CDMTCS
Research
Report
Series

Fidelity Thresholds and Robustness of Value-Indefiniteness-Based Spin-1 Qutrit Quantum Random Number Generators

Shan Ma
Central South University, China and
University of Auckland, New Zealand

CDMTCS-588
4 March 2026

Centre for Discrete Mathematics and
Theoretical Computer Science

Fidelity Thresholds and Robustness of Value-Indefiniteness-Based Spin-1 Qutrit Quantum Random Number Generators*

Shan Ma[1,2]
[1]*School of Automation, Central South University, Changsha 410083, China*
[2]*Department of Computer Science, University of Auckland, Auckland 1142, New Zealand*
shanma.adfa@gmail.com

***Abstract*—We investigate the robustness of qutrit quantum random number generators based on projective measurements of the spin-1 operator S_x. Building upon the Kochen–Specker theorem, we derive fidelity thresholds which can guarantee that an experimentally prepared state, despite preparation deviations, remains within the region where contextuality-based randomness certification holds. In addition, we obtain tight bounds quantifying how preparation deviations propagate to the measurement statistics. The developed results could provide a practical framework for assessing and certifying the performance of spin-1 qutrit quantum random number generators.**

***Index Terms*—Fidelity, quantum random number generator, qutrit, value indefiniteness**

I. Introduction

Quantum random number generators (QRNGs) play a significant role in quantum cryptography, quantum communications, and quantum computation tasks [1]. Classical random number generators, whether algorithmic or based on physical noise sources, can only produce pseudorandomness. This is because their outputs are generated by deterministic processes that can in principle be reconstructed or predicted. By contrast, QRNGs exploit the inherent indeterminacy of quantum measurement outcomes to produce randomness that is not predetermined by any classical description of the measured system [1], [2].

A particularly useful way to certify genuine quantum randomness relies on the value indefiniteness of quantum observables [3], [4]. According to the Kochen–Specker theorem [3], [4], for a discrete variable quantum system of dimension $n \geq 3$ prepared in a state $|\xi\rangle$, any projector $|\chi\rangle\langle\chi|$ satisfying $0 < |\langle\chi|\xi\rangle| < 1$ is value indefinite under the standard non-contextuality assumptions. This means that the outcome of such a projective measurement is not determined before the measurement; it is in fact produced at the moment of measurement and cannot be implied by any hidden classical information. This property makes value indefiniteness one of the most reliable foundations for certifying genuine quantum randomness [5]–[10].

According to the Kochen–Specker theorem, qutrits ($n = 3$) provide the lowest dimensional setting where value indefiniteness can be produced. Based on this fact, a practical and experimentally accessible realization of such contextuality based QRNGs is provided by the spin-1 system. In this setup, genuine randomness can be generated by measuring the projectors associated with the eigenstates of the spin operator in the x direction (S_x), which naturally yields a three-outcome observable [11], [12]. The spin operator S_x admits the spectral decomposition as follows

$$S_x = U_x \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} U_x^\dagger,$$

where the columns of U_x form an

orthonormal eigenbasis $\{|1_x\rangle, |0_x\rangle, |-1_x\rangle\}$ of S_x. The corresponding projectors $\{|1_x\rangle\langle 1_x|, |0_x\rangle\langle 0_x|, |-1_x\rangle\langle -1_x|\}$ define the three possible measurement outcomes $+1$, 0, and -1. Given any qutrit state $|\phi\rangle$, measuring S_x produces a three-outcome probability distribution determined by the overlaps between the prepared state $|\phi\rangle$ and the eigenstates of the spin operator S_x, i.e., $\{|1_x\rangle, |0_x\rangle, |-1_x\rangle\}$. This quantum random number generating approach is straightforward and can be easily implemented using current experimental platforms, making spin-1 qutrits a practical way for building reliable QRNGs.

