



CDMTCS Research Report Series





# An N-Dimensional Quantum Random Number Generator

J. M. Agüero Trejo and C. S. Calude

University of Auckland, New Zealand



CDMTCS-583 June 2025



Centre for Discrete Mathematics and Theoretical Computer Science

# An N-Dimensional Quantum Random Number Generator

José Manuel Agüero Trejo and Cristian S. Calude University of Auckland, New Zealand

#### Abstract

We present a method to construct an N-dimensional quantum number generator (QRNG) certified via valueindefiniteness (Kochen-Specker Theorem) working in a Hilbert space of dimension larger than 2 that generates quantum random N-digits with a pre-given probability distribution with  $0 < p_1, p_2, \ldots, p_N < 1$  and  $\sum_{i=1}^{N} p_i = 1$ .

Our construction is based on a unitary decomposition corresponding to a physically realisable photonic embodiment via photonic primitives such as beamsplitters and phase shifters.

We prove that every sequence of quantum random digits generated by the N-dimensional QRNG is highly incomputable and Borel normal, hence its randomness quality is better than that of every pseudo-random generator.

# **1** Introduction

Over the past decade, the use of quantum random number generators (QRNGs) has grown significantly due to the increasing demand for high-quality randomness across various fields—including cryptography, statistics, information science, medicine, and physics—as well as the limitations and sometimes catastrophic failures of pseudo-random number generators [15]. QRNGs are often regarded as superior to PRNGs because they rely on the inherent unpredictability of carefully selected and controlled quantum processes [13]. However, the superiority of a QRNG over any PRNG warrants deeper scientific justification, and to date, the only QRNG for which such a theory was developed is the 3D QRNG [7, 6].

In this paper, we generalise the construction in [6] to develop a uniform approach for constructing a class of photonic N-dimensional QRNGs for N > 2. This method is based on a universal unitary operator and a strategy for preparing quantum value-indefinite states that comply with the Located Kochen-Specker Theorem [2]. Measurements on these states yield outcomes that are produced with an apriori specified probability distribution.

We prove that every sequence of quantum random digits generated by the N-dimensional QRNG is highly incomputable and Borel normal, hence its randomness quality is better than that of every pseudo-random generator.

# 2 Notation and Definitions

An observable is a physical property or physical quantity that can be measured. In quantum physics, an observable is value-definite if it always yields the same value when measured, even if the system is in a superposition of states. The values that a value-definite observable can take are called eigenvalues, and the states of the system that correspond to these values are called eigenstates. A Hermitian operator is a linear operator that equals its own conjugate transpose, that is, it is self-adjoint. If each eigenvalue of a Hermitian operator has a unique corresponding eigenvector, then there exists a unique orthonormal basis for it; in this case we say that it has a non-degenerate spectrum. For more details, see [16].

By  $\mathbb{R}$  we denote the set of reals and by  $\mathbb{C}^N$  the complex Hilbert space of dimension N > 2.

# **3** Theoretical Results

In this section, we summarise the main known theoretical results.

#### 3.1 Localising value-indefinitness

Value-indefiniteness is the main concept in this paper and the Kocken-Specker Theorem [14] shows that in a Hilbert space of dimension N > 2, there exists a value-indefinite observable. This result is proved by assuming the following three hypotheses.

- Admissibility. This hypothesis guarantees agreement with quantum mechanics predictions. Fix a set O of onedimensional projection observables on C<sup>N</sup> and the value assignment function v : O → {0,1}. Then v is admissible if for every context C of O, we have ∑<sub>P∈C</sub> v(P) = 1. Accordingly, only one projection observable in a context can be assigned the value 1.
- **Non-contextuality of definite values.** Every outcome obtained by measuring a value definite observable is non-contextual, i.e. it does not depend on other compatible observables which may be measured alongside it.
- Eigenstate principle. If a quantum system is prepared in the state  $|\psi\rangle$ , then the projection observable  $P_{\psi}$  is value definite

Kocken-Specker Theorem proves only the existence of value-indefinite observables, hence it is not enough for our QRNGs, which work by *measuring value-indefinite observables*. The following result solves this problem:

**Theorem 1 (Located Kochen-Specker Theorem[2, 3])** Assume a quantum system prepared in the state  $|\psi\rangle$  in a Hilbert space  $\mathbb{C}^N$  with  $n \ge 3$ , and let  $|\phi\rangle$  be any quantum state such that  $0 < |\langle \psi | \phi \rangle| < 1$ . 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.

