CDMTCS
Research
Report
Series

ND-Photonic QRNGs in a Noisy Environment

J. M. Agüero Trejo[1], C. S. Calude[1] and O.C. Stoica[2]
University of Auckland[1] and NIPNE–HH[2]

CDMTCS-591
1 July 2026

Centre for Discrete Mathematics and
Theoretical Computer Science

ND-Photonic QRNGs in a Noisy Environment

J. M. Agüero Trejo[*], Cristian S. Calude[†], O. C. Stoica[‡]

Abstract

Standard pseudo-random generators have weaknesses that have led to the development of quantum random number generators (QRNGs). However, common QRNG validation methods, whether based on quantum indeterminism or statistical tests, are insufficient to guarantee high-quality randomness. In contrast, a mathematical theory based on the Located Kochen-Specker Theorem proves that 3D QRNGs produce maximally unpredictable outputs without using entanglement, and both theory and experiments have supported their security. The paper focuses on a practical photonic implementation of a 3D QRNG that is easier to deploy than cryogenic superconducting implementations. As any physical implementation is subject to various measurement errors, it is important to study theoretically and experimentally the type and role of errors in 3D QRNGs. In this paper, we will model the photonic 3D QRNG as an open quantum system, constructed as an arrangement of imperfect beam-splitters with a range of losses based on the fidelity of its components, and we will show that under certain conditions, the process remains within the scope of the Kochen-Specker Theorem, which guarantees maximum unpredictability.

1 Introduction

Random numbers play an essential role in many applications, such as cryptography. Currently, almost all practical applications rely on Pseudo-Random Number Generators (PRNGs), which have well-known pitfalls (predictability, short periods, and non-uniform distribution). This problem has motivated the development of several Quantum Random Number Generators (QRNGs), the best known being Quantis [29, 35]. To ensure a QRNG is suitable for security applications, either its outputs are postulated to be unpredictable based on the "intrinsic" indeterminism of quantum mechanics, and/or its unpredictability is tested with statistical tests. Both arguments are too weak to certify the quality of randomness.

3D QRNGs that generate provably maximally unpredictable strings by measuring localized value indefinite variables have been designed and studied [5]. These QRNGs do not use entanglement and are provably better than *any* PRNG [8]. In addition, robust experimental results probing the maximal unpredictability of quantum random strings generated by a 3D QRNG implemented with a superconducting transmon confirmed the theoretical results [9].

The photonic implementation of the 3D QRNG based on the located variant of the Kochen-Specker Theorem [4], studied in [6], does not require very low temperatures, so it is better suitable for practical applications than the 3D QRNG implemented with a superconducting transmon coupled to a microwave cavity attached to a dilution cryostat cooled down to the base temperature of $\sim$20 mK [30].

As any physical implementation is subject to various measurement errors, it is important to study, both theoretically and experimentally, the types and roles of errors in QRNGs. In what follows, we will study this problem for the photonic implementation of the 3D QRNG studied in [6] based on the located variant of the Kochen-Specker Theorem [4]. In this noisy environment, we can no longer assume that the operators used to model the photonic embodiment are unitary, hence we will model the 3D QRNG as an open quantum system, constructed as an arrangement of imperfect beam-splitters with a range of losses based on the fidelity of actual components, and we will show that under certain conditions, the process remains within the scope of the Kochen-Specker Theorem which guarantees maximum unpredictability.

We will also generalize the located variant of the Kochen-Specker Theorem [4] to unsharp measurements, by applying it to the pointer states.

[*]School of Computer Science, University of Auckland, New Zealand. Email: jagu688@aucklanduni.ac.nz, manuel.aguero15@gmail.com.
[†]School of Computer Science, University of Auckland, New Zealand. Email: c.calude@auckland.ac.nz, cscalude@gmail.com.
[‡]Department of Theoretical Physics, NIPNE–HH, Bucharest, Romania. Email: cristi.stoica@theory.nipne.ro, holotronix@gmail.com.

2 Notation and Definitions

A σ-algebra on a set $\mathcal{X}$ is a non-empty collection of subsets of $\mathcal{X}$ closed under complement, countable unions, and countable intersections. The *Borel space* associated to a topological space $\mathcal{X}$ is the pair $(\mathcal{X}, \mathcal{B})$, where $\mathcal{B}$ is the σ-algebra of Borel sets of $\mathcal{X}$. A *Borel function* is a measurable function between two Borel spaces, [28].

Let $\mathcal{H}$ be a Hilbert space and $\mathcal{B}(\mathcal{H})$ the algebra of bounded operators from $\mathcal{H}$ into itself. By $\mathcal{H}_N$ we denote an N-dimensional Hilbert space and $\mathcal{I}_N$ is the identity map on $\mathcal{B}(\mathcal{H})$. A quantum map ξ is a mapping from a space of density operators to another space of density operators $\rho \mapsto \rho' = \xi[\rho]$. A quantum map ξ is *positive* if it maps positive density operators ρ to positive density operators ρ' and it is *completely positive* if any trivial extension

$$\xi \otimes \mathcal{I}_N = \mathcal{B}(\mathcal{H}_d) \otimes \mathcal{B}(\mathcal{H}_N) \to \mathcal{B}(\mathcal{H}_d) \otimes \mathcal{B}(\mathcal{H}_N)$$

is *positive*.

3 Background

We denote the observable projecting onto the linear subspace spanned by a vector $|\psi\rangle$ as $\mathsf{P}_\psi = \frac{|\psi\rangle\langle\psi|}{\langle\psi|\psi\rangle}$. We then fix a positive integer $n > 2$ and let $\mathcal{O} \subseteq \{\mathsf{P}_\psi \mid |\psi\rangle \in \mathbb{C}^n\}$ be a non-empty set of one-dimensional projection observables on the Hilbert space $\mathbb{C}^n$.

A set $\mathcal{C} \subset \mathcal{O}$ is a *context* of $\mathcal{O}$ if $\mathcal{C}$ has n elements and for all $\mathsf{P}_\psi, \mathsf{P}_\phi \in \mathcal{C}$ with $\mathsf{P}_\psi \neq \mathsf{P}_\phi$, $\langle\psi|\phi\rangle$ =0. A *value assignment function* (on $\mathcal{O}$) is a partial function $v : \mathcal{O} \to \{0, 1\}$ assigning values to some (possibly all) observables in $\mathcal{O}$.[1] An observable $\mathsf{P} \in \mathcal{O}$ is *value definite* (under the assignment function v) if $v(\mathsf{P})$ is defined, i.e. $v(P) = 0$ or $v(P) = 1$; otherwise, it is *value indefinite* (under v). Similarly, we call $\mathcal{O}$ *value definite* (under v) if every observable $\mathsf{P} \in \mathcal{O}$ is value definite.

In what follows, we assume the following premises:

- **Admissibility.** This assumption guarantees agreement with quantum mechanics predictions. Fix a set $\mathcal{O}$ of one-dimensional projection observables in $\mathbb{C}^n$ and the value assignment function $v : \mathcal{O} \to \{0, 1\}$. Then v is admissible if the following two conditions hold for every context $\mathcal{C}$: a) if there exists $P \in \mathcal{C}$ with $v(P) = 1$, then $v(P') = 0$, for all $P' \in \mathcal{C} \setminus \{P\}$, b) if there exists $P \in \mathcal{C}$ with $v(P) = 0$, then $v(P') = 1$, for all $P' \in \mathcal{C} \setminus \{P\}$.
- **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 $v(\mathsf{P}_\psi) = 1$.

Theorem 1 (Located Kochen-Specker Theorem [1, 2, 4]) *Assume a quantum system prepared in the state $|\psi\rangle$ in a Hilbert space $\mathbb{C}^n$ with $n \geq 3$, and let $|\phi\rangle$ be any quantum state such that $0 < |\langle\psi|\phi\rangle| < 1$. Let $\mathcal{O}$ be a set of one-dimensional projection observables on $\mathbb{C}^n$ containing P_ψ and P_ϕ, and $v : \mathcal{O} \to \{0, 1\}$ a value asignment function. If the above three conditions are satisfied: i) admissibility, ii) non-contextuality and iii) eigenstate principle, then the projection observable P_ϕ is value indefinite.*

A measurement is *sharp* if it is perfectly accurate. Many important results in the study of quantum phenomena require sharp measurements. Nonetheless, experimentally, it is impossible to perform a perfectly precise measurement; working with *unsharp* measurements can significantly complicate and sometimes invalidate certain results.

Although an unsharp version of the Kochen-Specker exists [14, 13, 15, 19], so far, no unsharp equivalent of the localised variant of the Kochen-Specker Theorem has been formulated.

