MAXIMAL INTRINSIC RANDOMNESS OF A QUANTUM STATE

Maissa Beji
Supervised by : Peter Brown

INTRODUCTION

The promise of quantum randomness

Quantum random number generation (QRNG)

Quantum Key Distribution (QKD)

How to secure and quantify this randomness?

Researchers: Optimizing conditional entropy to tackle eavesdroppers and make scenarios more practical!

$H(X|E)$

Challenges:

- Generating secure random bits despite Eve entanglement with the state and the measurement
- Implementing optimal POVMs for randomness extraction amid experimental imperfections

OVERVIEW OF PREVIOUS WORK

Scenario 1: Projective Measurements (PVM)s

Source state ρ_A

Projective Measurement $\{M_x\}_x$

X

Classical random variable

Eavesdropper E

Bipartite state with side info $\boldsymbol{\rho_{AE}}$, Where $Tr(\rho_{AE}) = \rho_A$

The CQ-state after measurement:

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

Where $\rho_{E,x} = Tr[(\boldsymbol{M_x} \otimes \boldsymbol{I})\, \rho_{AE}]$

How can we assess Eve's knowledge to ensure that the measurement outcome is genuinely random?

We minimise over all possible E system the conditional entropy $H(X|E)$.

Key result: The optimization can be restricted to **rank-one PVMs.**

OVERVIEW OF PREVIOUS WORK

Scenario 2: POVMs

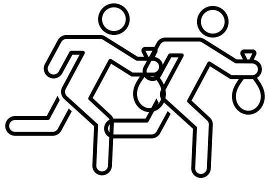
Source state ρ_A

POVM $\{M_x\}_x$

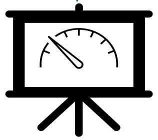
X

classical random variable

Naimark's dilation



Eavesdropper E



$(\{P_x\}_x, \sigma_B)$

The shared state ρ_{ABE},
Where $Tr_{BE}(\rho_{ABE}) = \rho_A$

Where $Tr_B(P_x(I_A \otimes \sigma_B)) = M_x$

The CQ-state after measurement:

$$\rho_{XE} = \sum_x |x\rangle\langle x| \otimes Tr_{AB}\big((P_x \otimes I_E)\rho_{ABE}\big)$$

The intrinsic H-randomness is optimizing $H(X|E)$ over all extensions of ρ_A **AND** over all Naimark dilations of $\{M_x\}$

OVERVIEW OF PREVIOUS WORK

Scenario 2: POVMs

How can we assess Eve's knowledge to ensure that the measurement outcome is genuinely random?

Key result: The optimization can be restricted to **rank-one extremal POVMs.**

However: Intrinsic randomness **isn’t continuous** for POVMs with a fixed source state, requiring impractically high precision to implement.

Key questions:

- Can we find **robust POVMs** that avoid these discontinuities while maintaining high randomness rates?
- Can decomposing a POVM into extremals offer a better upper bound on randomness?

PROBLEM STATEMENT

Definitions

Definition 1: Intrinsic H-randomness

Let ρA ∈ D(A) and let {Mx}x be a POVM on the system A. Then the intrinsic H-randomness of the pair (ρA, {Mx}x) is defined as:

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

Subject to the constraints:

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

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

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

Definition 2: Maximal Intrinsic H-randomness

Let ρA ∈ D(A) and let H be a conditional entropy. Then we define the maximal intrinsic H-randomness of ρA as:

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

PROBLEM STATEMENT

Example: The trivial measurement

Let's consider the following POVM measurement:

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

Naimark's dilation theorem :

$$P_x = I_A \otimes |x\rangle\langle x| \quad \rho_B = \sum_x p(x)|x\rangle\langle x|.$$

Where Px the PVM acting on A ⨂ B and ρB the state of the system B

A purification of ρB is given by

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

The tripartite state becomes

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

the post-measurement state is:

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

$$H(X|E) = 0$$

PROBLEM STATEMENT

An important Lemma

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

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

- Extremal rank-one POVMs can approach $R_H^{POVM}(\rho_A)$, but the limiting POVM is non−extremal with **lower randomness.**
- Noise or imperfections in measurements reduce the security and reliability of randomness.

RESULTS

Attack Strategy: Combining Trivial and Extremal POVMs

Let's consider a probabilistic convex combination of between **trivial POVM** and a **PVM**

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

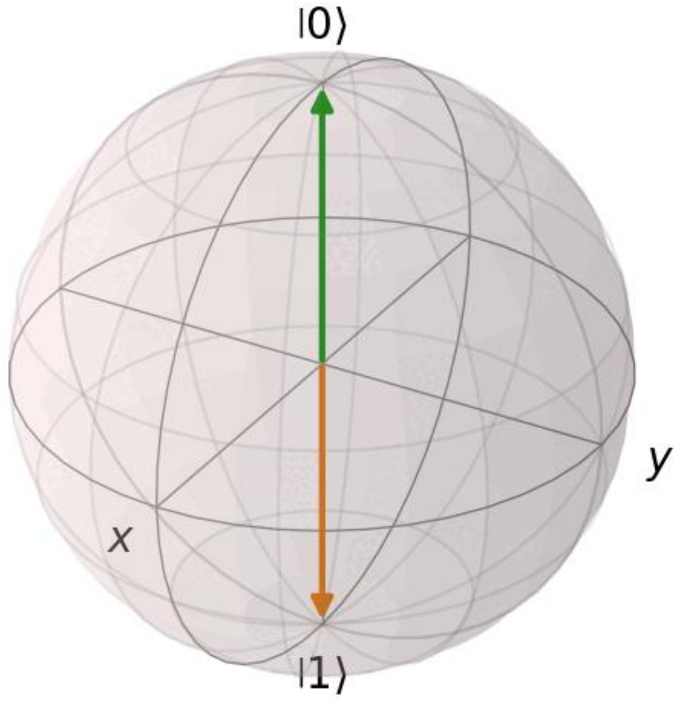
Key Elements and Definitions:

$$\sigma_B = |0\rangle\langle 0|, \quad P_x = |x\rangle\langle x| \otimes |0\rangle\langle 0|,$$