# 4 Photonic Components

In this section, we present the photonic components of the QRNGs.

#### 4.1 Beamsplitter

We use a transformation produced by a lossless beamsplitter and an external phase shifter to represent the annihilation operators of the quantum harmonic oscillator [11]. Here, the transmittance and reflectivity parameters are described within the unitary matrix, and the input and output states are represented with modes (u, v) and (u', v'), respectively:

$$\begin{pmatrix} u'\\v' \end{pmatrix} = \begin{pmatrix} \cos\theta & ie^{i\vartheta}\sin\theta\\i\sin\theta & e^{i\vartheta}\cos\theta \end{pmatrix} \begin{pmatrix} u\\v \end{pmatrix},$$

where  $\theta$  describes the square root of the reflectivity, the transmittance is given by  $\sin \theta$  and  $\cos \theta$  respectively, and  $\vartheta$  represents the phase of an external phase shifter on the second input port.

#### 4.2 A N-multiport beamsplitter

As demonstrated in [17], given an arbitrary N-dimensional unitary operator, we can represent a generalised rotation through the decomposition of the unitary matrix using a series of phase shifters and standard beamsplitters implemented in an optical experiment. A multiport beamsplitter is called *symmetric* if the norm of all its matrix elements are equal. To model the behaviour of an N-dimensional system, it is useful to generalise the effect of a standard beamsplitter to a single multiport symmetric beamsplitter acting on N-input modes and N-output modes. For dimensional N we may express it by:

$$BS_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \dots & 1\\ 1 & e^{i\varphi_{22}} & \dots & e^{i\varphi_{2N}}\\ \vdots & \vdots & \ddots & \vdots\\ 1 & e^{i\varphi_{N2}} & \dots & e^{i\varphi_{NN}} \end{pmatrix}.$$

The parametric family of this type of operator is known, allowing for a physical realisation with an *N*-multiport beam-splitter [17].

A natural example occurs for dimension 2, where a lossless symmetric beamsplitter may be used to perform a Hadamard transformation on a qubit:

$$\begin{pmatrix} |0'\rangle\\ |1'\rangle \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1\\ 1 & -1 \end{pmatrix} \begin{pmatrix} |0\rangle\\ |1\rangle \end{pmatrix}$$

# 5 An N-dimensional QRNG

In this section, we present the construction of an N-dimensional QRNG by measuring a value indefinite observable in  $\mathbb{C}^N$ , for an arbitrary  $N \ge 3$ .

#### 5.1 Preparation: the first measurement operator

We choose an *N*-dimensional unitary Hermitian operator with non-degenerate spectra. From Theorem 1, it follows that 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.

Ideally, we want an operator with eigenvectors corresponding to the standard Cartesian basis on dimension N. If this is the case, the basis states correspond to the N input modes of the final measurement device (the alternatives that satisfy the requirements are equivalent to a change of basis). For an arbitrary  $N \ge 3$  we may construct the spin state operators to find a suitable candidate (up to a change of basis) [1]. For example, in [8], for N = 3 the first measurement operator

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

corresponds to the spin state operator  $S(\frac{\pi}{2}, 0)$  by considering the orthonormal standard Carthesian basis.

We will use the first measurement operator to provide a value definite state (preparation state) so that its interaction with a secondary operator satisfies Theorem 1; that is, the eigenstates of the second measurement operator are neither orthogonal nor parallel to the preparation state.

#### 5.2 Number generation: the second measurement operator

To fulfill the conditions required to apply the Located Kochen-Specker Theorem, we choose an N-dimensional unitary Hermitian operator with distinct eigenvectors which is different from the one used in the first measurement operator.

We can construct such a unitary Hermitian operator by working with the parametric family of symmetric multiport beamsplitters on dimension N and finding an appropriate phase value.

This operator may be degenerate as a consequence the role of such operators and the non-contextuality assumption in the original formulation of the Kochen-Specker Theorem. To proceed, we recall the following conditions on a value assignment map V.

- For any self-adjoint operator  $\mathcal{O}$  corresponding to an observable O, we have that  $V(\mathcal{O}) \in \{o_i\}$ , where  $\{o_i\}$  are the eigenvalues of  $\mathcal{O}$ . That is, each observable corresponds to an element of physical reality, and the values assigned correspond to the set of possible outcomes.
- (Quasi-linearity) For commuting operators  $\mathcal{A}, \mathcal{B}$ , that is  $[\mathcal{A}, \mathcal{B}] = 0$ , we have that  $V(a\mathcal{A}+b\mathcal{B}) = aV(\mathcal{A}) + bV(\mathcal{B})$ , where  $a, b \in \mathbb{R}$ .
- (Non-contextuality) All observables are assigned values simultaneously regardless of what else is being measured with a given observable, that is, regardless of the measurement context.