In practice, however, the experimental realization of QRNGs is inevitably subject to noise and imperfections. In photonic implementations, for example, losses in waveguides and imprecise beam splitter ratios may cause deviations from the intended quantum state [13], [14]. The state actually prepared, denoted by $|\psi\rangle$, may differ from the ideal target state $|\phi\rangle$, and the fidelity $F(|\phi\rangle, |\psi\rangle) = |\langle\psi|\phi\rangle|^2$ is commonly used to measure this deviation [15]. For contextuality based certification, it is important that the actually prepared state $|\psi\rangle$ remains outside specific excluded regions in which the value indefiniteness guarantee fails. In particular, according to the Kochen–Specker theorem, the parallel set $\mathscr{E}_{\parallel}$, consisting of all states aligned with any of the eigenvectors $\{|1_x\rangle, |0_x\rangle, |-1_x\rangle\}$, belongs to such excluded region. In addition, the orthogonal set $\mathscr{E}_{\perp}$, consisting of all states orthogonal to any of the eigenvectors $\{|1_x\rangle, |0_x\rangle, |-1_x\rangle\}$, also belongs to such excluded region. Since experimental noise may push the prepared state into these excluded regions leading to the failure of the certification of randomness, a natural and practically important question arises: How much fidelity is needed to ensure that the experimentally prepared state remains in a region where contextuality based certification is valid?

In this paper, we will address this question. Specifically, for a target state written as $|\phi\rangle = a|1_x\rangle + b|0_x\rangle + c|-1_x\rangle$ which is assumed to be neither orthogonal nor parallel to any of the eigenvectors $\{|1_x\rangle, |0_x\rangle, |-1_x\rangle\}$ of the spin operator S_x, it is found that the largest possible overlap between $|\phi\rangle$ and states in the excluded region determines the required fidelity threshold. Based on this fact, we obtain that the required fidelity threshold is given by $F_{req}(|\phi\rangle, |\psi\rangle) = \max\{|a|^2, |b|^2, |c|^2, 1-|a|^2, 1-|b|^2, 1-|c|^2\}$. In other words, any experimentally prepared state $|\psi\rangle$ with fidelity above this threshold is guaranteed to avoid the excluded region and thus preserves the conditions needed for contextuality based randomness certification.

Furthermore, we also know that experimental imperfections on state preparation may also change the measurement statistics of the spin-1 observable, affecting the quality of the random numbers generated. To be specific, when the experimentally prepared state $|\psi\rangle$ has fidelity $F(|\phi\rangle, |\psi\rangle) = |\langle\psi|\phi\rangle|^2$, the resulting probabilities $q_m = \Pr(S_x = m)$ for $m \in \{+1, 0, -1\}$ can deviate from the ideal distribution p_m. In this paper, we show that these deviations are tightly constrained: each individual probability satisfies $|q_m - p_m| \leq \sqrt{1 - F(|\phi\rangle, |\psi\rangle)}$, and the total variation distance obeys the same upper bound, i.e., $\frac{1}{2}\sum_m |q_m - p_m| \leq \sqrt{1 - F(|\phi\rangle, |\psi\rangle)}$. The inequalities developed in this paper provide a feasible way to assess experimental performance, and are potentially useful for validating randomness generation within the spin-1 framework.

II. Notation and Preliminary Result

Fix a positive integer $n \geq 3$ and consider the n-dimensional Hilbert space $\mathbb{C}^n$. For any unit vector $|\varphi\rangle \in \mathbb{C}^n$, let $P_\varphi = |\varphi\rangle\langle\varphi|$ denote the one-dimensional projection observable onto the span of $|\varphi\rangle$. Let O be a non-empty, finite set of such projection observables.

A subset $C \subseteq O$ is called a context if it consists of n pairwise orthogonal projections; that is, $C = \{P_{\varphi_1}, \dots, P_{\varphi_n}\}$ with $\langle\varphi_i|\varphi_j\rangle = 0$ for all $i \neq j$.

A function $v : O \to \{0, 1\}$ is called an admissible value assignment if for every context $C \subseteq O$ we have $\sum_{P \in C} v(P) = 1$. That is, in any complete measurement context exactly one projector is assigned the value 1 and all others are assigned 0. A quantum measurement is said to be non-contextual if the value assigned to any observable $P \in O$ is independent of the context C in which P appears.

