $|x|_2 = 10$ and $|x^2|_4 = 5$. In the same way a sequence $\mathbf{x} \in A_b^\omega$ will be written as $\mathbf{x}^m$ when considered in $(A_b^m)^\omega$.

Let $\mathbf{x} \in A_3^\omega$ and consider the random variable $X_n(\mathbf{x}) = x_n$ on the probability space $(A_3^\omega, \mathcal{B}(A_3^\omega), \mathbb{P}_3)$, where $\mathbb{P}_3$ is the probability distribution of the QRNG. For simplicity we will write $X_n$ instead of $X_n(\mathbf{x})$ unless clarity suffers. Then $X_1, X_2, \ldots, X_n, \ldots$ is sequence of random variables mapping the sequence $\mathbf{x}$ to real-valued independent measurement outcomes, hence, it is a sequence of independent random variables with $\mathbb{P}_3(X_i = 1) = \frac{1}{2}$ and $\mathbb{P}_3(X_i = 0) = \mathbb{P}_3(X_i = 2) = \frac{1}{4}$. If $\mathbf{x} \in A_3^\omega$, then $\mathbf{y} = \varphi(\mathbf{x}) = \varphi(x_1)\varphi(x_2)\cdots \in A_2^\omega$, so we can consider the random variable $Y_i(\mathbf{y}) = y_i$. Since the random variables $X_i$ correspond to independent events, we have that $\mathbb{P}_3(Y_i = 1) = \mathbb{P}_3(X_i = 1) = \frac{1}{2}$ and the expected value $\mathbb{E}_3(Y_i = 0) = \mathbb{P}_3(X_i = 0) + \mathbb{P}_3(X_i = 2) = \frac{1}{2}$. Note that $Y_i$ takes values in $A_2$ with equal probabilities and $\mathbb{E}(Y_i) = 0 \cdot \mathbb{P}(Y_i = 0) + 1 \cdot \mathbb{P}(Y_i = 1) = \frac{1}{2}$. Thus $Y_1, Y_2, \ldots, Y_n, \ldots$ is an independent and identically distributed (i.i.d.) sequence of random variables with uniform distribution, i.e. in the Lebesgue probability space $(A_2^\omega, \mathcal{B}(A_2^\omega), \mathbb{P})$.

Is every sequence $\mathbf{y}$ Borel normal? To answer this question let's recall the definition of Borel normality. Let $N_i(x)$ be the number of occurrences of $i \in A_b$ in the string $x \in A_b^*$ and for every $u \in A_b^m$ let $N_u^m(x^m)$ be the number of occurrences of $u$ in the string $x^m \in (A_b^m)^*$. In the example above $N_0^1(x) = N_1^1(x) = 5$ and $N_{11}^2(x^2) = 1, N_{10}^2(x^2) = 3, N_{01}^2(x^2) = 0$. There are strings $x \in A_b^*$ for which $x^m$ does not exist for some, even all, $m$ (for example when $m$ is prime), but for all $m$ and $\mathbf{x} \in A_b^\omega$ the sequence $\mathbf{x}^m$ exists.

Recall that for $\mathbf{x} \in A_b^\omega$ and $n \geq 1$, $\mathbf{x}(n) = x_1 x_2 \ldots x_n \in A_b^*$. The sequence $\mathbf{x}$ is called *$m$-Borel normal* ($m \geq 1$) in case for every $u \in (A_b^m)^*$ one has:

$$\lim_{n\to\infty} \frac{N_u^m(\mathbf{x}^m(\lfloor \frac{n}{m} \rfloor))}{\lfloor \frac{n}{m} \rfloor} = \frac{1}{b^m}.$$

The sequence $\mathbf{x} \in A_b^\omega$ is called *Borel normal* if it is Borel $m$-normal, for every natural $m \geq 1$. In particular, a sequence $\mathbf{x}$ is Borel 1-normal when for every $a \in A_b$ we have:

$$\lim_{n\to\infty} \frac{N_a(\mathbf{x}(n))}{n} = \frac{1}{b}.$$

We can generalise this construction of the i.i.d. random variables $(Y_i)$ by considering bit strings of arbitrary length $m \geq 1$ and then use the Strong Law of Large Numbers [14] to get that *with probability one every bit sequence produced by the QRNG is Borel normal.* However, this result gives no new information as Borel Law of Large Numbers [15] states that with probability one every bit sequence is Borel normal. To get more insight we turn to a finite version of Borel normality [18] to analyse this property for prefixes of an arbitrary bit sequence produced via the ternary sequence generated by the QRNG.