From quasi-linearity, it follows that the map must preserve the algebraic structures of the operators. That is, for any Borel function f, we have that  $V(\mathcal{A}) = f(V(\mathcal{B}))$ , whenever  $\mathcal{A} = f(\mathcal{B})$ . This is the core element leading to a contradiction in many proofs of the Kochen-Specker Theorem. However, the contradiction only occurs for degenerate operators in the original Kochen-Specker formulation as a result of the following properties: If an operator  $\mathcal{A}$  is degenerate, for some non-degenerate operators  $\mathcal{B}, \mathcal{C}$  and Borel functions f, g, we have that

$$\mathcal{A} = f(\mathcal{B}) \text{ and } \mathcal{A} = g(\mathcal{C}), \text{ with } [\mathcal{B}, \mathcal{C}] \neq 0.$$

Thus, from quasi-linearity it follows that

$$V(\mathcal{A}) = f(V(\mathcal{B})) = g(V(\mathcal{C})).$$

The sum of the projectors of a complete orthonormal set of states yields the identity operator. So, since orthogonal projectors commute, the sum of their assigned values must be one. In the case of one-dimensional degenerate operators, we get a single projector with value one and N - 1 zero-valued projectors for an N-dimensional Hilbert space. This leads to a contradiction when considering all complete sets of projectors since a projector is a function of different non-commuting, non-degenerate operators. In other words, degenerate one-dimensional operators must be assigned the same value regardless of which non-degenerate operator it is considered to be a function of. As a consequence, we are forced to accept the existence of value-indefinite observables or some form of contextuality.

Note that the first measurement operator helps us prepare the measurement context with a corresponding value definite preparation state. Moreover, all Hermitian operators are self-adjoint, so degeneracy of an observable can be understood as having more than one measurement basis (or measurement context) for an observable and is not detrimental when localising a value-indefinite observable (nor it is required in the localised variant of the Kochen-Specker Theorem).

"What we observe is not nature itself, but nature exposed to our method of questioning", W. Heisenberg, [12]

#### 5.3 State preparation, outcome probabilities, strong incomputability and Borel normality

Choose any probability distribution  $p_1, p_2, p_3, \ldots, p_N$  with  $\sum_i p_i = 0$  and  $0 < p_i < 1$ . We apply the process described in [8] to select a preparations state  $|\psi\rangle$  defined with the first measurement operator. In this way, we ensure that the conditions imposed by the Localised Kochen-Specker Theorem are met by performing the second measurement on  $|\psi\rangle$ . That is, we may construct value indefinite observables which, by measurement, produce outcomes with the probabilities  $p_1, p_2, p_3, \ldots, p_N$ .

An N-dimensional QRNG can operate indefinitely many times in an algorithmic fashion of the form "preparation, measurement, reset" and generate infinite sequences. Generalising the certification of a 3D QRNG in [6] one can show that every sequence generated by any N-dimensional QRNG is incomputable, that is, no sequence produced by an N-dimensional QRNG can be reproduced exactly by any algorithm, in particular, by any pseudo-random generator. This shows that the quality of the quantum random digits produced by every N-dimensional QRNG is provable better than the one produced by any pseudo-random number generator

A stronger result can be obtained by using the non-probabilistic model for unpredictability [4, 5], the Eigenstate principle and:

**epr principle**: If a repetition of measurements of an observable generates a computable sequence, then this implies these observables were valued definite.

The proof of Theorem 5.1 from [6] can be generalised from N = 3 to every N > 2:

**Theorem 2** Assume the epr and Eigenstate principles. Let  $\mathbf{x}$  be an infinite sequence generated by an N-dimensional QRNG. Then no single digit  $x_i \mathbf{x}$  can be predicted.

Now, fix 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  $(A_b^m)^*$ . By  $A_b^\omega$  we denote the set of all infinite sequences  $\mathbf{x} = x_1 x_2 \cdots$  with  $x_i \in A_b^*$ .