Given a value assignment function v, an observable $P \in O$ is value definite if $v(P)$ is specified (meaning its measurement outcome is predetermined); otherwise P is value indefinite.

The Eigenstate Principle states that if a quantum system is prepared in a state $|\varphi\rangle$, then the projector P_φ corresponding to that state must be value definite.

Theorem 1 (Located Kochen–Specker Theorem [3], [4])**.** Let a quantum system be described by a state $|\xi\rangle$ in $\mathbb{C}^n$ with $n \geq 3$. Let $|\chi\rangle$ be any state that is neither orthogonal nor parallel to $|\xi\rangle$, so that $0 < |\langle\chi|\xi\rangle| < 1$. If a value assignment $v : O \to \{0,1\}$ satisfies the following three assumptions:

(i) *Admissibility*: in every context exactly one projector has value 1;
(ii) *Non-contextuality*: the value of any observable is independent of the context in which it is measured;
(iii) *Eigenstate Principle*: the projector P_ξ has value 1,

then the projector P_χ is value indefinite.

The Located Kochen–Specker Theorem states that whenever two quantum states have a nontrivial overlap $0 < |\langle\chi|\xi\rangle| < 1$ for quantum systems of dimension $n \geq 3$, the corresponding projector P_χ cannot be assigned a predetermined value under any non-contextual admissible assignment. In other words, measurements of such projectors are intrinsically value indefinite and therefore can be used for producing genuine quantum randomness.

III. 3-Dimensional QRNG

Since qutrits ($n = 3$) provide the lowest dimensional setting in which the Located Kochen–Specker theorem applies, a feasible realization of value-indefiniteness-based QRNGs is provided by the spin-1 system. In this setup, genuine randomness is achieved by measuring the projectors corresponding to the eigenstates of the spin operator in the x direction (S_x). The spin-1 operator in the x direction is given by

$$S_x = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = U_x \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} U_x^\dagger, \tag{1}$$

where

$$\begin{aligned} U_x &= \big[\, |1_x\rangle \;\; |0_x\rangle \;\; |-1_x\rangle \,\big] \\ &= \frac{1}{2}\begin{pmatrix} 1 & \sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & -\sqrt{2} & 1 \end{pmatrix}. \end{aligned} \tag{2}$$

The three projectors onto these eigenstates are given by

$$\begin{aligned} P_{1_x} &= |1_x\rangle\langle 1_x|\,, \qquad P_{0_x} = |0_x\rangle\langle 0_x|\,, \\ P_{-1_x} &= |-1_x\rangle\langle -1_x|\,. \end{aligned} \tag{3}$$

Note that $\{P_{1_x},\ P_{0_x},\ P_{-1_x}\}$ form a complete set of mutually orthogonal rank 1 projections. As a result, they constitute a measurement context for 3-dimensional quantum systems. A spin-1 QRNG generates randomness by preparing a qutrit state $|\phi\rangle$ and measuring the three projectors $\{P_{1_x}, P_{0_x}, P_{-1_x}\}$, which produces exactly one of the outcomes $\{+1, 0, -1\}$. The statistics of these outcomes are determined by the overlaps between the prepared state $|\phi\rangle$ and the eigenbasis $\{|1_x\rangle \;\; |0_x\rangle \;\; |-1_x\rangle\}$.

It is worth to mention that if we want to obtain a desired output distribution

$$\begin{aligned} &\Pr(S_x = +1) = p_1, \qquad \Pr(S_x = 0) = p_2, \\ &\Pr(S_x = -1) = p_3, \end{aligned} \tag{4}$$

with $p_i > 0,\ p_1 + p_2 + p_3 = 1$, the target prepared states $|\phi\rangle$ can be parametrized by

$$|\phi\rangle = \sqrt{p_1}\, e^{i\theta_1}|1_x\rangle + \sqrt{p_2}\, e^{i\theta_2}|0_x\rangle + \sqrt{p_3}\, e^{i\theta_3}|-1_x\rangle, \tag{5}$$

where θ_j are free phase parameters [12]. As for any quantum state, a global phase is physically irrelevant, so θ_1 can be set to zero without loss of generality. To relate this parametrization to physical implementations, it is useful to express the state $|\phi\rangle$ described in Eq. (5) in the computational basis

