Maximal Intrinsic Randomness of a Quantum State

Maissa BEJI

Supervisor: Peter BROWN

Télécom Paris

January 24, 2025

Contents

1 Introduction

1.1 Context

Quantum intrinsic randomness plays a key role in making cryptographic systems secure. It provides the unpredictability needed for secure protocols like quantum key distribution (QKD) and quantum random number generation (QRNG) [1]. Analyzing and quantifying this randomness, especially in adversarial scenarios, ensures the reliability and security of systems that depend on it.

Researchers have investigated various aspects of quantum randomness by focusing on the optimization of conditional entropy under varying levels of power granted to an eavesdropper, enabling more realistic and practical scenarios [2]. These studies aim to understand the resourcefulness of quantum states and establish practical approaches for leveraging their inherent randomness in real-world implementations.

One challenge in this context is determining how a party, such as Alice, can generate random bits independent of an eavesdropper, even when the eavesdropper shares entanglement with the source and measurement apparatus, while accounting for the existence of optimal POVMs for arbitrary state randomness extraction, which is further complicated by inevitable experimental imperfections in measurement devices.

1.2 Literature review

Previous work [3] has explored two distinct scenarios in intrinsic randomness extraction:

The first scenario outlines a basic framework where Alice generates random numbers from a d-dimensional quantum state, ρ_A, through projective measurements (PVM). In this case, an adversary (Eve) may share correlations with Alice's source via a joint state ρ_{AE}, subject to the constraint $\mathrm{Tr}_E(\rho_{AE}) = \rho_A$. Eve holds a purification of the state but does not have access to the measurements performed by Alice. The measurement process results in a classical-quantum state:

$$\rho_{XE} = \sum_x |x\rangle\langle x| \otimes \rho_{E,x}$$

where $\rho_{E,x} = \mathrm{Tr}_A[(M_x \otimes I)\rho_{AE}]$. The extractable randomness is then quantified by the minimum $H(X|E)$ over all possible ρ_{AE}.

The second scenario expands on the first by considering more powerful adversarial capabilities. In this case, Alice employs general measurements (POVMs) instead of projective measurements, while Eve may also share quantum correlations with the measurement apparatus through the Naimark dilation space. Specifically, if B represents the quantum system of the measurement device, the initial tripartite state ρ_{ABE} (where $\mathrm{Tr}_{BE}(\rho_{ABE}) = \rho_A$) evolves under a POVM $\{M_x\}_x$. Using Naimark's dilation theorem, this POVM can be realized as a projective measurement $\{P_x\}_x$ on the joint system AB, satisfying the consistency condition:

$$\mathrm{Tr}_B[P_x(I_A \otimes \rho_B)] = M_x.$$

The post-measurement state is then given by:

$$\rho_{XE} = \sum_{x} |x\rangle\langle x| \otimes \mathrm{Tr}_{AB}[(P_x \otimes I_E)\rho_{ABE}].$$

The amount of intrinsic randomness is determined by minimizing $H(X|E)$ over two elements: all possible extensions of the fixed state ρ_A and all valid Naimark implementations of the chosen POVM $\{M_x\}_x$. In this setup, a tripartite source ρ_{ABE} is distributed to Alice, a measurement device, and the adversary Eve. The marginal state ρ_A is trusted and known, but the states held by the measurement device and the adversary are completely unknown.

1.3 Motivation

The second scenario highlights significant challenges in achieving the theoretical maximum intrinsic randomness. This work [3] demonstrated that when the POVM is extremal and rank-one, the minimization problem for intrinsic randomness can be solved explicitly. However, it was also shown that this measure of intrinsic randomness is discontinuous across the set of POVMs for a fixed state ρ_A. This discontinuity implies that even minor imperfections in measurement devices can significantly reduce randomness rates, posing challenges for practical implementations.