A major source of error in integrated photonics is photon loss, whether from escaping waveguides, from detector physical limitations, or from using a source that is not guaranteed to emit exactly one photon at a time. A way to model loss is to include additional modes in the model, such as waveguides that guide the lost photons to outputs not monitored by photon detectors. This implies an increase in the dimension of the Hilbert space, for example, by adding another waveguide to each of the three waveguides to model loss. This may be useful in some situations, but in fact, the problem takes care of itselfif we can guarantee that the source is single-photon: if the photon is lost, the detector will simply not detect a photon, and if two or more detectors click, we are dealing with an external photon, and we ignore the result. In practice, we can ignore undetected photons without affecting the quality of the QRNG. We will use heralded photons: in this

[1] The partiality of the function v means that $v(\mathsf{P})$ can be $0, 1$ or indefinite.

approach, the photons are generated in pairs, and the detection of the photon is verified by the simultaneous detection of its "twin". If only the twin photon is detected, we are dealing with a loss, which is automatically ignored anyway. If the twin photon is not detected, we will ignore the result, as it may be due to a stray photon.

We will make tests to ensure that the physically realized device is not significantly affected by losses or external noise. Such a test consists of coupling in series another device identical to this one but mirroring its behavior, so that it inverts the unitary transformation implemented by this one. The details are given in the article [10].

Another point of caution is that the noise and unsharpness may lead to violations of the inequality $0 < |\langle\psi|\phi\rangle| < 1$. This would make Theorem 1 inapplicable. The physical meaning of this inequality is that, for each of the detectors, there is always a non-vanishing probability that it detects the output photon. If one of them, corresponding to the observable P_ϕ, has zero probability to click, then we get $|\langle\psi|\phi\rangle| = 0$. If the other detectors have zero probability to click, $|\langle\psi|\phi\rangle| = 1$. Experiments should confirm that the inequality is consistently satisfied. But this is automatically ensured by the tests showing that the theoretical probabilities are obtained.

In this article, we study the behaviour of a QRNG [7] which selects a value of an indefinite observable in $\mathbb{C}^n$ and then measures it unsharply.

To this end, we will analyse each step of the QRNG.

4 First and Second Measurement Operator

4.1 First measurement operator

Choose an N-dimensional Hermitian operator with non-degenerate spectrum (that is, the operator has no linearly independent eigenvectors for the same eigenvalue). From Theorem 1, it follows that for any diagonalisable observable O with spectral decomposition $\mathsf{O} = \sum_{i=1}^{N} \lambda_i \mathsf{P}_{\lambda_i}$, where λ_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.

So ideally, we want an operator with eigenvalues corresponding to the standard Cartesian basis on dimension N; hence, the basis states correspond to the n inputs of the final measurement device (more generally, an operator satisfying the requirements up to a change of basis). We will use the first measurement operator to provide a value definite state (preparation state) so that, together with the second operator, it satisfies Theorem 1; that is, the eigenstates of the second measurement operator are neither orthogonal nor parallel to the preparation state.

Note that choosing a non-degenerate operator allows us to map each one of its distinct eigenvectors to each input port of a physical arrangement. Also, in [8], choosing the $\mathsf{S}_z = \mathsf{S}(0,0)$ operator conforms to the Cartesian standard basis and plays an important role when introducing imperfections.

4.2 Second measurement operator

Choose an N-dimensional Hermitian and unitary operator with distinct eigenvectors. This operator must be different from the first measurement operator.

To do the measurement of an observable represented by a Hermitian operator using an integrated photonic implementation, we apply a unitary transformation that maps the eigenbasis of the second measurement operator into the standard Cartesian basis implemented by the detectors of the N modes.

As an example for three dimensions, in [8], the first measurement was the generalised spin-1 observable

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

The $\mathsf{S}_x = \mathsf{S}(\frac{\pi}{2}, 0)$ operator was chosen to be the unitary second measurement operator U_x:

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

Note that the degeneracy of U_x is not a problem. To see this, it is useful to analyze the role of these operators and the non-contextuality assumption in the original formulation of the Kochen-Specker Theorem. First, we recall the following conditions for a value assignment map v.

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

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

$$\mathsf{A} = f(\mathsf{B}) \text{ and } \mathsf{A} = g(\mathsf{C}), \text{ with } [\mathsf{B}, \mathsf{C}] \neq 0. \tag{3}$$

Thus, from Quasi-linearity it follows that

$$v(\mathsf{A}) = f\big(v(\mathsf{B})\big) = g\big(v(\mathsf{C})\big). \tag{4}$$

As the sum of the projectors of a complete orthonormal set of states yields the identity operator and orthogonal projectors commute, the sum of their assigned values must be one. For one-dimensional degenerate operators, we obtain a single projector with value 1 and $N - 1$ zero-valued projectors in an N-dimensional Hilbert space. This leads to a contradiction when considering all complete sets of projectors, since we consider a projector to be 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 introduce some form of contextuality.

Note that the first measurement operator helps us prepare the measurement context with a corresponding value definite preparation state. Moreover note that all our Hermitian operators are self-adjoint (this property is also essential for our error handling framework), and degeneracy of an observable can then be simply understood as having more than one measurement basis (or measurement context) for an observable, and is not detrimental when localizing a value-indefinite observable (nor is it required in the localized variant of the Kochen-Specker Theorem). As Heisenberg said in [27],

"What we observe is not nature itself, but nature exposed to our method of questioning"

Taking the 3D-QRNG as an example, note that the first measurement operator prepares an eigenstate of a spin projector along a different axis from the second measurement operator, while satisfying Theorem 1. So, since eigenvalue relations are preserved for rotated states [14] (see section 6 for more details), all eigenstates of the sharp spin projectors used in this implementation are eigenstates of the unsharp spin projectors. Moreover, from Theorem 1 we see that for any diagonalisable observable O with spectral decomposition $\mathsf{O} = \sum_{i=1}^{n} \lambda_i \mathsf{P}_{\lambda_i}$ where λ_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, in general, we have the following result.

Theorem 2 *If the following conditions hold for a QRNG certified via value-indefiniteness:*

a) The preparation state is an eigenstate of the first measurement operator.

b) The second measurement operator does not commute with the first measurement operator.

c) The choice of preparation state ($|\psi\rangle$) satisfies the conditions of Theorem 1 with respect to each eigenstate ($|\phi\rangle$) of the second measurement operator.

Then, unsharp measurements do not affect the value indefiniteness of the outcomes.

Note that these results hold for the binary protocol proposed in [20] due to its unitary equivalence to the ternary protocol from [8]. The guarantee of value indefiniteness alone does not ensure that the distribution of outcomes is desirable. Nonetheless, the conditions above represent a natural arrangement that still allows for a good distribution of outcomes while facilitating a feasible physical implementation

For example in the ternary case, choosing the eigenstates $|\pm 1\rangle$ along the z-axis as preparation states lead to the distribution $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$. In the binary case we may choose the state $|1\rangle$ or $|0\rangle$ to obtain the distribution $\frac{1}{2}, \frac{1}{2}$ with the measurement operator

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

We have seen that, under certain conditions, value indefiniteness is unaffected by unsharp measurements. Nonetheless, it is important to examine the effects of experimental imperfections on the distribution of outcomes.

5 Limits of Measurements

Both imperfect technology and the laws of nature limit the practical realization of ideal quantum measurements. These limitations make our measurements unsharp, but, as we will see, they also provide a way to ensure the value indefiniteness even for unsharp measurements. The reason is that these limitations have the same fundamental origin as the Kochen-Specker Theorem.

Wigner [41, 17] showed that observables that can be realized as ideal measurements are rare, since they have to satisfy severe constraints due to the conservation laws. His proof concerns the pre-measurement, which is the unitary evolution of the measuring device interacting with the observed system, leading to the superposition of more possible outcomes, before the resolution achieved by invoking the Projection Postulate. Given that this is a unitary process, Wigner used the conservation laws to examine whether they constrain the realizability of accurate, repeatable measurements of sharp observables. It turns out that *sharp measurements cannot be both accurate and repeatable*. His result was generalized by Araki and Yanase [11], which is known as the Wigner-Araki-Yanase (WAY) Theorem [34].

In this context, accuracy is the requirement that the result of a measurement represents faithfully the value of the measured observable. Repeatability is the requirement that if a measurement is repeated, it yields the same result. For measurements used in preparation, repeatability is simply the accuracy of the preparation. A system prepared so that an observable A has a certain value a satisfies repeatability if, by measuring the observable A, the same value a is obtained. Repeatability directly relates to the Eigenstate principle from Section §3. For discrete observables, it is possible, in principle, to satisfy either accuracy or repeatability, but not both [34].

But Ozawa showed that measurements of non-discrete observables are irrepeatable even if we give up accuracy [37] (moreover, the limitation of repeatability, but also of accuracy, extends to discrete observables, if the Hamiltonian is non-negative [40]).