$\{|0\rangle, |1\rangle, |2\rangle\}$. Using Eq. (2), one obtains the explicit parametrization of $|\phi\rangle$ as

$$|\phi\rangle = U_x \begin{pmatrix} \sqrt{p_1}e^{i\theta_1} \\ \sqrt{p_2}e^{i\theta_2} \\ \sqrt{p_3}e^{i\theta_3} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} \sqrt{p_1}e^{i\theta_1} + \sqrt{2p_2}e^{i\theta_2} + \sqrt{p_3}e^{i\theta_3} \\ \sqrt{2p_1}e^{i\theta_1} - \sqrt{2p_3}e^{i\theta_3} \\ \sqrt{p_1}e^{i\theta_1} - \sqrt{2p_2}e^{i\theta_2} + \sqrt{p_3}e^{i\theta_3} \end{pmatrix}. \quad (6)$$

IV. Robustness of QRNGs via Fidelity Analysis

In any realistic experimental implementation of QRNGs, imperfections and noise are inevitable in the state preparation process, which may lead to deviations between the target state $|\phi\rangle$ and the actually prepared state $|\psi\rangle$. These deviations may arise from, for example, losses in waveguides and imprecise beam splitter ratios in quantum optics.

To facilitate analysis, we assume $|\phi\rangle$ and $|\psi\rangle$ are pure states. A commonly used measure of the overlap between the two pure states $|\phi\rangle$ and $|\psi\rangle$ is in terms of the fidelity

$$F(|\phi\rangle, |\psi\rangle) = |\langle\psi|\phi\rangle|^2, \quad (7)$$

which takes values in [0, 1], with $F(|\phi\rangle, |\psi\rangle) = 1$ corresponding to identical states (up to a global phase) and $F(|\phi\rangle, |\psi\rangle) = 0$ corresponding to orthogonal states. Any intermediate value $0 < F(|\phi\rangle, |\psi\rangle) < 1$ quantifies a nontrivial overlap between the two states $|\phi\rangle$ and $|\psi\rangle$.

According to Theorem 1, to certify genuine quantum randomness, the prepared state $|\psi\rangle$ should avoid the specific region where one or more measurement projectors become value definite. For convenience, we write the target qutrit state as:

$$|\phi\rangle = a|1_x\rangle + b|0_x\rangle + c|-1_x\rangle, \quad (8)$$

where $|a|^2 + |b|^2 + |c|^2 = 1$. Here the excluded region $\mathscr{E}$ contains any normalized state $|\psi\rangle$ violating the condition $0 < |\langle m_x|\psi\rangle|^2 < 1$ for at least one $m \in \{+1, 0, -1\}$. Explicitly, the excluded region $\mathscr{E}$ is described by

$$\mathscr{E} = \Big\{|\psi\rangle : \ |\psi\rangle \propto |m_x\rangle \text{ or } \langle m_x|\psi\rangle = 0, \text{ for some } m \in \{+1, 0, -1\}\Big\}. \quad (9)$$

Based on (9), we have the following fidelity threshold for quantum randomness certification.

Theorem 2. Given the target pure state $|\phi\rangle = a|1_x\rangle + b|0_x\rangle + c|-1_x\rangle \notin \mathscr{E}$, any pure state $|\psi\rangle$ satisfying the fidelity

$$F(|\phi\rangle, |\psi\rangle) > \max\left\{|a|^2, |b|^2, |c|^2, 1-|a|^2, 1-|b|^2, 1-|c|^2\right\} \quad (10)$$

cannot lie in the region $\mathscr{E}$.

Proof. To prove this, we only need to show that if $|\psi\rangle \in \mathscr{E}$, the inequality (10) is violated. It can be seen from Eq. (9) that the excluded set $\mathscr{E}$ is the union of parallel and orthogonal sets defined by the eigenbasis $\{|1_x\rangle \ |0_x\rangle \ |-1_x\rangle\}$. So we distinguish two cases.