For every $\varepsilon > 0$ and integer $m > 1$ we say that a string $x \in A_2^*$ is *Borel normal with accuracy* $(m, \varepsilon)$ if

$$\left| \frac{N_u^m(x^m(\lfloor \frac{|x|_2}{m} \rfloor))}{\lfloor \frac{|x|_2}{m} \rfloor} - 2^{-m} \right| \leq \varepsilon, \tag{2}$$

for each $u \in A_2^m$ and $1 \leq m \leq \log_2 \log_2 |x|_2$.

It is useful to consider as $\varepsilon$ a computable function of $|x|_2$ converging to zero when $|x|_2$ to infinity. For example, in [18,19] the accuracy is $\sqrt{\frac{\log_2 |x|_2}{|x|_2}}$ and in [4] it is $\frac{1}{\log_2 |x|_2}$. Almost all algorithmic random strings of any length are Borel normal with these accuracies [18,19]. Furthermore, *if all prefixes of a bit sequence are Borel normal, then the sequence itself is also Borel normal.*

Please cite this article in press as: J.M. Agüero Trejo, C.S. Calude, A new quantum random number generator certified by value indefiniteness, Theoret. Comput. Sci. (2020), https://doi.org/10.1016/j.tcs.2020.08.014

**Lemma 1.**

*Let $\mathbf{x} \in A_2^\omega$ be a ternary sequence generated by the QRNG and let $\mathbf{y} = \varphi(\mathbf{x})$. Then for every $m > 1$, the probability that $\mathbf{y}(m)$ is Borel normal with accuracy $\left(m, \sqrt{\frac{\log_2 |x|_2}{|x|_2}}\right)$ is at least $1 - \frac{1}{\sqrt{\log_2 m}}$.*

**Proof.** Using [19, Lemma 5.43] we deduce that for every $m > 1$,

$$\#\left\{z \in A_2^m \mid z \text{ is not Borel normal with accuracy } \left(m, \sqrt{\frac{\log_2 |x|_2}{|x|_2}}\right)\right\} \leq \frac{2^m}{\sqrt{\log_2 m}},$$

hence the probability that $\mathbf{y}(m)$ is Borel normal with accuracy $\left(m, \sqrt{\frac{\log_2 |x|_2}{|x|_2}}\right)$ is greater or equal to

$$1 - \frac{1}{\sqrt{\log_2 m}}. \quad \square \tag{3}$$

We note that the probability (3) increases with $m$ but this is not enough to deduce that $\mathbf{y} = \varphi(\mathbf{x})$ is Borel normal: we only get Borel normality with probability one. With larger and larger probabilities the prefixes of $\mathbf{y}$ are Borel normal, a property which is useful for practical purposes – when only finitely many bits of $\mathbf{y}$ can be computed – and this property can be *tested* (and it was tested in [21,35,4]).

## 8. Conclusions

We have proposed a new ternary QRNG based on measuring located value indefinite observables and proved that every sequence generated is maximally unpredictable, 3-bi-immune (a stronger form of bi-immunity), and its prefixes are Borel normal. The ternary quantum random digits produced by the QRNG are algorithmically transformed into quantum random bits using an alphabetic morphism which preserves all the above properties. One important question remains to be studied: how various forms of measurement error affect the properties of the quantum random bits obtained with this QRNG, see [1,2,34]. The QRNG proposed in this paper will be realised physically with qutrits with a method similar to the one used in [30] and the quality of randomness of samples of strings of length $2^{32}$ will be tested in comparison with strings of pseudo-random bits, produced by the best available pseudo-random number generators, using various methods including those in [4].

One referee asked the following interesting question. Suppose a randomness test rejects the hypothesis of randomness for many long strings of quantum random bits generated by the proposed QRNG. Does this fact refute the corresponding physical theory on which the QRNG is based on? Such an approach may be attractive to physicists, because it is somewhat cheaper than other sophisticated precision experiments designed to test the validity of quantum mechanics. Tentatively the answer is negative. First, theoretically, that is, ignoring a whole host of possibly erroneous hypotheses entering the empirical interpretation, every test of randomness applies to finitely many, admittedly, very long, strings of quantum random bits, so it does not prove non-randomness, which is an asymptotic property of the *infinite* sequences quantum random bits. Second, following [31], we would check for a bug in the QRNG implementation and/or some questionable/flawed assumptions implicitly made in its construction. Third, if no issues were found with the implementation and the test is failed in many cases on a large variety of very long strings obtained with different QRNGs based on the same theory, then the theoretical assumptions made in Section 3 would be scrutinised.