In particular, Ozawa's result implies that there is no way to choose the axis of a spin measurement with perfect accuracy. To measure a spin along a particular axis, one needs to align the Stern-Gerlach device's magnets along that axis. This requires tuning two real parameters, for example, the polar angle θ and the azimuthal angle φ. This would be impossible already in a classical world, because it requires controlling an infinite amount of information. But in a quantum world, there is an additional kind of obstruction. An intrinsic quantum source of unsharpness, in addition to noise and experimental errors, is the physical law itself. Ozawa's theorem on measurements of continuous or non-discrete observables says more than the classical fact that infinite precision is impossible in practice: it implies that, whatever axis one chooses, if one wants to verify how the axis is oriented, one will get a different result. In particular, since the measurement of the spin of an atom is based on its interaction with the magnetic field, it will not reflect with perfect accuracy the original set-up of the axis along which one intends to measure the spin.

Under these conditions, one may wonder whether it is still possible to ensure in practice that the conditions of the Located Kochen-Specker Theorem 1 can be satisfied. In the following Section §6 we will present previous results in this direction.

6 Breuer's Unsharp Kochen-Specker Theorem

In this section, we discuss Breuer's generalizations of the Kochen-Specker Theorem to unsharp spin 1 observables, notice their limits of applicability, and show that they are insufficient to certify the QRNG if the observable is unsharp.

Breuer presented his generalization of the Kochen-Specker Theorem to unsharp spin-1 observables in [13, 14]. He labeled the states by intermediate values using some thresholds δ (which he called *unsharpness tolerance*) and $1 - \delta$,

where $0.5 > \delta \geq 0$. Triads are then labeled with the values "almost true" (for eigenvalues $\geq 1-\delta$) and "almost false" (for eigenvalues $\leq \delta$), reducing the proof of the unsharp case to that of the sharp case. But the results of an experiment are always sharp values, even if the measurement is unsharp, because we read them from the pointer, which is a macroscopic object that displays sharp values. Macroscopically distinct states are orthogonal. So one does not observe the intermediate values assigned by the unsharp commuting observables; they remain "hidden". That is, the "unsharp eigenvalues" may be indefinite, but they remain unobservable. Also, there is a non-vanishing probability to get the wrong result reported, hence the use of the term "almost" in Breuer's articles [13, 14].

Before stating the Breuer Theorem, we need some notation. We denote the unsharp spin-1 observables, forming a positive operator-valued measure, by $F^{\mathbf{n},\epsilon}(i)$, $i \in \{-1,0,1\}$. The directions $\mathbf{m}$ are distributed with a density $w_{\mathbf{N},\epsilon}(\mathbf{m})$ around the direction $\mathbf{N}$ in space. The eigenvalues of the three positive operators $F^{\mathbf{z},\epsilon}(i)$ are three values from the set $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$. Breuer also assumed that the unsharpness is the result of the experimenter's ignorance of what spin observable, assumed to be sharp, is in fact measured,

Assumption 1 (Breuer's Unsharpness Assumption) *We can model unsharp measurements as sharp measurements of inaccurately known sharp observables.*

That is, the assumption is that the spin-1 measurement is sharp along *some* well-defined axis; we don't know with perfect accuracy which axis it is. This was the assumption of Breuer Theorems 3 and 4. For example, in [14], p. 197, right before Proposition 2, it is stated and justified as follows:

> [If the unsharp spin properties] transform covariantly under rotations, they are angular momentum properties and can be regarded as spin properties with the same justification as the sharp spin properties $\mathsf{P}_{n,i}$. This is in line with Weyl's idea of defining observables by their transformation properties under some kinematic group.

It can be formulated equivalently as the assumption that unsharp measurements are *post-processing* of projective measurements (PVMs), which implies that value indefiniteness is achieved. We can use this to build a genuinely random QRNG.

Assumption 1 is stated in Breuer's papers before he stated his theorem, but it is not restated in the theorem. However, the proof is based on it. That is, the POVM is assumed to commute, which allows simultaneous diagonalization. This is a strong restriction. We will discuss this below.

Theorem 3 (Breuer's Unsharp Kochen-Specker Theorem, version 1) *For any unsharpness tolerance $0.5 > \delta \geq 0$, if in an unsharp spin-1 measurement*

(A1) the densities of apparatus misalignments transform covariantly, i.e. if $w_{R\mathbf{n},\epsilon}(R\mathbf{m}) = w_{\mathbf{n},\epsilon}(\mathbf{m})$ for all rotations R, and

(A2) the measurement inaccuracy described by the densities $w_{\mathbf{n},\epsilon}(\mathbf{m})$ of the apparatus misalignments is so small that the unsharp spin observables $F^{\mathbf{n},\epsilon}(i)$ have, for all $i \in \{-1,0,1\}$, the eigenvalues α_1 and α_4 larger or equal to $1-\delta$, and the eigenvalues α_2 and α_3 smaller or equal to δ,

Then not all sharp spin observables in a Kochen-Specker set of directions can consistently be assigned approximate truth values in a non-contextual way.

As said, in addition to these assumptions, Breuer used Assumption 1 in his proof, discussed below.

In a subsequent article [15], Breuer avoids approximate truth values. Instead, he uses four numbers as labels: the four eigenvalues α_j shared by the three unsharp operators. In this version of his theorem, Breuer makes the very mild assumption that some eigenvalues are distinct. His newer theorem holds under weaker assumptions about measurement inaccuracy, but it still relies on Assumption 1.

Theorem 4 (Breuer's Unsharp Kochen-Specker Theorem, version 2) *If the densities of apparatus misalignments transform covariantly, $w_{R\mathbf{n},\epsilon}(R\mathbf{m}) = w_{\mathbf{n},\epsilon}(\mathbf{m})$, and if the density of misalignments is such that both α_1 and α_4 are different from both α_2 and α_3, then there is a finite set of intended measurement directions for which not all results of inaccurate measurements can be predetermined in a non-contextual way.*

We will first try to justify Breuer's assumption, but then we will find it too restrictive.

Quantum physicists who studied measuring devices realized that all that can be observed in a Stern-Gerlach experiment is, in fact, the place where the Silver atom hits the metallic plate. This is the pointer state. We observe the pointer state and, from this, infer something about the state of the Silver atom. While the impact mark may be very small, we will

call it "macroscopic" or "classical" because its observation does not require a quantum measuring device. Of course, it is a quantum state, not a classical one, but it behaves quite classically. Anyway, let us use the terms "macroscopic" or "macrostate" to refer to pointer states.

Remark 1 *Macroscopically distinguishable quantum states are orthogonal.*

This entails that the pointer observables are always sharp.

Another observation, based on Ozawa Theorem about measurements of continuous or non-discrete observables discussed in Section §5, is the following:

Remark 2 *There is always an inaccuracy in the direction of the axis along which we intend to measure the spin.*

Note that this also applies to photonic implementations or other implementations that require phase shifters to select the observable, since the phases are continuous parameters.

On the other hand, it was argued that Ozawa Theorem can be evaded by relative observables, for example, relative position [34, 33] or, in our case, relative orientation in space.

Together, Remarks 1 and 2 seem to justify Breuer's Assumption 1.

Alas, as noticed by Breuer himself, Assumption 1 can be satisfied only if the POVM is commutative, that is, any two of its constitutive positive operators commute. Unsharp measurements whose statistics are realizable as smeared (or fuzzy) sharp measurements are exactly the commutative POVMs [12, 18]. This implies that

Remark 3 *We cannot rely on Assumption 1 for unsharp measurements. Most unsharp measurements are irreducible to smeared sharp measurements. In most cases, there is no underlying sharp observable being fuzzified.*

Remark 4 *Moreover, even when the POVM is commutative, and hence it gives the same probabilities as a sharp measurement of an unknown observable, it does not imply that the unsharp measurement* really is *a sharp measurement of an unknown observable. The reason is that there are more ways to interpret the same POVM as a probabilistic distribution over definite states, as the distinction between* improper *and* proper mixtures *shows ([24], chapter 7.2, [25], chapter 8, [23], chapter 7). This makes it difficult to connect what was measured to what the pointer indicates, which is necessary to determine whether the pointer's state is due to value indefiniteness.*

In addition, other reasons prevent the use of the unsharp Kochen-Specker Theorems proved by Breuer to guarantee value indefiniteness. In Breuer First Theorem 3, even if the state is an eigenvector of $F^{\mathbf{n},\epsilon}(i)$, this does not guarantee the outcome. The "almost true" and "almost false" labeling is unobservable, so the value indefiniteness of the labeling has no determinate implication for the resulting outcome. In particular, it cannot be used to guarantee the quality of the numbers produced by a QRNG. In the second theorem given by Breuer, the state vectors are labeled as functions of the outcome and of the eigenvalues they have under the corresponding unsharp operator. But again, being an eigenvector of $F^{\mathbf{n},\epsilon}(i)$ does not guarantee the outcome. Even under Assumption 1, the outcome cannot tell us the actual sharp observable that was measured, and so we cannot tell us what eigenstate and what eigenvalue were really observed. Also, the 4 possible eigenvalues are shared among 3 operators. So even if they were pre-labeled, would this determine the outcome? If the label is α_1, α_2, or α_3, we can't know if the outcome is 1 or -1. Only if it is α_4 can we know that the outcome is 0. Therefore, even if Breuer Theorems are an important generalization of the Kochen-Specker Theorem, it seems that we cannot use them to certify randomness.