Case I: Parallel Sets ($\mathscr{E}_{\parallel}$). If $|\psi\rangle$ is aligned with an eigenstate, i.e., $|\psi\rangle = |m_x\rangle$ for some $m \in \{+1, 0, -1\}$. The maximum fidelity is achieved when $|\psi\rangle$ is aligned with the component of $|\phi\rangle$ having the largest magnitude. Bearing Eq. (8) in mind, the possible fidelity values are:

$$F(|\phi\rangle, |1_x\rangle) = |\langle\phi|1_x\rangle|^2 = |a|^2,$$
$$F(|\phi\rangle, |0_x\rangle) = |\langle\phi|0_x\rangle|^2 = |b|^2,$$
$$F(|\phi\rangle, |-1_x\rangle) = |\langle\phi|-1_x\rangle|^2 = |c|^2.$$

Thus, if $|\psi\rangle = |m_x\rangle$ for some $m \in \{+1, 0, -1\}$, $\max_{\psi\in\mathscr{E}_{\parallel}} F(|\phi\rangle, |\psi\rangle) = \max\{|a|^2, |b|^2, |c|^2\}$. Therefore, if $|\psi\rangle \in \mathscr{E}_{\parallel}$, the inequality (10) does not hold.

Case II: Orthogonal Sets ($\mathscr{E}_{\perp}$). Suppose $|\psi\rangle$ is orthogonal to an eigenstate, i.e., $\langle m_x|\psi\rangle = 0$ for some $m \in \{+1, 0, -1\}$. For example, assume $\langle 1_x|\psi\rangle = 0$. This means $|\psi\rangle$ is in the 2D space spanned by $\{|0_x\rangle, |-1_x\rangle\}$. The fidelity $F(|\phi\rangle, |\psi\rangle)$ is maximized when $|\psi\rangle$ is aligned with the projection of $|\phi\rangle$ onto this space, which is $b|0_x\rangle + c|-1_x\rangle$ based on Eq. (8). The maximum fidelity in this case is

$$\max_{\psi\in\mathscr{E}_{\perp,1_x}} F(|\phi\rangle, |\psi\rangle) = ||b|0_x\rangle + c|-1_x\rangle||^2 = |b|^2 + |c|^2 = 1 - |a|^2.$$

Similarly,

- If $\langle 0_x|\psi\rangle = 0$: Maximum fidelity is $\max_{\psi\in\mathscr{E}_{\perp,0_x}} F(|\phi\rangle, |\psi\rangle) = 1 - |b|^2$.

- If $\langle -1_x|\psi\rangle = 0$: Maximum fidelity is $\max_{\psi\in\mathscr{E}_{\perp,-1_x}} F(|\phi\rangle,|\psi\rangle) = 1-|c|^2$.

Thus, $\max_{\psi\in\mathscr{E}_\perp} F(|\phi\rangle,|\psi\rangle) = \max\{1-|a|^2, 1-|b|^2, 1-|c|^2\}$. Therefore, if $|\psi\rangle \in \mathscr{E}_\perp$, the inequality (10) does not hold.

Because the overall excluded region is $\mathscr{E} = \mathscr{E}_\parallel \cup \mathscr{E}_\perp$, based on the previous analysis in Case I and Case II, we conclude if $|\psi\rangle \in \mathscr{E}$, the maximum fidelity $\max_{\psi\in\mathscr{E}} F(|\phi\rangle,|\psi\rangle) \leq \max\left\{|a|^2,|b|^2,|c|^2,1-|a|^2,1-|b|^2,1-|c|^2\right\}$. This means the inequality (10) is violated. In other words, if the prepared state $|\psi\rangle$ satisfies (10), it cannot be in the excluded region $\mathscr{E}$. This completes the proof. □