## Declaration of competing interest

The authors declare that there is no conflict of interest.

## Acknowledgements

This work was supported by The U.S. Office of Naval Research Global under Grant N62909-19-1-2038. The cooperation and support of S. Feng from the Office of Naval Research Global, N. Allen and K. Pudenz at Lockheed Martin and A. Fedorov and his team at University of Queensland are much appreciated. We also thank M. Dumitrescu, L. Staiger, C. Stoica and, particularly K. Svozil, for many useful discussions and suggestions.

Please cite this article in press as: J.M. Agüero Trejo, C.S. Calude, A new quantum random number generator certified by value indefiniteness, Theoret. Comput. Sci. (2020), https://doi.org/10.1016/j.tcs.2020.08.014

## References

[1] A.A. Abbott, L. Bienvenu, G. Senno, Non-uniformity in the quantis random number generator, Report CDMTCS-472, Centre for Discrete Mathematics and Theoretical Computer Science, University of Auckland, Auckland, New Zealand, Nov. 2014.
[2] A.A. Abbott, C.S. Calude, Von Neumann normalisation of a quantum random number generator, Computability 1 (1) (2012) 59–83.
[3] A.A. Abbott, C.S. Calude, J. Conder, K. Svozil, Strong Kochen-Specker theorem and incomputability of quantum randomness, Physical Review A 86 (062109) (Dec 2012).
[4] A.A. Abbott, C.S. Calude, M.J. Dinneen, N. Huang, Experimentally probing the algorithmic randomness and incomputability of quantum randomness, Physica Scripta 94 (4) (feb 2019) 045103.
[5] A.A. Abbott, C.S. Calude, K. Svozil, Value-indefinite observables are almost everywhere, Physical Review A 89 (032109) (2013).
[6] A.A. Abbott, C.S. Calude, K. Svozil, A quantum random number generator certified by value indefiniteness, Mathematical Structures in Computer Science 24 (e240303) (2014) 6.
[7] A.A. Abbott, C.S. Calude, K. Svozil, Value indefiniteness is almost everywhere, Physical Review A 89 (3) (2014) 032109.
[8] A.A. Abbott, C.S. Calude, K. Svozil, A non-probabilistic model of relativised predictability in physics, Information 6 (4) (2015) 773–789.
[9] A.A. Abbott, C.S. Calude, K. Svozil, On the unpredictability of individual quantum measurement outcomes, in: L.D. Beklemishev, A. Blass, N. Dershowitz, B. Finkbeiner, W. Schulte (Eds.), Fields of Logic and Computation II - Essays Dedicated to Yuri Gurevich on the Occasion of His 75th Birthday, in: Lecture Notes in Computer Science, vol. 9300, Springer, 2015, pp. 69–86.
[10] A.A. Abbott, C.S. Calude, K. Svozil, A variant of the Kochen-Specker theorem localising value indefiniteness, Journal of Mathematical Physics 56 (Oct. 2015) 102201, https://doi.org/10.1063/1.4931658.
[11] J.S. Bell, On the problem of hidden variables in quantum mechanics, Reviews of Modern Physics 38 (1966) 447–452.
[12] J.S. Bell, Speakable and Unspeakable in Quantum Mechanics, Cambridge University Press, Cambridge, 1987.
[13] L. Bienvenu, A.R. Day, R. Hölzl, From bi-immunity to absolute undecidability, J. Symbolic Logic 78 (4) (2013) 1218–1228.
[14] P. Billingsley, Probability and Measure, 3rd ed., John Wiley & Sons, New York, Toronto, London, 1994.
[15] É. Borel, Les probabilités dénombrables et leurs applications arithmétiques, Rendiconti del Circolo Matematico di Palermo (1884–1940) 27 (1909) 247–271.
[16] A. Cabello, A simple proof of the Kochen-Specker theorem, European Journal of Physics 15 (179–183) (1994).
[17] A. Cabello, J.M. Estebaranz, G. García-Alcaine, Bell-Kochen-Specker theorem: a proof with 18 vectors, Physics Letters A 212 (1996) 183–187.
[18] C. Calude, Borel normality and algorithmic randomness, in: G. Rozenberg, A. Salomaa (Eds.), Developments in Language Theory, World Scientific, Singapore, 1994, pp. 113–129.