Take for example, for  $A_2 = \{0, 1\}, m = 2, A_2^2 = \{00, 01, 10, 11\}$ ; the string  $x = 10110100 \in A_2^*$  will be denoted by  $x^2 = (10)(11)(01)(00)$  when considered in  $A_2^2$ . Clearly,  $|x|_2 = 8$  and  $|x^2|_4 = 4$ . 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  $N_i(x)$  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  $x^m \in (A_b^m)^*$ . Recall that for  $\mathbf{x} \in A_b^\omega$  and  $n \ge 1$ ,  $\mathbf{x}(n) = x_1 x_2 \dots x_n \in A_b^*$ . The sequence  $\mathbf{x}$  is called *m*-Borel normal  $(m \ge 1)$  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  $m \ge 1$ , [9].

For applications that require binary strings, in order to ensure the results from [7, 8] apply, we need to choose a suitable probability distribution and a suitable alphabetic morphism; this is dependent on the dimension N.

In particular, for dimension  $N = 2^m$  with positive integer m > 1, choosing an equally likely distribution of outcomes allows us to achieve Borel *m*-normality through a simple alphabetic morphism  $\varphi$ : assign a different string from the alphabet  $A_2^m$  to each of the possible N outcomes. **Theorem 3** Let m > 1 and the  $2^m$ -dimensional QRNG described above, in which the preparation state was selected so that each outcome occurs with probability of  $2^{-m}$ . Fix an alphabetic morphism given by a bijection  $\varphi : A_{2^m} \to A_2^m$ . Then, for every sequence  $\mathbf{x}$  generated by the QRNG, the binary sequence  $\varphi(\mathbf{x})$  is m-Borel normal.

## 6 A 4-dimensional Example

We can find the first measurement operator for an arbitrary  $N \ge 3$  by constructing the spin state operator for N. For dimension N = 4, we have the Hermitian non-degenerate operator

$$\frac{1}{2} \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 \end{pmatrix}.$$

Since the operator is non-degenerate, it has distinct eigenvectors and eigenvalues that we can map to each input port. These are given by  $\{\frac{3}{2}, \frac{1}{2}, -\frac{1}{2}, -\frac{3}{2}\}$  and the corresponding eigenvectors with respect to the Cartesian Standard basis are:

$$|1\rangle = \begin{pmatrix} 1\\0\\0\\0 \end{pmatrix}, |2\rangle = \begin{pmatrix} 0\\1\\0\\0 \end{pmatrix}, |3\rangle = \begin{pmatrix} 0\\0\\1\\0 \end{pmatrix}, |4\rangle = \begin{pmatrix} 0\\0\\0\\1 \end{pmatrix}.$$

For the second measurement operator an element of the family of symmetric multiport beamsplitters on dimension 4 is given by:

$$\frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{i\phi} & -1 & -e^{i\phi} \\ 1 & -1 & 1 & -1 \\ 1 & -e^{i\phi} & -1 & e^{i\phi} \end{pmatrix}$$

Choosing the phase  $\phi = \pi$  we get the unitary Hermitian operator

with eigenvectors

$$|1_U\rangle = \begin{pmatrix} 0\\ -1\\ 0\\ 1 \end{pmatrix}, |2_U\rangle = \begin{pmatrix} -1\\ 2\\ 1\\ 0 \end{pmatrix}, |3_U\rangle = \begin{pmatrix} 2\\ 1\\ 0\\ 1 \end{pmatrix}, |4_U\rangle = \begin{pmatrix} 1\\ 0\\ 1\\ 0 \end{pmatrix}.$$

For dimension N = 4 and equally likely outcomes  $(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$  this process yields the state

$$\left|\psi\right\rangle = \frac{1}{2}\left|3\right\rangle + \frac{1}{2}\left|4\right\rangle.$$

Indeed, applying the second measurement to  $|4\rangle$  we get that

$$\langle 1_U | \psi \rangle = \langle 4 | \psi \rangle = \frac{1}{2} \langle 4 | 4 \rangle = \frac{1}{2}, \implies |\langle 1_U | \psi \rangle|^2 = \frac{1}{4},$$

$$\langle 2_U | \psi \rangle = \langle 3 | \psi \rangle = \frac{1}{2} \langle 3 | 3 \rangle = \frac{1}{2}, \implies |\langle 1_U | \psi \rangle|^2 = \frac{1}{4},$$

$$\langle 3_U | \psi \rangle = \langle 4 | \psi \rangle = \frac{1}{2} \langle 4 | 4 \rangle = \frac{1}{2}, \implies |\langle 1_U | \psi \rangle|^2 = \frac{1}{4},$$

$$\langle 4_U | \psi \rangle = \langle 3 | \psi \rangle = = \frac{1}{2} \langle 3 | 3 \rangle \frac{1}{2}, \implies |\langle 1_U | \psi \rangle|^2 = \frac{1}{4}.$$

So we get a value indefinite outcome with the desired probability distribution. Finally, by Theorem 3 we may guarantee Borel 2-normality for applications requiring binary strings.