This raises two critical research questions: Can robust POVMs be identified that avoid these discontinuities while still achieving high randomness rates? Additionally, can a decomposition of a POVM into extremals provide a better upper bound on the maximum intrinsic randomness? Addressing these questions is essential for advancing reliable and experimentally feasible quantum randomness generation techniques.

1.4 Contributions

Building on these challenges, we made two key advances: First, we investigated how different combinations of trivial measurements and extremal rank-1 projectors affect intrinsic randomness generation. Second, we developed an algorithmic approach to decompose arbitrary POVMs into a combination of extremal rank-1 POVMs.

By systematically analyzing POVM decompositions, we provide a practical framework for:

- Identifying POVMs that balance optimal randomness generation with experimental stability.
- Establishing tighter upper bounds on maximum intrinsic randomness through careful examination of extremal decompositions.

Strategic combinations of stable measurements offer improved performance parameters compared to perfect extremal measurements, providing concrete solutions for experimental implementations.

2 Preliminaries

In the following, we note the quantum systems and their associated Hilbert spaces by capital letters $\mathcal{A}$ or $\mathcal{B}$. The set of quantum states for a system $\mathcal{A}$ is denoted $\mathcal{D}(\mathcal{A})$.
A collection of operators $\{M_x\}_x$ forms a POVM on system $\mathcal{A}$ when $M_x \in \mathcal{P}(\mathcal{A})$ and $\sum_x M_x = I_{\mathcal{A}}$. When $\{M_x\}_x$ consists of projectors, we call this a PVM (projective measurement). A POVM $\{M_x\}_x$ is extremal if for any POVMs $\{F_x\}_x$, $\{G_x\}_x$, and $0 < \lambda < 1$, the condition $M_x = \lambda F_x + (1 - \lambda)G_x$ for all x implies that $F_x = G_x = M_x$.

Theorem 2.1 Naimark Dilation.
Let $\{M_x\}_x$ be a POVM on A. Then, there exists a state $\sigma_B \in D(B)$ and a PVM $\{P_x\}_x$ on AB such that

$$\mathrm{Tr}_B(P_x(I_A \otimes \sigma_B)) = M_x$$

3 Problem Statement

To rigorously understand intrinsic randomness in quantum systems, it is essential to establish precise definitions. Previous work [3] has introduced formal measures for quantifying randomness generated by a POVM applied to a quantum state.

Definition 3.1. Intrinsic H-randomness Let $\rho_A \in D(A)$ and let $\{M_x\}_x$ be a POVM on the system A. Then the intrinsic H-randomness of the pair $(\rho_A, \{M_x\}_x)$ is defined as:

$$I_H^{\mathrm{POVM}}(\rho_A, \{M_x\}_x) := \inf H(X|E)$$

subject to the constraints:

$$\rho_{XE} = \sum_x |x\rangle\langle x| \otimes \mathrm{Tr}_{AB}\left[(P_x \otimes I_E)|\rho\rangle\langle\rho|_{ABE}\right],$$

$$\mathrm{Tr}_B[\rho_{AB}] = \rho_A, \quad \rho_{AB} \in D(AB),$$

$$\mathrm{Tr}_B\left[P_x(I_A \otimes \rho_B)\right] = M_x,$$

$$\{P_x\}_x \text{ is a projective measurement.}$$

Here, $|\rho\rangle_{ABE} = \sum_k \sqrt{\rho_{AB}}|k\rangle_{AB} \otimes |k\rangle_E$ is a purification of ρ_{AB}.
This definition simplifies the optimization to involve only Naimark dilations and bipartite states ρ_{AB}.