[19] C. Calude, Information and Randomness—an Algorithmic Perspective, 2nd ed., Springer, Berlin, 2002.
[20] C.S. Calude, K. Celine, Z. Gao, S. Jain, L. Staiger, F. Stephan, Bi-immunity over Different Size Alphabets, 2020, work in preparation.
[21] C.S. Calude, M.J. Dinneen, M. Dumitrescu, K. Svozil, Experimental evidence of quantum randomness incomputability, Phys. Rev. A 82 (2) (Aug. 2010) 022102.
[22] C.S. Calude, G. Longo, Classical, quantum and biological randomness as relative unpredictability, Nat. Comput. 15 (2) (2016) 263–278.
[23] G.J. Chaitin, Algorithmic information theory, IBM Journal of Research and Development 21 (350–359) (1977) 496.
[24] W.R. Clements, P.C. Humphreys, B.J. Metcalf, W.S. Kolthammer, I.A. Walmsley, Optimal design for universal multiport interferometers, Optica 3 (12) (Mar. 2016) 1460–1465.
[25] R. Downey, D. Hirschfeldt, Algorithmic Randomness and Complexity, Springer, Berlin, 2010.
[26] A. Einstein, B. Podolsky, N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, Physical Review 47 (10) (May 1935) 777–780.
[27] W. Feller, An Introduction to Probability Theory and Its Applications, Vol. 1, John Wiley & Sons, New York, 1950.
[28] M. Herrero-Collantes, J.C. Garcia-Escartin, Quantum random number generators, Rev. Mod. Phys. 89 (Feb. 2017) 015004.
[29] S.B. Kochen, E. Specker, The problem of hidden variables in quantum mechanics, Journal of Mathematics and Mechanics 17 (1967) 59–87; Reprinted in E. Specker, Selecta, Brikhäuser Verlag, Basel, 1990.
[30] A. Kulikov, M. Jerger, A. Potočnik, A. Wallraff, A. Fedorov, Realization of a quantum random generator certified with the Kochen-Specker theorem, Phys. Rev. Lett. 119 (Dec 2017) 240501.
[31] I. Lakatos, Philosophical Papers. 1. The Methodology of Scientific Research Programmes, Cambridge University Press, Cambridge, 1978.
[32] A.K. Lenstra, J.P. Hughes, M. Augier, J.W. Bos, T. Kleinjung, C. Wachter, Ron was wrong, whit is right, Santa Barbara: IACR: 17, https://eprint.iacr.org/2012/064.pdf, 2012.
[33] M. Li, P.M.B. Vitányi, An Introduction to Kolmogorov Complexity and Its Applications, 4th edition, Springer Verlag, New York, NY, 2019.
[34] L. Loveridge, Quantum Measurements in the Presence of Symmetry, PhD thesis, University of York, 2012.
[35] A.C. Martínez, A. Solís, R.D.H. Rojas, A.B. U'Ren, J.G. Hirsch, I.P. Castillo, Testing randomness in quantum mechanics, CoRR, arXiv:1810.08718, 2018.
[36] E. Merzbacher, Quantum Mechanics, 3rd ed. edition, Wiley & Sons, New York, 1998.
[37] A. Peres, Two simple proofs of the Kochen-Specker theorem, Journal of Physics A: Mathematical and General 24 (4) (1991) L175–L178.
[38] M. Reck, A. Zeilinger, H.J. Bernstein, P. Bertani, Experimental realization of any discrete unitary operator, Phys. Rev. Lett. 73 (Jul. 1994) 58–61.
[39] H. Rogers Jr., Theory of Recursive Functions and Effective Computability, MacGraw-Hill, New York, 1967.
[40] M. Sipser, Introduction to the Theory of Computation, 1st edition, International Thomson Publishing, 2013 (3rd ed.).
[41] K. Svozil, Physical [A]Causality. Determinism, Randomness and Uncaused Events, Springer, Berlin, 2018.
[42] J. von Neumann, Various techniques used in connection with random digits, National Bureau of Standards Applied Math Series 12 (1951) 36–38; Reprinted in A.H. Traub (Ed.), John Von Neumann, Collected Works (Vol. V), MacMillan, New York, 1963, pp. 768–770.
[43] B. Yurke, S.L. McCall, J.R. Klauder, SU(2) and SU(1,1) interferometers, Physical Review A 33 (1986) 4033–4054.

Please cite this article in press as: J.M. Agüero Trejo, C.S. Calude, A new quantum random number generator certified by value indefiniteness, Theoret. Comput. Sci. (2020), https://doi.org/10.1016/j.tcs.2020.08.014