V. Effect of Preparation Imperfections on QRNG Statistics

The derived fidelity thresholds in Theorem 2 provide a criterion to ensure the prepared state remains in the region where value indefiniteness is preserved. We now proceed to quantify how state preparation imperfections affect the final measurement statistics. Recall that the measurement observable, S_x, is represented by

$$S_x = U_x \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} U_x^\dagger,$$

where $U_x = \left[\, |1_x\rangle \;\; |0_x\rangle \;\; |-1_x\rangle \,\right]$. If the target state is $|\phi\rangle$, the ideal measurement distribution is given by:

$$p_m = |\langle m_x|\phi\rangle|^2, \qquad m \in \{+1,0,-1\}.$$

In practice, state preparation imperfections may result in an actual prepared state $|\psi\rangle$ that deviates from the target state $|\phi\rangle$, which directly results in shifts in the observed probabilities $q_m = \Pr(S_x = m) = |\langle m_x|\psi\rangle|^2$. A critical question then is how large these statistical deviations can be when the preparation fidelity $F(|\phi\rangle,|\psi\rangle)$ is bounded from below. The following result provides a bound that connects the guaranteed fidelity of the state preparation with the resulting deviations in the measurement statistics.

Theorem 3. Let $|\phi\rangle$ be the target state with ideal probabilities $p_m = |\langle m_x|\phi\rangle|^2$. If the prepared state $|\psi\rangle$ satisfies the fidelity $F(|\phi\rangle,|\psi\rangle) = |\langle\psi|\phi\rangle|^2 \geq r$, then the observed probabilities $q_m = |\langle m_x|\psi\rangle|^2$ obey the following inequalities:

$$|q_m - p_m| \leq \sqrt{1-r}, \tag{11}$$

$$\frac{1}{2}\sum_{m\in\{+1,0,-1\}} |q_m - p_m| \leq \sqrt{1-r}. \tag{12}$$

Proof. Let $\sigma = |\phi\rangle\langle\phi|$ and $\rho = |\psi\rangle\langle\psi|$. Let $\{P_{m_x}\}_{m\in\{+1,0,-1\}}$ be the projective measurement with $P_{m_x} = |m_x\rangle\langle m_x|$, so that $p_m = \mathrm{Tr}(P_{m_x}\sigma)$ and $q_m = \mathrm{Tr}(P_{m_x}\rho)$. To prove the inequality (12), we need to refer to a relationship between the classical distance and the quantum trace distance. Recall that for two density operators ρ and σ on the same Hilbert space, the quantum trace distance (D_{Tr}) is defined as

$$D_{\mathrm{Tr}}(\rho,\sigma) \triangleq \frac{1}{2}\|\rho-\sigma\|_1, \; \|X\|_1 \triangleq \mathrm{Tr}\sqrt{X^\dagger X}. \tag{13}$$

It has been known that the total variation distance is bounded by the trace distance [15, Sec. 9.2.3]; that is,

$$\frac{1}{2}\sum_m |q_m - p_m| \leq D_{\mathrm{Tr}}(\rho,\sigma).$$

Here for pure states σ and ρ, the trace distance admits the closed form

$$D_{\mathrm{Tr}}(\rho,\sigma) = \sqrt{1-|\langle\psi|\phi\rangle|^2} = \sqrt{1-F(|\phi\rangle,|\psi\rangle)}.$$

See [15, Sec. 9.2.3] for details. Applying the constraint $F(|\phi\rangle,|\psi\rangle) \geq r$, we obtain

$$\frac{1}{2}\sum_m |q_m - p_m| \leq \sqrt{1-F(|\phi\rangle,|\psi\rangle)} \leq \sqrt{1-r}.$$

To obtain the inequality (11), for any subset S of the outcome set $\{+1,0,-1\}$, define $p(S) \triangleq \sum_{m\in S} p_m$ and $q(S) \triangleq \sum_{m\in S} q_m$. Then it can be shown that the total variation distance satisfies

$$\frac{1}{2}\sum_m |q_m - p_m| = \sup_S |q(S) - p(S)|.$$

In particular, for any single outcome m we may choose $S = \{m\}$ to obtain

$$\begin{aligned} |q_m - p_m| &= |q(\{m\}) - p(\{m\})| \\ &\leq \sup_S |q(S) - p(S)| = \frac{1}{2}\sum_k |q_k - p_k|. \end{aligned}$$

Combining with (12) gives $|q_m - p_m| \leq \sqrt{1-r}$ for all m, which proves (11). □

The bounds developed in Theorem 3 quantify how preparation imperfections influence the output statistics of a spin-1 QRNG. From Theorem 2 and Theorem 3 one can see that if the fidelity is above the required threshold, then not only is value indefiniteness preserved, but the resulting probabilities are guaranteed to remain close to their ideal values.