On the other hand, unsharp observables that cannot be understood as sharp measurements of unknown sharp observables already exhibit non-classicality, which can be understood as contextuality (Spekkens' "generalized contextuality") [38, 31]. This is precisely because the unsharp observable includes non-commuting positive operators. Interestingly, this understanding can reveal contextuality in single unsharp measurements and even in two-dimensional Hilbert spaces, for example, by treating the qubit SIC-POVM (symmetric, informationally complete, positive operator-valued measure) as an unsharp observable. Therefore, a deeper analysis may show that even in the unsharp case, the obtained pointer states arise from value indefiniteness, thereby complementing Breuer's results.

7 The Physicality of the Stinespring Dilation

In this article, we will use the Stinespring dilation to show that even if the measurement used by the QRNG is unsharp, it can be understood as a sharp measurement in a larger Hilbert space. This may seem like a mathematical trick in which we invoke a larger Hilbert space conveniently imagined for our purposes. Still, in this section, we will show that the larger Hilbert space has a solid physical basis. The Stinespring dilation is not in an imagined Hilbert space but is already

realized concretely and physically in the experimental setup. The usual way we understand measurements as being about the observed system obfuscates this fact, restricting the larger Hilbert space and leading to unsharpness, and weakening the connection between the value-indefinite properties and what the pointer indicates.

To this end, we will recall Ozawa's analysis of measurements and see that it concerns the observer-plus-pointer system as a whole. Ozawa's analysis reveals that the observable we intend to measure may be different from what we really measure, but even if it is unsharp, the combined observable, the one actually taking place, is sharp. It only seems unsharp if we ignore the larger system and trace out over its degrees of freedom, as is usually done when discussing quantum measurements. Therefore, it is physically justified to use the Stinespring dilation, as it actually occurs in the total system. We include an extension of the unsharp Located Kochen-Specker Theorem, which is more general than Breuer's, in that it doesn't assume only the restrictive kind of unsharpness, and it ensures that the observed values are indefinite, just by applying the sharp Located Kochen-Specker Theorem to the total system.

Let us start by stating the obvious objection that, by using the Stinespring dilation, we dilate in a fictitious extension of the Hilbert space of the physical systems under consideration.

Objection 1 *The construction of the dilation is theoretical, and to be of help in practice, it must be realized physically, because it makes no sense to invoke nonexistent contexts.*

Fortunately, the Stinespring dilation is not only justified but, in fact, how things happen in reality. The most realistic description of a measuring device is based on the Stinespring dilation. In the following, we will explain this. We will show that real-world measurements automatically realize the Stinespring dilation, which is known as the *measurement dilation*.

Let us remember the question "what does a Stern-Gerlach device measure?" At first sight, the obvious answer is that it measures the spin of the observed system, which may be, for example, a Silver atom or a neutron. But taking a closer look revealed that it measures the position where the observed Silver atom hits the metallic plate.

Recall that Wigner examined the spin measurement and concluded that such a measurement cannot be both accurate and repeatable (that is, undisturbing) [17]. He then showed that, if the measuring device contained an infinite number of particles, the ideal of a measurement would be attainable in principle. He also proposed other ways to distinguish between the two possible spin values by extending the set of possible outcomes to include an "error" outcome and discarding such results. Unfortunately, this idea cannot be used in practice to discard outputs (in particular, outputs of the QRNG) that are caused by noise or experimental error, since this would require knowing which unsharp observable is produced as a result of their effects and building the measuring device accordingly.

But this situation is not at all that bad for us, as we shall see.

Remark 1 is of extreme importance to understand what observable is actually measured in a quantum measurement. We may *intend* to measure a particular observable, and design and build a device to do this job, but ultimately, we have to track back from the pointer state to infer what the actual observable was. This is explained for example in [37], [18] Section §7.7, and [33] Section §2.2. We evolve the combined state backward in time, including the measuring device (and, if needed, the environment) and the observed system, and then trace out the measuring device. What remains is the actually measured observable of the system under observation.

In [37], Ozawa showed that a measuring device can be constructed, abstractly, for any observable E. His construction, called *measurement dilation*, is based on *Naĭmark Dilation Theorem* [36], which can be seen as a particular case of *Stinespring Dilation Theorem* [39].

Let the observed system be S, and the measuring device be A, with the respective Hilbert spaces $\mathcal{H}_S$ and $\mathcal{H}_A$, and let $\mathcal{H} = \mathcal{H}_S \otimes \mathcal{H}_A$. Let $\mathsf{Z} \in \mathcal{L}(\mathcal{H}_A)$ be the pointer observable, taken to be a Hermitian operator because we assume it to be sharp, based on Remark 1. Let us detail this for the measurement of an N-dimensional system, assuming that we measure the observable $\mathsf{O} = \sum_{i=1}^{N} \lambda_i \mathsf{P}_{\lambda_i}$ as in Section §4, where $|\lambda_i\rangle_S$ are the eigenstates of O and $\mathsf{P}_{\lambda_i} = |\lambda_i\rangle_S \langle\lambda_i|_S$. Let $|\text{ready}\rangle_A$ and $|\zeta_1\rangle_A, \ldots, |\zeta_N\rangle_A$ be the eigenvectors of the pointer state. Let $|\psi\rangle_S = \sum_{i=1}^{N} a_i |\lambda_i\rangle_S$ be the initial state of the observed system. Then, the pre-measurement consists of entangling the pointer of the measuring device with the observed system, by applying the evolution operator U:

$$|\psi\rangle_S \otimes |\text{ready}\rangle_A \overset{\mathsf{U}}{\mapsto} \sum_{i=1}^{N} a_i |\lambda_i\rangle_S \otimes |\zeta_i\rangle_A , \tag{6}$$

where $a_i = \langle\lambda_i|\psi\rangle_S$.

But this is true if the measurement is sharp. In general, this is not the case, and this is precisely the subject of this article.

The pointer is a subsystem of the measuring device, but an observable of a subsystem is also an observable of the full system; we will not need to refine this further in the following. Similarly, on the total system $S+A$, the pointer observable is $\mathsf{I}_S \otimes \mathsf{Z}$. The environment, including other systems that may affect our measurements, must also be considered. For simplicity, we will consider it included in the measuring device, since it indeed affects the measurement. Again, there is no need to treat it separately, and this is not even the right way, because we will describe a measurement that is not necessarily ideal. We assume that the interaction between the measuring device and the observed system begins at time t_0, and that the pointer indicates the outcome starting at time $t_1 > t_0$, when the measurement ends. Let $\widehat{\mathbf{U}}_{t_1,t_0}$ denote the unitary evolution operator of the combined system during the measurement.

Let $\varrho \in \mathcal{T}(\mathcal{H}_A)$ be the "ready" state of the measuring device, and $\rho \in \mathcal{T}(\mathcal{H}_S)$ the state of the observed system, at $t = t_0$. Let the measured observable be the *positive operator-valued measure* (POVM) $E : \mathcal{E} \to \mathcal{L}(\mathcal{H}_S)$, where $\mathcal{E}$ is a σ-algebra of subsets of a set Ω, representing the space of possible outcomes resulting from the measurement of E. The POVM E should satisfy the following *probability reproducibility condition* [16, 18]:

$$\mathrm{tr}\left(\rho E\left(X\right)\right) = \mathrm{tr}\left(\widehat{\mathbf{U}}_{t_1,t_0}\rho \otimes \varrho \widehat{\mathbf{U}}_{t_1,t_0}^{\dagger} \mathsf{I}_S \otimes Z(X)\right), \tag{7}$$

where $X \in \mathcal{E}$ and Z is the sharp observable $\mathsf{Z}(X)$ seen as a POVM. Let us assume that the "ready" state of the pointer is pure, $\varrho = |\phi\rangle\langle\phi|$, where $|\phi\rangle \in \mathcal{H}_A$. We define the isometric embedding

$$V_\phi : \mathcal{H}_S \to \mathcal{H}_S \otimes \mathcal{H}_A, V_\phi |\psi\rangle = |\psi\rangle \otimes |\phi\rangle, \tag{8}$$

for any $|\phi\rangle \in \mathcal{H}_S$. Then, E can be uniquely extracted from equation (7),

$$E\left(X\right) = V_\phi^\dagger \widehat{\mathbf{U}}_{t_1,t_0}\left(\mathsf{I}_S \otimes Z(X)\right)\widehat{\mathbf{U}}_{t_1,t_0} V_\phi. \tag{9}$$

This is a particular case of the Stinespring construction for the observable E, realized as the pointer observable $\mathsf{I}_S \otimes Z(X)$, evolved back in time to t_0. It is called the *measurement dilation*.