Definition 3.2. Maximal intrinsic H-randomness Let $\rho_A \in D(A)$ and let H be a conditional entropy. Then we define the maximal intrinsic H-randomness of ρ_A as:

$$R_H^{\mathrm{POVM}}(\rho_A) = \sup_{\{M_x\}_x} I_H^{\mathrm{POVM}}(\rho_A, \{M_x\}_x).$$

In other words, the intrinsic randomness is defined by focusing on measuring the randomness that can be extracted when a POVM is applied to a quantum state ρ_A. The goal is to determine the minimum conditional entropy $H(X|E)$, which quantifies how unpredictable the measurement outcomes X are to an eavesdropper E, who may have partial information about the system. To quantify the maximal intrinsic randomness, we need to find the best measurement strategy.

To illustrate this, consider the trivial measurement example, which demonstrates a case where no intrinsic randomness is produced. This example highlights the importance of measurement choice in achieving randomness extraction:
The POVM is defined as

$$M_x = p(x) I_A,$$

where $p(x)$ is a probability distribution and I_A is the identity operator on system A.
This POVM can be implemented through Naimark's dilation theorem, which allows the

realization of a POVM as a Projective Valued Measure (PVM) in an extended Hilbert space. In this case:
The projectors are defined as

$$P_x = I_A \otimes |x\rangle\langle x|,$$

which act on the combined system $A \otimes B$.
The state of system B is

$$\rho_B = \sum_x p(x)|x\rangle\langle x|.$$

A purification of ρ_B is given by

$$|\psi\rangle_{BE} = \sum_x \sqrt{p(x)}|x\rangle_B \otimes |x\rangle_E,$$

where E is an auxiliary system.
The tripartite state becomes

$$\rho_A \otimes |\psi\rangle\langle\psi|_{BE}.$$

After measurement, the post-measurement state is:

$$\rho_{XE} = \sum_x p(x)|x\rangle\langle x|_X \otimes |x\rangle\langle x|_E.$$

In this example, the conditional entropy $H(X|E) = 0$, showing that the measurement produces no intrinsic randomness. Furthermore, Eve does not need to share entanglement with ρ_A, as the classical-quantum state ρ_{XE} is independent of ρ_A.

The authors presented an intriguing result, demonstrating that the optimization problem can be effectively addressed by focusing on the set of extremal rank-one POVMs, as outlined in the following Lemma.

Lemma 3.1 Reduction to extremal rank-one POVMs. let $\rho_A \in D(A)$. Then,

$$R_H^{\text{POVM}}(\rho_A) = \sup_{\text{Extremal rank-one}} \{M_x\}_x \, I_H^{\text{POVM}}(\rho_A, \{M_x\}_x).$$

It is shown that a sequence of extremal rank-one POVMs can be constructed to achieve an intrinsic randomness rate that approaches $R_H^{\text{POVM}}(\rho_A)$. However, the limiting POVM of this sequence is non-extremal and exhibits an intrinsic randomness rate significantly lower than $R_H^{\text{POVM}}(\rho_A)$. Experimentally, this implies that even slight noise or imperfections in the measurement process can significantly impact the security and reliability of the extracted randomness.
To address this, one potential approach involves devising an attack strategy against Eve by constructing a probabilistic combination of the trivial measurement and an extremal rank-one POVM. Another intriguing possibility is to investigate whether a general POVM can be decomposed into a probabilistic combination of extremal POVMs. This decomposition could provide new insights into maximizing intrinsic randomness while maintaining practical robustness against experimental imperfections. Using the convexity of the intrinsic randomness, it is established that if $\{M_x\}$ and $\{N_x\}$ are two extremal rank-one POVMs, an upper bound on the intrinsic randomness of their convex combination can be computed.