Figure 1: Photonic realisation of the unitary decomposition. The numbering on the left side indicates the input modes

#### 6.1 Unitary decomposition

Consider the following beamsplitter matrix:

$$BS = \begin{pmatrix} e^{i\phi}\cos\theta & -\sin\theta\\ e^{i\phi}\sin\theta & \cos\theta \end{pmatrix}.$$

We note that BS is equivalent to the beamsplitter matrix presented in Section 4.1 by a phase factor. We work here with the matrix BS because its form facilitates the decomposition technique in [10].

Here,  $\phi$  represents a phase and  $\theta$  an angle. Let  $BS_{i,j}$  represent the beamsplitter between modes i and j we have:

Beamsplitter	$\theta$	$\phi$
$BS_{1,2}$	$\frac{\pi}{4}$	0
$BS_{3,4}$	$\frac{\pi}{4}$	$-\pi$
$BS_{2,3}$	$\frac{\pi}{4}$	0
$BS_{1,2}$	$\frac{\pi}{2}$	$-\pi$
$BS_{3,4}$	$\frac{\pi}{2}$	2.55
$BS_{2,3}$	$\frac{\pi}{4}$	$\pi$

## Acknowledgement

We thank E. H. Allen and C. Stoica for discussions and comments which improved the paper.

## References

- [1] Spin Matrices For Arbitrary Spin, https://tinyurl.com/59k22mhj.
- [2] A. A. Abbott, C. S. Calude, J. Conder, and K. Svozil. Strong Kochen-Specker theorem and incomputability of quantum randomness. *Physical Review A*, 86(062109), Dec 2012.
- [3] A. A. Abbott, C. S. Calude, and K. Svozil. Value-indefinite observables are almost everywhere. *Physical Review A*, 89(032109), 2013.
- [4] A. A. Abbott, C. S. Calude, and K. Svozil. A non-probabilistic model of relativised predictability in physics. *Information*, 6(4):773–789, 2015.
- [5] A. A. Abbott, C. S. Calude, and K. Svozil. On the unpredictability of individual quantum measurement outcomes. In L. D. Beklemishev, A. Blass, N. Dershowitz, B. Finkbeiner, and W. Schulte, editors, *Fields of Logic and Computation II*, volume 9300 of *Lecture Notes in Computer Science*, pages 69–86. Springer, 2015.
- [6] J. M. Agüero Trejo and C. S. Calude. Photonic ternary quantum random number generators. *Proc. R. Soc. A*, 479:1–16, 2023.

- [7] J. M. Agüero Trejo and C. S. Calude. A new quantum random number generator certified by value indefiniteness. *Theoretical Computer Science*, 862:3–13, Mar. 2021.
- [8] J. M. Agüero Trejo and C. S. Calude. Photonic ternary quantum random number generators. *Proc. R. Soc. A*, 479:1–16, 2023.
- [9] C. Calude. Borel normality and algorithmic randomness. In G. Rozenberg and A. Salomaa, editors, *Developments in Language Theory*, pages 113–129. World Scientific, Singapore, 1994.
- [10] W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Kolthammer, and I. A. Walmsley. Optimal design for universal multiport interferometers. *Optica*, 3(12):1460–1465, Dec. 2016.
- [11] C. Gerry and P. L. Knigh. Introductory Quantum Optics. Cambridge University Press, Cambridge, UK, 2005.
- [12] W. Heisenberg. Physics and Philosophy: The Revolution in Modern Science. Harper, New York, 1958.
- [13] ID Quantique SA. Random Number Generation White Paper. Quantum versus Classical Random Number Generators. idQuantique, Geneva, Switzerland, May 2020.
- [14] S. B. Kochen and E. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics (now Indiana University Mathematics Journal)*, 17(1):59–87, 1967.
- [15] J. Markoff. Flaw found in an online encryption method. https://tinyurl.com/2n3pkzex, 2021. New York Times. [Online; accessed 8-May-2025].
- [16] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2010.
- [17] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73(1):58–61, July 1994.