Remark 5 (Practical realizability of sharp measurements) *In practice, it is difficult, if not impossible, to build an ideal measuring device for an intended observable E, so in fact equation (9) should be understood rather as a definition of what observable a particular measuring device measures.*

Remark 6 (Unsharpness of the observable for the observed system) *Equation (9) implies that, in fact, the measurements are usually unsharp when understood as being about the observed system. Even though Remark 1 implies that the pointer observable itself is sharp, the pointer state indicates* an unsharp observable E of the observed system S, *because of the restriction done by the isometric embedding $V_\phi : \mathcal{H}_S \to \mathcal{H}_S \otimes \mathcal{H}_A$ from equation (8).*

Remark 7 (The physicality of the Stinespring dilation) *At the same time, the isometric embedding $V_\phi : \mathcal{H}_S \to \mathcal{H}_S \otimes \mathcal{H}_A$ from equation (8) and taking the trace in equation (7) do not represent physical processes, but they describe the observer's inference about the observed system S, and the observer's* ignorance *of the total state. In reality, the pointer observable corresponds to the observable $\widehat{\mathbf{U}}_{t_1,t_0}\left(\mathsf{I}_S \otimes Z(X)\right)\widehat{\mathbf{U}}_{t_1,t_0}$, which, being a unitary transformation of the sharp pointer observable $\mathsf{I}_S \otimes Z(X)$, it is sharp too. This is important because it shows that the Stinespring dilation is realized in practice in every quantum measurement. It does not have to be realized in an imagined auxiliary Hilbert space, because it is already realized physically. Still, the standard descriptions of the measurement restrict what the pointer state tells us to the observed system S.*

8 The Problem of the Overlap of Unsharp Outcomes

Another potential objection to using the Stinespring Dilation Theorem, due to the unsharpness, is that

Objection 2 *The unsharpness of the measurements leads to overlap between the probability distributions of the possible outcomes, and we need to ensure it does not compromise the quality of randomness.*

This overlap is, in fact, because in practice the measurements are unsharp, but this is true only if we consider the observable to be restricted to the observed system, and not to be an observable of the whole system.

As an extreme example of such an overlap, note that, for an ideal 3D-Photonic QRNG, random numbers are generated. Still, the total unprojected state vector is determined by the unitary evolution and therefore does not exhibit randomness. This means that the randomness of the three alternative outcomes cancels out in the unprojected state, which is what

we get if we lose track of which outcome obtains, for example, by using a single detector for all three possible modes. This corresponds to replacing the projective measurement in the 3D-Photonic QRNG with the trivial POVM consisting solely of the identity operator. While this is an extreme example that completely washes out the value of indefiniteness, it illustrates the problem posed by unsharpness.

However, once we understood that the pointer observable is sharp and that the observed system is used to put the pointer state into various mutually orthogonal states, we realized that we do not actually care about the real state of the observed system. Our random numbers are generated by the detectors in response to the photons, not by the photons themselves. It can be argued that since the detectors have to reset between measurements, this prevents performing the measurements alongside other compatible measurements. Therefore, one cannot speak of the Kochen-Specker Theorem in this case [26]. This is true if we want to test the theorem, for example, for violations of inequalities. But all we need is to ensure value-indefiniteness for a single measurement, guaranteed by counterfactual, not by actual measurements. For this reason, the failure of detectors to reset exactly in the same state does not affect value indefiniteness, because alternative observables needed for this exist in principle in the extended Hilbert space, which is physical, even if they are not *de facto* measured. Another argument against POVM contextuality [26] is that the dilation is not unique. However, in our case, we refer to Ozawa's measurement dilation, which is physical and uniquely given by the pointer observable. So we can focus only on the pointer observable, and apply the Localized Kochen-Specker Theorem to its observation, and not merely to the measurement of the observed system.

In the Ozawa measurement dilation, the observable measured may be unsharp, but the total system undergoes a sharp measurement; see equation (9) and its discussion. Note that a sharp measurement can still be performed on an impure state, and can still result in an impure state, see, for example, the case of the EPR experiment. The reason is that a reduced density operator can also be projected, and if the observable is a degenerate operator, the state may remain impure. Hence, Ozawa's measurement dilation does not guarantee a pure state. We assume the existence of a larger system that includes the observed system and the pointer, and that the larger system is in a pure state. Then, if the observed system was not in the same state as the one resulting from the pre-measurement, $|\langle\Psi|\Phi\rangle| < 1$. At the same time, since $|\Phi\rangle$ is obtained by a non-trivial projection from $|\Psi\rangle$, the inequality $|\langle\Psi|\Phi\rangle| > 0$ also holds.

We now list some assumptions that will allow us to generalize Theorem 1, and explain why they are automatically satisfied.

1. There exists, physically, a larger system that includes the observed system and the pointer, and whose total state is pure before and after the measurement. This makes sense because in most formulations of quantum mechanics, at least the total state of the universe is assumed to be a pure state. We denote by $\mathcal{H}_A$ the Hilbert space of the pointer, by $\mathcal{H}_S$ the Hilbert space of the observed system and whatever environment needs to be included, and by $\mathcal{H} = \mathcal{H}_S \otimes \mathcal{H}_A$ the total Hilbert space.

2. The preparation and pre-measurement result in a total state of the combined system represented by the state vector $|\Psi\rangle$.

3. Immediately after the measurement, the system can be found with nontrivial probabilities in at least two macroscopically distinct states $|\Phi\rangle$ and $|\Phi'\rangle$, both eigenstates of the extended pointer observable $\mathsf{I}_S \otimes \mathsf{Z}$.

The last condition shows that a nontrivial projection occurred. The reason is that, from the above assumptions, $|\Psi\rangle = a\,|\Phi\rangle + a'\,|\Phi'\rangle + \ldots$, where $|\Phi\rangle\,, |\Phi'\rangle \ldots$ are mutually orthogonal, being macroscopically distinct, and at least $a = \langle\Phi|\Psi\rangle$ and $a' = \langle\Phi'|\Psi\rangle$ are not 0. Then, this implies that $|\langle\Phi|\Psi\rangle| < 1$, and from

$$1 = |\langle\Psi|\Psi\rangle|^2 = |\langle\Psi|\Phi\rangle|^2 + \left|\langle\Psi\middle|\Phi'\rangle\right|^2 + \ldots > |\langle\Psi|\Phi\rangle|^2 \tag{10}$$

one obtains

$$0 < |\langle\Psi|\Phi\rangle| < 1. \tag{11}$$

For more clarity, let us see how this works in the case of a sharp measurement. For sharp measurements, $|\Psi\rangle = \sum_{i=1}^{N} a_i\,|\lambda_i\rangle_S \otimes |\zeta_i\rangle_A$ and $|\Phi\rangle = |\lambda_k\rangle_S \otimes |\zeta_k\rangle_A$ as in equation (6). Then, a way to ensure $0 < |\langle\Psi|\Phi\rangle| < 1$ is if $a_k = \langle\lambda_k|\psi\rangle \neq 0$ and at least another component $a_j \neq 0$, where $j \neq k$. Then, $|\Phi'\rangle = |\lambda_j\rangle_S \otimes |\zeta_j\rangle_A$. This is what happens in the sharp version, Theorem 1. But the same condition (11) can be ensured regardless of the state of the observed system, because $\langle\zeta_k|\zeta_j\rangle_A \neq 0$, which is satisfied because $|\zeta_k\rangle$ and $|\zeta_j\rangle$ represent macroscopically distinct states. In other words, the same value of indefiniteness obtained by applying Theorem 1 to the states of the observed system can be obtained by applying Theorem 1 to the states of the pointer. But this condition is satisfied by the pointer states even if the measurement is not sharp, because even in this case the macroscopically distinct pointer states $|\Phi\rangle$ and

$|\Phi'\rangle$ are orthogonal, but $|\Psi\rangle$ is a nontrivial linear combination of them. Then, the condition $0 < |\langle\Psi|\Phi\rangle| < 1$ can be validated simply by verifying empirically that the measurement sometimes yields $|\Phi\rangle$, and sometimes yields $|\Phi'\rangle$.

Under these assumptions, we can prove the following result by simply applying Theorem 1 to the pointer states.