4 Results

4.1 Analytical Results

This section explores the transition between a trivial POVM and an extremal rank-one POVM by analyzing their probabilistic convex combination:

$$L_x = (1-p)|x\rangle\langle x| + p\frac{I}{d_A},$$

where $M_x = |x\rangle\langle x|$ is the extremal rank-one POVM, $N_x = \frac{I}{d_A}$ is the trivial POVM, and $p \in [0,1]$ is the mixing parameter.
For a qubit system, the input state is defined as:

$$\rho_A = |+\rangle\langle +|.$$

The isometry $V : A \to AB$ is given by:

$$V = \sum_x \sqrt{M_x} \otimes |x\rangle.$$

The joint state ρ_{AB} is computed as:

$$\rho_{AB} = V\rho_A V^\dagger,$$

where $V^\dagger$ is the adjoint of V. The purification of ρ_{AB} is:

$$|\psi_{ABE}\rangle = \sum_i \sqrt{\lambda_i}|v_i\rangle|v_i\rangle,$$

where λ_i are the eigenvalues and $|v_i\rangle$ are the eigenstates of ρ_{AB}. Here, $|\psi_{ABE}\rangle$ captures the purified state, with $|v_i\rangle$ forming an orthonormal basis in the auxiliary space E.
The projective operator is defined as:

$$P_x = I_A \otimes |x\rangle\langle x|.$$

After measurement, the resulting state is:

$$\rho_{XE} = \sum_x |x\rangle\langle x| \otimes \mathrm{Tr}_{AB}\left[(P_x \otimes I_E)\,\rho_{ABE}\right].$$

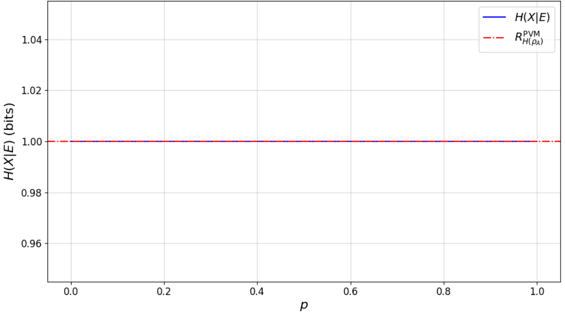

Figure 4.1: The intrinsic randomness compared to $R_H^{\mathrm{PVM}}(\rho_A)$ for the state $\rho_A = |+\rangle\langle +|$.

The numerical calculation indicates that the conditional entropy remains constant, equal to the maximum intrinsic randomness. This outcome is surprising and warrants further investigation. I attempted to verify the correctness of the implementation, and it appears that the canonical dilation may not be the optimal approach for this computation.
Additionally, performing the calculation across all possible Naimark dilations proves to be challenging. This complexity raises concerns about the potential power Eve could control from these results, which remains difficult to assess fully.

We define the following elements:

$$\sigma_B = |0\rangle\langle 0|, \quad P_x = |x\rangle\langle x| \otimes |0\rangle\langle 0|, \quad Q_x = I_A \otimes |x\rangle\langle x|, \quad \tau_B = \frac{I}{2}.$$

In this context, $(\{P_x\}_x, \sigma_B)$ is a Naimark dilation of $\{M_x\}_x$, while $(\{Q_x\}_x, \tau_B)$ is a dilation of $\{N_x\}_x$.
For $p \in [0, 1]$, the combined state is defined as:

$$\omega_{BF} = (1-p)\sigma_B \otimes |0\rangle\langle 0|_F + p\tau_B \otimes |1\rangle\langle 1|_F.$$

The projective measurement on ABF is expressed as:

$$R_x = P_x \otimes |0\rangle\langle 0|_F + Q_x \otimes |1\rangle\langle 1|_F.$$

This setup dilates the mixed measurement $\{(1-p)M_x + pN_x\}_x$.
The purification of ω_{BF} is given by:

$$|\psi_{BFE}\rangle = \sqrt{1-p}|00\rangle|a_0\rangle + \sqrt{\frac{p}{2}}|01\rangle|a_1\rangle + \sqrt{\frac{p}{2}}|11\rangle|a_2\rangle,$$

where $\{|a_0\rangle, |a_1\rangle, |a_2\rangle\}$ forms an orthonormal basis in the auxiliary system E.
The initial state ρ_A remains pure. After measurement, the final state is:

$$\rho_{XE} = \sum_x |x\rangle\langle x| \otimes \mathrm{Tr}_{AB'}\left[(R_x \otimes I_E)\rho_{AB'E}\right],$$

where $\rho_{AB'E} = \rho_A \otimes |\psi\rangle\langle\psi|$.
For this example, the von Neumann conditional entropy is given by:

$$H(X|E) = 1 - p.$$

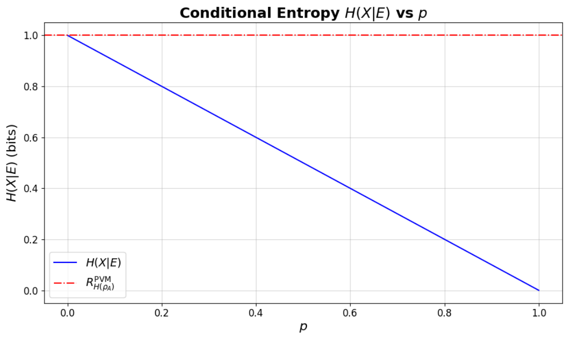

Figure 4.2: The intrinsic randomness compared to $R_H^{\mathrm{PVM}}(\rho_A)$ for the state $\rho_A = |+\rangle\langle +|$.

As the probability p increases, we approach the trivial measurement where Eve's control over the state grows, leading to a decrease in the intrinsic randomness. This is reflected in the decrease of the conditional entropy $H(X|E)$, which approaches 0 as p tends to 1, indicating less uncertainty and more control by Eve.

It becomes particularly interesting to analyze a more general state ρ_A, which can be expressed in its eigenbasis. Consider the qubit state $\rho_A \in D(\mathbb{C}^2)$, which admits a spectral decomposition given by

$$\rho_A = \lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1|,$$

with $\lambda_0 > \frac{1}{2}$. As demonstrated in [3], the parameterized POVM $\{|\psi_x(t)\rangle\langle\psi_x(t)|\}_x$, where $t \in [\frac{1}{2}, 1]$, is defined as:

$$\begin{aligned}
|\psi_0(t)\rangle &= \sqrt{\frac{1}{2t}}|0\rangle, \\
|\psi_1(t)\rangle &= \sqrt{\frac{4t-1}{12t}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle, \\
|\psi_2(t)\rangle &= \sqrt{\frac{4t-1}{12t}}|0\rangle + \frac{1}{\sqrt{3}}e^{\frac{2i\pi}{3}}|1\rangle, \\
|\psi_3(t)\rangle &= \sqrt{\frac{4t-1}{12t}}|0\rangle + \frac{1}{\sqrt{3}}e^{\frac{4i\pi}{3}}|1\rangle.
\end{aligned}$$

This POVM achieves the intrinsic randomness $\mathcal{R}_H^{\mathrm{POVM}}(\rho_A)$ when $t = \lambda_0$, which corresponds to the largest eigenvalue of ρ_A. The calculation of the randomness utilizes the von Neumann entropy, emphasizing the optimality of the parameterization in this case.

We apply the same strategy as before, aiming to map the extremal POVM to the trivial one. This process leads to the following expression:

$$L_x = (1-p)|\psi_x\rangle\langle\psi_x| + p\frac{I}{4}, \quad \text{where } x \in \{0,1,2,3\}.$$

Using this framework, we can construct the corresponding Naimark dilation, which is given by:

$$R_x = P_x \otimes |0\rangle\langle 0|_F + Q_x \otimes |1\rangle\langle 1|_F,$$

where:

$$P_x = |\psi_x\rangle\langle\psi_x| \otimes |0\rangle\langle 0|, \quad Q_x = I_A \otimes |\psi_x\rangle\langle\psi_x|.$$

The purification of the state ω_{BF}, defined similarly to the earlier case, is given by:

$$|\psi_{BFE}\rangle = \sqrt{1-p}\,|00\rangle|0\rangle + \sqrt{\frac{p}{4}}\,|\phi^+\rangle|1\rangle,$$

where $|\phi^+\rangle$ denotes the Bell state.