VI. Example

We provide a quantum optical example to illustrate the developed results. Consider a single photon path qutrit encoded in three spatial modes. The target state is written in the S_x eigenbasis as

$$|\phi\rangle = a|1_x\rangle + b|0_x\rangle + c|-1_x\rangle, \tag{14}$$

and is prepared by the state preparation block (left dashed red box in Fig. 1) using beam splitters and phase shifters. The measurement projectors $\{P_{1_x}, P_{0_x}, P_{-1_x}\}$ can be implemented in linear optics by applying a 3-mode interferometer realizing $U_x^\dagger$ (right dashed red box in Fig. 1), followed by path resolved detection at the three output ports. The interferometer converts the S_x eigenstate measurement into output port detection, so that detector clicks (D_{+1}, D_0, D_{-1}) implement the projectors $(P_{1_x}, P_{0_x}, P_{-1_x})$ and yield outcomes $S_x \in \{+1, 0, -1\}$.

For a target state $|\phi\rangle$ that is neither orthogonal nor parallel to any eigenvector in $\{|1_x\rangle, |0_x\rangle, |-1_x\rangle\}$, Theorem 2 states that the required fidelity threshold is given by

$$\begin{aligned} &F_{\text{req}}(|\phi\rangle, |\psi\rangle) \\ &= \max\left\{|a|^2, |b|^2, |c|^2,\ 1-|a|^2,\ 1-|b|^2,\ 1-|c|^2\right\}. \end{aligned}$$

Hence, any experimentally prepared state $|\psi\rangle$ with fidelity $F(|\phi\rangle, |\psi\rangle) > F_{\text{req}}(|\phi\rangle, |\psi\rangle)$ is guaranteed to avoid the excluded region and thus preserves the conditions needed for contextuality based randomness certification. For example, taking $(|a|^2, |b|^2, |c|^2) = (0.50, 0.30, 0.20)$ yields

$$\begin{aligned} &F_{\text{req}}(|\phi\rangle, |\psi\rangle) \\ &= \max\{0.50, 0.30, 0.20, 0.50, 0.70, 0.80\} = 0.80. \end{aligned}$$

In this case, if the experimentally prepared state $|\psi\rangle$ satisfies $F(|\phi\rangle, |\psi\rangle) > 0.8$, it is guaranteed to lie outside the excluded region, and the contextuality based certification remains valid.

Let p_m denote the ideal outcome distribution for $m \in \{+1, 0, -1\}$ and let q_m denote the observed distribution obtained when the actual state $|\psi\rangle$ is measured. Once the fidelity $F(|\phi\rangle, |\psi\rangle)$ is estimated, Theorem 3 states that the deviations are bounded by

$$|q_m - p_m| \leq \sqrt{1 - F(|\phi\rangle, |\psi\rangle)} \quad \forall m, \tag{15}$$

$$\frac{1}{2}\sum_m |q_m - p_m| \leq \sqrt{1 - F(|\phi\rangle, |\psi\rangle)}. \tag{16}$$

For instance, if $F(|\phi\rangle, |\psi\rangle) = 0.96$, then $\sqrt{1 - F(|\phi\rangle, |\psi\rangle)} = 0.2$, then each outcome probability deviates from its ideal value by at most 0.2, and the total variation distance is at most 0.2.

VII. Conclusion

In this paper, we have developed a fidelity based analysis framework for spin-1 qutrit QRNGs. We have analyzed the minimum state preparation accuracy required to avoid sets that undermine value indefiniteness. We have also established explicit quantitative bounds on how state preparation imperfections influence the observed statistics. The results presented in this paper provide potentially useful tools for assessing the robustness and reliability of quantum contextuality based randomness generation. Moreover, the method could be extended to the analysis of higher dimensional QRNGs.

VIII. Acknowledgments

We thank Prof. C. S. Calude and Prof. O. C. Stoica for insightful discussions.