Theorem 5 (A Located Kochen-Specker Theorem for unsharp measurements) *For possibly unsharp measurements, assuming that identically prepared systems result in nontrivial probabilities in the macroscopically distinct total pointer observables $|\Phi\rangle$ and $|\Phi'\rangle$, the observable P_Φ is value indefinite.*

Proof. As we have seen, these conditions ensure that $0 < |\langle\Psi|\Phi\rangle| < 1$. Then, we can apply Theorem 1 to the pointer states, from which it follows that the total observable P_Φ is value indefinite. □

Remark 8 *Can we extend the conclusion of Theorem 5 to the reduced observable that we measure on the observed system? We don't know, but we do not need it. The whole point of Theorem 5 was to avoid the necessity to extend value indefiniteness to unsharp observables. This allows us to evade Objection 2. Recall from Section §7 that what we can observe is the pointer observable $Z(X)$ of the measuring device, and not directly an observable of the observed system. The pointer observable $Z(X)$ is sharp and extends to the sharp observable $\mathsf{I}_S \otimes Z(X)$ on the total system, containing the observed system and the measuring device. To obtain the measured observable, we apply backward the time evolution and obtain $\widehat{\mathbf{U}}_{t_1,t_0}\,(\mathsf{I}_S \otimes Z(X))\,\widehat{\mathbf{U}}_{t_1,t_0}$ as in equation (9). To obtain the measured observable $E(X)$ of the system that we intended to observe, we apply to this the isometric embedding V_ϕ from equation (8) and its adjoint $V_\phi^\dagger$, as in equation (9). This is the inverse operation of the dilation. If we are interested in the observed system, what we measure in fact is the observable $E(X)$, regardless of what observable we intended to measure. But what we measure sharply is only the pointer observable $\mathsf{I}_S \otimes Z(X)$. And this is perfect for our analysis of the unsharp measurements, since all measurements, sharp or unsharp, are modeled by the Ozawa measurement dilation described in Section §7. To use the results of the measurement as random numbers, all we need is to ensure the value indefiniteness of the observable P_Φ, where $|\Phi\rangle$ is an eigenvector of $\mathsf{I}_S \otimes Z(X)$, and not of the observable $E(X)$. This is what we achieve in Theorem 5. Whether or not this implies the value indefiniteness of the observable $E(X)$ is irrelevant, as long as we have shown that the projector associated with the pointer state is value indefinite. Hence, its measurement is a random digit.*

9 The Effect of Experimental Imperfection in the Distribution of Outcomes

We illustrate the effect of experimental imperfection in the distribution of outcomes, and the solution based on the Stinespring dilation, for a 3D QRNG.

One of the main ways to implement beamsplitters in integrated photonics is to use *multimode interferometers* (MMIs). Here, single-mode waveguides are coupled to a multimode fiber with a specified number of allowed modes. Moreover, phase modulation can be achieved by using a thermal phase shifter. For example, a thermal shifter may be implemented in silicon devices by connecting a resistive silicon strip adjacent to the waveguide to a metal pad, where a voltage is applied to control the temperature.

Thus, by integrating two MMIs (acting as balanced beamsplitters) with a thermal phase shifter, we may construct a *Mach-Zehnder Interferometer* (MZI).

This solution offers two main advantages when implementing our device.

1. MMI's performance is close to that of an ideal balanced beamsplitter.
2. A MZI characterized by a tunable phase-shifter can be mapped onto a beam splitter with tunable reflectivity.

Thus, the first advantage allows us to obtain the preparation state described by the first measurement operator, and, together with the second advantage, we can design a physically realizable arrangement of Mach-Zehnder interferometers that implements our desired unitary operator.

Thus, MZIs are a suitable element to model errors in a photonic implementation. An MZI is composed of two balanced beamsplitters and two phase shifters (one internal and one external),

$$\begin{aligned}\mathsf{M} &= \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} e^{i\phi_2} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} e^{i\phi_1} & 0 \\ 0 & 1 \end{pmatrix} \\ &= ie^{\frac{i\phi_2}{2}} \begin{pmatrix} e^{i\phi_1}\sin\frac{\phi_2}{2} & \cos\frac{\phi_2}{2} \\ e^{i\phi_1}\cos\frac{\phi_2}{2} & -\sin\frac{\phi_2}{2} \end{pmatrix}\end{aligned} \tag{12}$$

Thus, we may introduce loss by setting different angles to the beam splitters as follows:

$$\widetilde{\mathsf{M}} = \begin{pmatrix} \cos\beta & i\sin\beta \\ i\sin\beta & \cos\beta \end{pmatrix} \begin{pmatrix} e^{i\phi_2} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \cos\alpha & i\sin\alpha \\ i\sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} e^{i\phi_1} & 0 \\ 0 & 1 \end{pmatrix} \tag{13}$$

Letting

$$\begin{cases} x &= \cos(\alpha-\beta)\sin(\frac{\phi_2}{2}) - i\cos(\alpha+\beta)\cos(\frac{\phi_2}{2}) \\ y &= \sin(\alpha+\beta)\cos(\frac{\phi_2}{2}) - i\sin(\alpha+\beta)\sin(\frac{\phi_2}{2}) \end{cases} \tag{14}$$

we have

$$\widetilde{\mathsf{M}} = ie^{\frac{i\phi_2}{2}} \begin{pmatrix} e^{i\phi_1}x & y \\ e^{i\phi_1}y & -x \end{pmatrix}. \tag{15}$$

Similarly, the phase values will be imprecise in the real case scenario, so adjusting $\widetilde{\mathsf{M}}$ to $\widetilde{\mathsf{M}}(\phi_1', \phi_2')$ and solving for $\widetilde{\mathsf{M}}(\phi_1', \phi_2') = \mathsf{M}$ describes a restriction induced by errors. For example, for ϕ_2 we get

$$\phi_2' = 2\arcsin\sqrt{\frac{\sin^2(\frac{\phi_2}{2}) - \cos^2(\alpha+\beta)}{\cos^2(\alpha-\beta) - \cos^2(\alpha+\beta)}}. \tag{16}$$

That is,

$$2\left|\alpha+\beta-\frac{\pi}{2}\right| < \phi_2 < \pi - 2|\alpha-\beta|. \tag{17}$$

Note that this type of imperfections may be addressed by the use of additional phase shifters to obtain a Hermitian operator $\widetilde{\mathsf{U}}$ with high fidelity, without affecting the result from the previous sections. Now, there is an additional consideration we must take during the two-dimensional decomposition of our measurement operator.

For example, for the unitary matrix U_x from equation (2), in the 3-dimensional case we have $\mathsf{U}_x = \mathsf{B}_{1,2}^{-1} \cdot \mathsf{B}_{2,3} \cdot \mathsf{D} \cdot \mathsf{B}_{1,2}$ where

$$\begin{aligned} \mathsf{B}_{1,2} &= \begin{pmatrix} \sqrt{\frac{2}{3}} & \frac{1}{\sqrt{3}} & 0 \\ \frac{i}{\sqrt{3}} & -i\sqrt{\frac{2}{3}} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathsf{B}_{2,3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{i\sqrt{3}}{2} \\ 0 & \frac{i\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \\ \mathsf{B}_{1,2}^{-1} &= \begin{pmatrix} \sqrt{\frac{2}{3}} & -\frac{i}{\sqrt{3}} & 0 \\ \frac{1}{\sqrt{3}} & i\sqrt{\frac{2}{3}} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \mathsf{D} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}. \end{aligned} \tag{18}$$

These matrices are generated through Clements' unitary decomposition [22], [21], where off diagonal elements of U_x are nulled by applying transformations $\mathsf{T}_{m,n}$ by beam-splitters between channels m and n with $m = n-1$ such as the resulting $\mathsf{B}_{1,2}$, $\mathsf{B}_{2,3}$ and $\mathsf{B}_{1,2}^{-1}$ matrices. Nonetheless, in a practical setting, imperfections in the MZI interferometers used to carry out these transformations make it impossible to realize a perfect cross ($s = 0$) and bar ($s = \infty$) states where s is the splitting ratio. If θ is the ideal angle for each beam splitter in a MZI, then with $\theta + \sigma = \alpha$ and $\theta + \rho = \beta$ we have that the splitting ratio is restricted by $|\sigma+\rho| \leq |s| \leq \cot|\sigma-\rho|$ where σ, ρ are the error offsets. In the bar state, the inputs connect directly to the outputs, while in the cross state, each input is directed to the opposite output. So, if a given nulling step falls within these "forbidden regions, nulling is imperfect, and an off-diagonal residual prevents perfect diagonalization of the matrix, leading to an "uncorrectable" error. For example, the matrix $\mathsf{B}_{1,2}$ has a splitting ratio of $s = \mathsf{T}_{1,1}/\mathsf{T}_{1,2} = \sqrt{\frac{2}{3}}\Big/\frac{1}{\sqrt{3}} = \sqrt{2}$ so it does not fall into a "forbidden" region. Nonetheless, this restriction on splitting ratios means that other unitarily equivalent choices of operators may offer very desirable properties at the expense of greater sensitivity to errors.

Let

$$\mathsf{A} = \frac{1}{\sqrt{2}} \begin{pmatrix} \sqrt{2} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{pmatrix}, \mathsf{B} = \frac{1}{2} \begin{pmatrix} \sqrt{2} & \sqrt{2} & 0 \\ 1 & -1 & -\sqrt{2} \\ 1 & 1 & -\sqrt{2} \end{pmatrix}. \tag{19}$$

	phase	angle
A	0	$\frac{\pi}{2}$
	π	$\frac{\pi}{6}$
	$-\pi$	$\frac{\pi}{2}$
B	π	$\frac{\pi}{6}$
	$-\frac{\pi}{2}$	$\frac{\pi}{2}$
	0	$\frac{\pi}{6}$

Table 1: angles and phases for operators A and B.