Additionally, we incorporate a purification of ρ_A, expressed as:

$$|\psi_{AE}\rangle = \sqrt{\lambda_0}|00\rangle + \sqrt{\lambda_1}|11\rangle.$$

Finally, the combined tripartite state ρ_{ABE} is given by:

$$\rho_{ABE} = |\psi_{AE}\rangle\langle\psi_{AE}| \otimes |\psi_{B'E}\rangle\langle\psi_{B'E}|,$$

where we treat systems B and F as a single composite system B'.

The state post-measurement is described by the same expression as in the previous cases.

The figure below illustrates the behavior of the conditional entropy $H(X|E)$ as a function of p for three different values of λ. It demonstrates how the conditional entropy decreases as p increases.

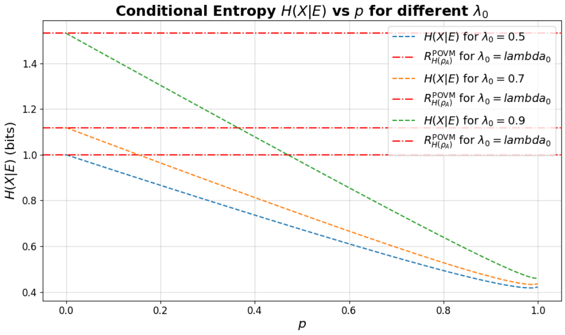

Figure 4.3: Conditional entropy $H(X|E)$ as a function of p for different values of λ for the state $\rho_A = \lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1|$.

Key observations include:

- For $p = 0$, where the POVM is fully extremal, the conditional entropy $H(X|E)$ coincides with the maximum intrinsic randomness achievable using extremal POVMs.
- The conditional entropy appears to decrease linearly as p increases, irrespective of λ, eventually reaching a value of 0.4 bits when $p = 1$.
- The observed limit of 0.4 bits for $p = 1$ reflects a specific property of the decomposition process. Further investigation is needed to provide a complete explanation for this limiting behavior.

This trend highlights the dependence of conditional entropy on the mixing parameter p and reinforces the interplay between extremal and trivial POVMs in determining intrinsic randomness.
This result provides a concrete example of how randomness depends on the relative weights of the trivial and extremal components. The ability to explicitly calculate $H(X|E)$ for this combination not only provides a benchmark for comparing more complex decompositions or POVMs but also highlights a specific type of linear attack by Eve. This raises a critical question: what if Eve could implement a more sophisticated, non-linear strategy, such as a logarithmic attack, to exploit the structure of the POVM? Exploring this could help us understand how robust intrinsic randomness is against different types of attacks and reveal weaknesses in current randomness extraction methods.

4.2 Numerical Results

This section is based on the work [4], which demonstrates that any POVM can be decomposed into a convex combination of extremal rank-one POVMs.
We are given a rank-1 POVM $P_N = \{a_i E_i\}$, where E_i are normalized operators and $a_i > 0$. The goal is to express this POVM as a convex combination of rank-1 POVMs, specifically as:

$$P_N = \sum_k p_k P(k)_n,$$

Where p_k are positive coefficients and $P(k)_n$ represents the decomposition of the original POVM into a convex combination of rank-1 POVMs.
To construct a POVM with N outcomes using rank-1 operators, we begin by considering a set of n arbitrary rank-1 operators $\{E_i\}$. Our goal is to determine a set of positive coefficients $\{a_i\}$ such that the following condition holds:

$$\sum_{i=1}^{n} a_i E_i = I,$$

Where I is the identity operator. This equation ensures that the sum of the rank-1 operators, weighted by the coefficients a_i, forms a valid POVM. The coefficients a_i must be positive to guarantee the positivity of the operators and ensure the validity of the POVM.
The next step is to determine the coefficients a_i by solving a linear program. This is done under the constraints imposed by the Bloch sphere representation and the identity condition. Specifically, the linear program must ensure that the weighted sum of the rank-1 operators E_i produces the identity matrix I, while respecting the geometric constraints of the Bloch sphere. These constraints ensure that the operators E_i remain valid quantum measurement elements.
The next step is to determine the coefficients a_i by solving an iterative linear program. At each iteration, the program is adjusted to satisfy the constraints of the Bloch sphere representation and the identity condition. The process continues until we reach a unique solution, where the POVM cannot be decomposed further. If the POVM isn't rank-one, we use its spectral decomposition to treat it as new elements in the POVM.

Exemple:
Consider the POVM with five outcomes:

$$P = \left\{ \frac{2}{5}E_1, \frac{2}{5}E_2, \frac{2}{5}E_3, \frac{2}{5}E_4, \frac{2}{5}E_5 \right\},$$

The E_i are rank-1 projectors located on the Bloch sphere's equator. Selecting the trine formed by elements 1, 3, and 4, the original POVM can be written as:

$$P = pP^{(1)} + (1-p)P^{(\text{aux})},$$

where

$$p = \frac{1}{5},$$

and

$$P^{(1)} = \left\{ \frac{2}{\sqrt{5}}E_1, 0, \left(1 - \frac{1}{\sqrt{5}}\right)E_3, \left(1 - \frac{1}{\sqrt{5}}\right)E_4, 0 \right\}.$$

$$P^{(\text{aux})} = \left\{ 0, \frac{2}{5-\sqrt{5}}E_2, \frac{3-\sqrt{5}}{5-\sqrt{5}}E_3, \frac{3-\sqrt{5}}{5-\sqrt{5}}E_4, \frac{2}{5-\sqrt{5}}E_5 \right\}$$

We iterate the decomposition until the original 5-outcome POVM is expressed as a convex combination of 3-outcome POVMs. Finally, the 5-outcome POVM can be written as

$$P = p_1P^{(1)} + p_2P^{(2)} + p_3P^{(3)},$$

where

$$P^{(2)} = \left\{0, \left(1-\frac{1}{\sqrt{5}}\right)E_2, \left(1-\frac{1}{\sqrt{5}}\right)E_4, 0, \frac{2}{\sqrt{5}}E_5\right\}$$

$$P^{(3)} = \left\{0, \frac{2}{\sqrt{5}}E_2, 0, \left(1-\frac{1}{\sqrt{5}}\right)E_4, \left(1-\frac{1}{\sqrt{5}}\right)E_5\right\}$$

and p_1, p_2, p_3 are appropriate weights for the 3-outcome POVMs.

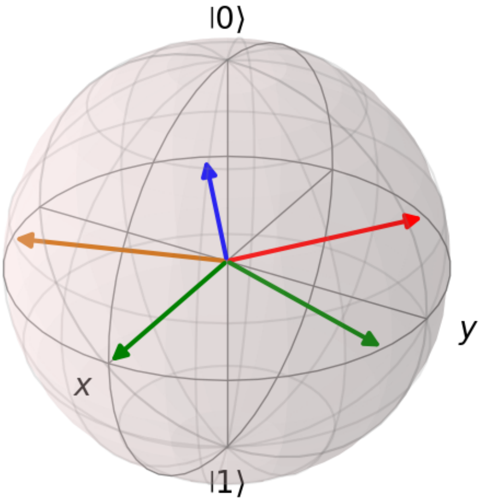

Figure 4.4: The Bloch sphere representation of the selected POVM.