References

[1] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.*, vol. 89, p. 015004, 2017.

[2] C. S. Calude, M. J. Dinneen, M. Dumitrescu, and K. Svozil, "Experimental evidence of quantum randomness incomputability," *Phys. Rev. A*, vol. 82, p. 022102, 2010.

[3] A. A. Abbott, C. S. Calude, J. Conder, and K. Svozil, "Strong Kochen-Specker theorem and incomputability of quantum randomness," *Phys. Rev. A*, vol. 86, p. 062109, 2012.

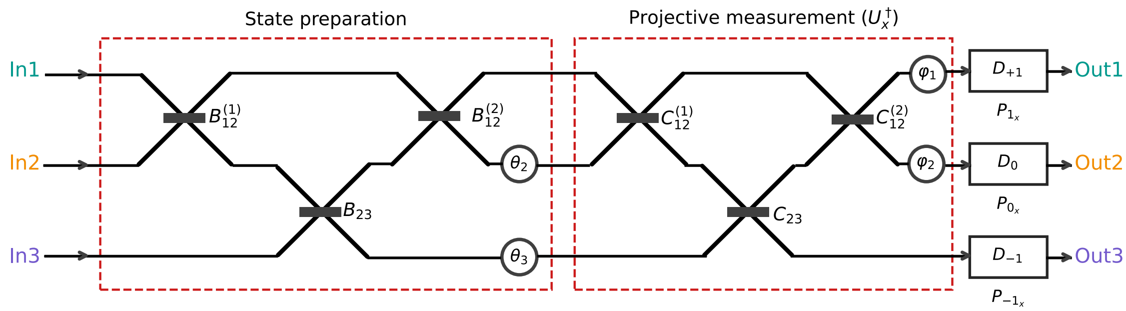

Fig. 1. Single photon path-qutrit implementation. The left block aims at preparing the target state. The right block realizes the S_x projective measurement via a 3-mode interferometer $U_x^\dagger$ and path resolved detection, with clicks (D_{+1}, D_0, D_{-1}) corresponding to $(P_{1_x}, P_{0_x}, P_{-1_x})$ and outcomes $S_x \in \{+1, 0, -1\}$.

[4] A. A. Abbott, C. S. Calude, and K. Svozil, "Value-indefinite observables are almost everywhere," *Phys. Rev. A*, vol. 89, p. 032109, 2014.

[5] 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.*, vol. 119, p. 240501, 2017.

[6] S. Kochen and E. P. Specker, "The problem of hidden variables in quantum mechanics," *Journal of Mathematics and Mechanics*, vol. 17, pp. 59–87, 1967.

[7] A. Cabello, J. Estebaranz, and G. García-Alcaine, "Bell-Kochen-Specker theorem: A proof with 18 vectors," *Physics Letters A*, vol. 212, pp. 183–187, 1996.

[8] C. Budroni, A. Cabello, O. Gühne, M. Kleinmann, and J.-Å. Larsson, "Kochen-Specker contextuality," *Rev. Mod. Phys.*, vol. 94, p. 045007, 2022.

[9] A. A. Abbott, C. S. Calude, and K. Svozil, "A variant of the Kochen-Specker theorem localising value indefiniteness," *J. Math. Phys.*, vol. 56, p. 102201, 2015.

[10] A. A. Abbott, C. S. Calude, M. D. Dinneen, and N. Huang, "Experimentally probing the algorithmic randomness and incomputability of quantum randomness," *Physica Scripta*, vol. 94, p. 045103, 2019.

[11] J. M. Agüero Trejo and C. S. Calude, "A new quantum random number generator certified by value indefiniteness," *Theoretical Computer Science*, vol. 862, pp. 3–13, 2021.

[12] J. M. Agüero Trejo and C. S. Calude, "Photonic ternary quantum random number generators," *Proc. A*, vol. 479, p. 20220543, 2023.

[13] D. F. Walls and G. J. Milburn, *Quantum Optics*, 2nd ed. Springer-Verlag Berlin Heidelberg, 2008.

[14] C. Gerry and P. Knight, *Introductory Quantum Optics*. Cambridge University Press, 2004.

[15] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.