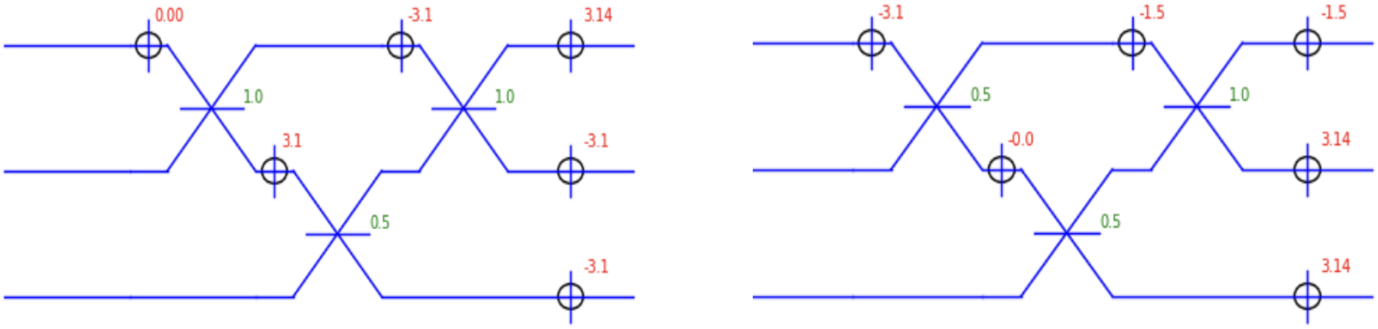

Figure 1: A and B arrangements.

Now consider the unitarily equivalent operator $\mathsf{U}' = \mathsf{AB}$. We may implement this operator by concatenating two U_x interferometers and adjusting their angles and phases as in Table 1. We can use this table to see that its splitting ratios fall into a "forbidden" region.

However, there are ways to mitigate this issue at the cost of additional complexity; for example, we may displace the cross and bar states by adding a splitter at the input, performing the transformation $s \to (s + i\tan\eta)/(1 + is\tan\eta)$. Alternatively, we may find a unitarily equivalent operator with the same output distribution to circumvent this issue.

We are now ready to examine the overall effect of errors on the outcome distribution.

Consider the completely positive map (CP-map)

$$\Phi : L(\mathcal{H}) \to L(\mathcal{H}), \varrho : \mathcal{H} \to \mathcal{H}, Tr(\varrho) = 1, \varrho \geq 0 \tag{20}$$

where ϱ is a positive semi-definite operator acting on the Hilbert space $\mathcal{H}$ such that

$$\Phi(\varrho) = \sum_i \mathsf{K}_i \varrho \mathsf{K}_i^\dagger \text{ and } \sum_i \mathsf{K}_i^\dagger \mathsf{K}_i \leq I. \tag{21}$$

Note that for $\varrho^2 = \varrho$, we have the projection operator; that is, there exists a $|\psi\rangle \in \mathcal{H}$ such that $\varrho = |\psi\rangle\langle\psi|$.

We call $\{\mathsf{K}_i\}$ a Kraus operator which need not be unitary (note that if it is unitary we have $\varrho \mapsto \mathsf{U}\varrho\mathsf{U}^\dagger$).

Theorem 6 (Stinespring dilation [39]) *Let A be a $\mathcal{C}^*$-algebra, $\mathcal{H}$ be a Hilbert space and $B(\mathcal{H})$ be bounded operator on $\mathcal{H}$. Then, for every CP-map $\Phi : A \to B(\mathcal{H})$ there exist a Hilbert space $\mathcal{K}$ and a unital *-homomorphism $\varphi : A \to B(\mathcal{K})$ such that $\Phi(a) = \mathsf{V}^*\varphi(a)\mathsf{V}$, where $\mathsf{V} : \mathcal{H} \to \mathcal{K}$ is a bounded operator.*

So a CP-map can be expressed as a map $\mathsf{V}^*(\cdot)\mathsf{V}$ in a "larger space". Thus, we can see a quantum channel realized by partial tracing a unitary operator acting on a potentially larger Hilbert space. In other words, a CP-map acts as a partial observation of a unitary operation in a larger space where

$$\Phi(\varrho) = tr_{\mathcal{K}}\{\mathsf{V}(\varrho \otimes |E\rangle\langle E|)\mathsf{V}^\dagger\} \tag{22}$$

where $|E\rangle$ is an ancilla state. So, since $\widetilde{\mathsf{U}}$ is Hermitian, we can describe it as a non-unitary Kraus operator interacting with the environment in a larger space that follows a unitary evolution.

Note that the unitary equivalence of an operator allows us to reduce any operators with the same eigenvalues to the U_x case, thus generalizing this result to any unitarily equivalent operator and its corresponding decomposition. In the case of

the operator with binary outcomes U', this allows us to dismiss altogether the outcomes from the probability zero output port, where the forbidden regions arising from the splitting ratios will make this a non-zero branch by a small margin. By doing so, at the expense of slower bit-generation speed, we may adjust the "real" angles and phase values to mitigate bias in the two main output ports while retaining the indefiniteness of the values.

To model the real distribution of outcomes, we can describe the measurement performed by $\widetilde{\mathsf{U}}$ as a completely positive map acting on a noisy quantum channel

$$\xi(\rho) = \sum_k \mathsf{E}_k \rho \mathsf{E}_k^\dagger, \tag{23}$$

where ρ is our density operator and E_k are the Kraus operators describing the effect of errors. To broadly model the possible effect of errors, we set E_k to represent the depolarising channel on a single qutrit. That is, with some probability, the qutrit remains intact or undergoes a bit flip and/or phase flip error.

Let

$$\begin{gathered}
\mathsf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega \end{pmatrix},\ \mathsf{B} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \\
\mathsf{C} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},\ \mathsf{D} = \mathsf{C}^\dagger,\ \mathsf{E} = \begin{pmatrix} 0 & \omega & 0 \\ 0 & 0 & \omega^2 \\ 1 & 0 & 0 \end{pmatrix} \\
\mathsf{F} = \begin{pmatrix} 0 & 0 & \omega^2 \\ 1 & 0 & 0 \\ 0 & \omega & 0 \end{pmatrix},\ \mathsf{G} = \begin{pmatrix} 0 & \omega^2 & 0 \\ 0 & 0 & \omega \\ 1 & 0 & 0 \end{pmatrix},\ \mathsf{H} = \begin{pmatrix} 0 & 0 & \omega \\ 1 & 0 & 0 \\ 0 & \omega^2 & 0 \end{pmatrix}
\end{gathered} \tag{24}$$

where ω is the third root of unity. Let p be the expected likelihood of errors, estimated by assessing the efficiency of the physical implementation, for example, by conducting the test described in [10]. Then, the depolarising channel is given by the Kraus operators

$$\mathsf{E}_0 = \sqrt{1-p}\mathsf{I}_3, \mathsf{E}_1 = \sqrt{\frac{p}{8}}\mathsf{D}, \mathsf{E}_2 = \sqrt{\frac{p}{8}}\mathsf{B},$$

$$\mathsf{E}_3 = \sqrt{\frac{p}{8}}\mathsf{C}, \mathsf{E}_4 = \sqrt{\frac{p}{8}}\mathsf{E}, \mathsf{E}_5 = \sqrt{\frac{p}{8}}\mathsf{F}, \mathsf{E}_6 = \sqrt{\frac{p}{8}}\mathsf{G}, \mathsf{E}_7 = \sqrt{\frac{p}{8}}\mathsf{H}, \mathsf{E}_8 = \sqrt{\frac{p}{8}}\mathsf{A}.$$

So

$$\xi(\rho) = \sum_k \mathsf{E}_k \rho \mathsf{E}_k^\dagger = (1-p)\rho + \frac{p}{8}\left(\mathsf{A}\rho\mathsf{A}^\dagger + \mathsf{B}\rho\mathsf{B}^\dagger + \ldots + \mathsf{H}\rho\mathsf{H}^\dagger\right). \tag{25}$$

Then, for a qutrit prepared in state $|1\rangle$ we have

$$(1-p)\,|1\rangle\langle 1| + \frac{p}{8}\left(3\,|-1\rangle\langle -1| + 2\,|1\rangle\langle 1| + 3\,|0\rangle\langle 0|\right). \tag{26}$$

Thus, we get the outcome probabilities:

$$\begin{aligned}
\langle 1_x|\,\xi(\rho)\,|1_x\rangle &= \frac{1}{4} + \frac{3p}{32}, \\
\langle 0_x|\,\xi(\rho)\,|0_x\rangle &= \frac{1}{2} - \frac{3p}{16}, \\
\langle -1_x|\,\xi(\rho)\,|-1_x\rangle &= \frac{1}{4} + \frac{3p}{32}.
\end{aligned} \tag{27}$$

Thus, the conditions for the localized Kochen-Specker Theorem are still met, and we can estimate the outcome probabilities by setting the expected error rate p. We can apply this same method to the binary case and any valid preparation state. That is, for

$$\mathsf{U}' = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & -1 \\ 0 & 0 & 0 \end{pmatrix}, \tag{28}$$

with preparation states $|1\rangle$ or $|0\rangle$, $\mathsf{U}\xi(\rho)\mathsf{U}^\dagger$ yields an outcome in either of the first two outputs ports with probability $\frac{1}{2} \pm \frac{3p}{16}$.