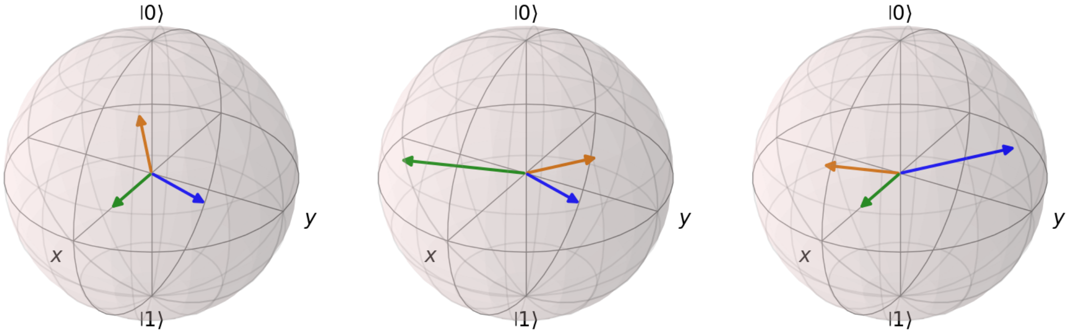

Figure 4.5: **Decompositions:** The three decompositions of the POVM elements with corresponding probabilities:
(a) The POVM elements $\{E_1, E_3, E_4\}$ are chosen with probability $p_1 = 0.4472$,
(b) The POVM elements $\{E_2, E_4, E_5\}$ are chosen with probability $p_2 = 0.2764$,
(c) The POVM elements $\{E_2, E_3, E_5\}$ are chosen with probability $p_2 = 0.2764$.

Note that the POVM elements have varying weights, as shown in Figure 4.5, and the algorithm functions as explained in the article. Since many measurement optimization problems involve maximizing a specific objective, which leads to an optimal solution, this decomposition method shows great potential.

During the implementation of the decomposition algorithm, I encountered several challenges in testing and ensuring the correctness of the results. Although initial tests with simple, well-known POVMs showed that the algorithm was working for basic cases, there were issues when dealing with more complex and non-rank-one POVMs. Specifically, errors arose in the iterative steps, and the algorithm sometimes failed to produce the expected results, especially when handling the spectral decomposition of non-rank-one POVMs
Additionally, I implemented an algorithm to compute the conditional entropy $H(X \mid E)$ by finding the best decomposition that maximizes intrinsic randomness. While this approach showed potential, issues remain, particularly in computing ρ_{XE}. Despite these limitations, the method demonstrates the feasibility of using the decomposition for computing conditional entropy, though further refinement is necessary.

5 Conclusion

This project examined the decomposition of POVMs to compute conditional entropy and establish benchmarks for the upper bounds of intrinsic randomness. An analytical approach was first pursued, exploring a convex combination between the trivial measurement and extremal rank-1 projectors to deepen the understanding of POVM structures. Additionally, an algorithm was implemented to decompose arbitrary POVMs into extremal rank-1 projectors while ensuring completeness and positivity constraints were satisfied.

Numerical instabilities, particularly in complex computational cases, posed challenges and affected the reliability of results for certain examples.

For future work, the algorithm could be adjusted to handle general POVMs more effectively, addressing challenges posed by numerical instabilities. Additionally, exploring scenarios with more powerful adversaries, especially those without constraints on the dimensionality of the Naimark dilation, could provide a deeper understanding of the security and robustness of the approach.

Bibliography

[1] Miguel Herrero-Collantest and Juan Carlos Garcia-Escartin. Quantum random number generators.Reviews of Modern Physics,89(1):015004,(2017).

[2] Meng, Shuyang and Curran, Fionnuala and Senno, Gabriel and Wright, Victoria and Farkas, Mátė and Scarani, Valerio and Acín, Antonio. "Maximal intrinsic randomness of a quantum state" (2023).

[3] Anco, Kriss Gutierrez, Tristan Nemoz, and Peter Brown. "How much secure randomness is in a quantum state?." arXiv preprint arXiv:2410.16447 (2024).

[4] G. Sent´ıs, B. Gendra, S. D. Bartlett,= and A. C. Doherty. Decomposition of any quantum measurement into extremals. (2013)