Note that whenever the preparation states belong to the orthonormal basis states, we have that $\xi(\rho)$ is diagonal. Moreover, the unitary decomposition process nullifies the diagonal elements at each step. Thus, by measuring the detectors' efficiency and applying this analysis component-wise during the unitary decomposition, we may manipulate the bias using additional phase shifters in the outputs, in a similar way to how we may displace the cross and bar states. In this manner, one can reduce and distribute the bias as needed to ensure we remain within the localized Kochen-Specker bounds.

10 Conclusions

Despite errors, we can ensure that the behavior of this class of QRNGs corresponds to a Hermitian process, which is a completely positive map acting on a quantum channel. The measurement operator is no longer unitary, but it can be modeled as a non-unitary operator that interacts with the environment in a larger unitary system.

Of course, it is essential to ensure the quality of the QRNG by having experimental ways to verify that the implementation is as accurate and as close to unitarity as possible. The symmetry inverter testing device will verify the unitarity of the QRNG [10]. In combination with the verification of the reproducibility of the theoretically predicted probabilities, and the results that the Kochen-Specker Theorem 1 is robust under unsharpness, the viability of the QRNG can be ensured.

In addition, the preparation stage allows the use of any state that is not parallel nor orthogonal to an eigenstate of the second measurement operator [4]. This permits flexibility in choosing operators that preserve the value indefiniteness certification under unsharp measurements. Hence, under certain conditions, the process remains within the scope of the Kochen-Specker Theorem, guaranteeing a high degree of incomputability [3].

Moreover, to understand the effect of error margins arising from experimental imperfections [32], we examined the measurement performed by an imperfect unitary as a completely positive map acting on a noisy quantum channel. In this manner, we were able to model the effects of the depolarising channel acting on a single qubit. This allows us to develop a partial model of the impact that different sources of errors (e.g., dark counts from the single photon detectors) have on the distribution of outputs.

Acknowledgment

We thank Professors A. Cabello, S. Ma and M. Zimand for their comments, which improved the paper.

References

[1] 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.

[2] A. A. Abbott, C. S. Calude, and K. Svozil. Value indefiniteness is almost everywhere. *Physical Review A*, 89(3):032109–032116, 2014.

[3] A. A. Abbott, C. S. Calude, and K. Svozil. A non-probabilistic model of relativised predictability in physics. *Information*, 6(4):773–789, 2015.

[4] A. A. Abbott, C. S. Calude, and K. Svozil. A variant of the Kochen-Specker theorem localising value indefiniteness. *Journal of Mathematical Physics*, 56, 102201, http://dx.doi.org/10.1063/1.4931658, Oct 2015.

[5] 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.

[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. An N–dimensional quantum random number generator. Report CDMTCS-583, Centre for Discrete Mathematics and Theoretical Computer Science, University of Auckland, Auckland, New Zealand, May 2025.

[8] J. M. Agüero Trejo and C. S. Calude. Photonic ternary quantum random number generators. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 479(2273):20220543, May 2023.

[9] J. M. Agüero Trejo, C. S. Calude, M. J. Dinneen, A. Fedorov, A. Kulikov, R. Navarathna, and K. Svozil. How real is incomputability in physics? *Theoretical Computer Science*, 1003:114632, 2024.

[10] J. M. Agüero Trejo, C. S. Calude, and O. C. Stoica. Testing the 3d qrng by undoing. Report CDMTCS-587, Centre for Discrete Mathematics and Theoretical Computer Science, University of Auckland, Auckland, New Zealand, Dec. 2025.

[11] H. Araki and M. Yanase. Measurement of quantum mechanical operators. *Phys. Rev.*, 120(2):622, 1960.

[12] R. Beneduci. Positive operator valued measures and feller markov kernels. *J. Math. Anal. Appl.*, 442(1):50–71, 2016.

[13] T. Breuer. Kochen-specker theorem for finite precision spin-one measurements. *Physical review letters*, 88(24):240402, 2002.

[14] T. Breuer. A kochen-specker theorem for unsharp spin 1 observables. In *Non-locality and Modality*, pages 195–203. Springer, 2002.

[15] T. Breuer. Another no-go theorem for hidden variable models of inaccurate spin 1 measurements. *Philosophy of Science*, 70(5):1368–1379, 2003.

[16] P. Busch. "No information without disturbance": Quantum limitations of measurement. In W. Myrvold, J. Christian, and P. Pearle, editors, *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle*, volume 73 of *Western Ontario Series in Philosophy of Science*, pages 229–256. Springer, 2009.

[17] P. Busch. Translation of "Die Messung quantenmechanischer Operatoren" by EP Wigner. *Arxiv preprint quant-ph/1012.4372*, pages 1–10, December 2010. arXiv:quant-ph/1012.4372.

[18] P. Busch, P. Lahti, J.-P. Pellonpää, and K. Ylinen. *Quantum measurement*, volume 23. Springer, Switzerland, 2016.

[19] A. Cabello. Finite-precision measurement does not nullify the Kochen-Specker theorem. *Phys. Rev. A*, 65(5):052101, 2002.

[20] C. S. Calude and K. Svozil. Binary quantum random number generator based on value indefinite observables. *Scientific Reports*, 14(1):12845, June 2024.

[21] D. Cilluffo. Commentary on the decomposition of universal multiport interferometers: how it works in practice. *Arxiv preprint quant-ph/2412.11955*, pages 1–13, 2024. arXiv:quant-ph/2412.11955.

[22] 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, 2016.

[23] B. d'Espagnat. *Veiled reality: An analysis of present-day quantum mechanical concepts*. CRC Press, Boca Raton, FL, USA, 2018.

[24] B. d'Espagnat. *Conceptual Foundations of Quantum Mechanics*. W.A. Benjamin, New York, 1976.

[25] B. d'Espagnat. *On physics and philosophy*. Princeton University Press, Princeton, NJ, 2006.

[26] A. Grudka and P. Kurzyński. Is there contextuality for a single qubit? *Phys. Rev. Lett.*, 100(16):160401, 2008.

[27] W. Heisenberg. *Physics and Philosophy: The Revolution in Modern Science*. Harper, New York, 1958.

[28] A. Holevo. *Probabilistic and statistical aspects of quantum theory*, volume 1 of *PSNS*. Springer Basel, Basel, Switzerland, 2011.

[29] ID Quantique SA. *Random Number Generation – White Paper. What is the Q in QRNG?* idQuantique, Geneva, Switzerland, May 2020.

[30] A. Kulikov, M. Jerger, A. Potočnik, A. Wallraff, and A. Fedorov. Realization of a quantum random generator certified with the Kochen-Specker theorem. *Phys. Rev. Lett.*, 119:240501, Dec 2017.

[31] R. Kunjwal. Beyond the Cabello-Severini-Winter framework: Making sense of contextuality without sharpness of measurements. *Quantum*, 3:184, 2019.

[32] K. Landsman. *Foundations of Quantum Theory: From Classical Concepts to Operator Algebras*, volume 188 of *Fundamental Theories of Physics*. Springer, Cham, Switzerland, 2017.

[33] L. Loveridge. A relational perspective on the Wigner-Araki-Yanase theorem. *Journal of Physics: Conference Series*, 1638(1):012009, 2020.

[34] L. Loveridge and P. Busch. 'measurement of quantum mechanical operators' revisited. *Eur. Phys. J. D*, 62(2):297–307, 2011.

[35] V. Mannalath, S. Mishra, and A. Pathak. A Comprehensive Review of Quantum Random Number Generators: Concepts, Classification and the Origin of Randomness. page 44.

[36] M. Naimark. About second-kind self-adjoint extensions of symmetrical operator. *Izv. Akad. Nauk USSR, Ser. Mat*, 4:53–104, 1940.

[37] M. Ozawa. Quantum measuring processes of continuous observables. *J. Math. Phys.*, 25(1):79–87, 1984.

[38] R. Spekkens. Contextuality for preparations, transformations, and unsharp measurements. *Phys. Rev. A*, 71(5):052108, 2005.

[39] W. Stinespring. Positive functions on C*-algebras. *Proc. Amer. Math. Soc.*, 6(2):211–216, 1955.

[40] O. Stoica. Can we accurately read or write quantum data? *Physica Scripta*, 100(8):085108, 2025.

[41] E. Wigner. Die Messung quantenmechanischer Operatoren. *Zeitschrift für Physik A Hadrons and nuclei*, 133(1):101–108, 1952.