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

({Px}x , σB) is Naimark dilation of {Mx}x

({Qx}x , τB) is a dilation of {Nx}x



RESULTS

Attack Strategy: Combining Trivial and Extremal POVMs

Let's consider a probabilistic convex combination of between trivial POVM and a PVM

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

Key Elements and Definitions:

$$\sigma_B = |0\rangle\langle 0|, \quad P_x = |x\rangle\langle x| \otimes |0\rangle\langle 0|,$$

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

({Px}x , σB) is Naimark dilation of {Mx}x

({Qx}x , τB) is a dilation of {Nx}x

Combined State and Measurement:

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

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

Purification and Final State:

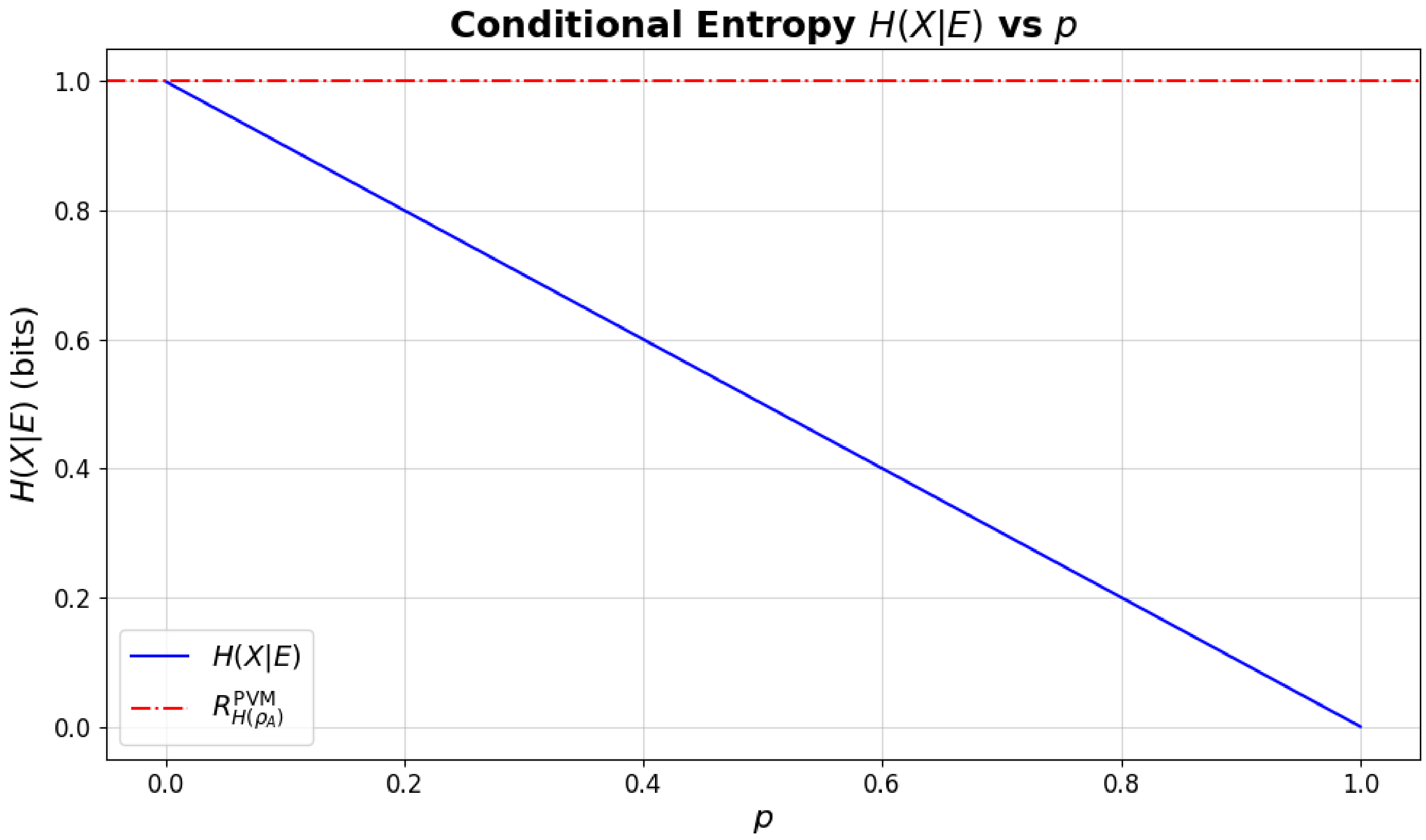
$$|\psi_{BFE}\rangle = \sqrt{1-p}|00\rangle|a_0\rangle + \sqrt{\frac{p}{2}}|01\rangle|a_1\rangle + \sqrt{\frac{p}{2}}|11\rangle|a_2\rangle,$$

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

$H(X|E) = 1 - p$ for
ρA = |+⟩⟨+|.

RESULTS

Attack Strategy: Combining Trivial and Extremal POVMs



RESULTS

Attack Strategy: Combining Trivial and Extremal POVMs

Let's consider a probabilistic convex combination of between **trivial POVM** and an **extremal rank-one POVM.**

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

For the state: $\rho_A = \lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1|,$

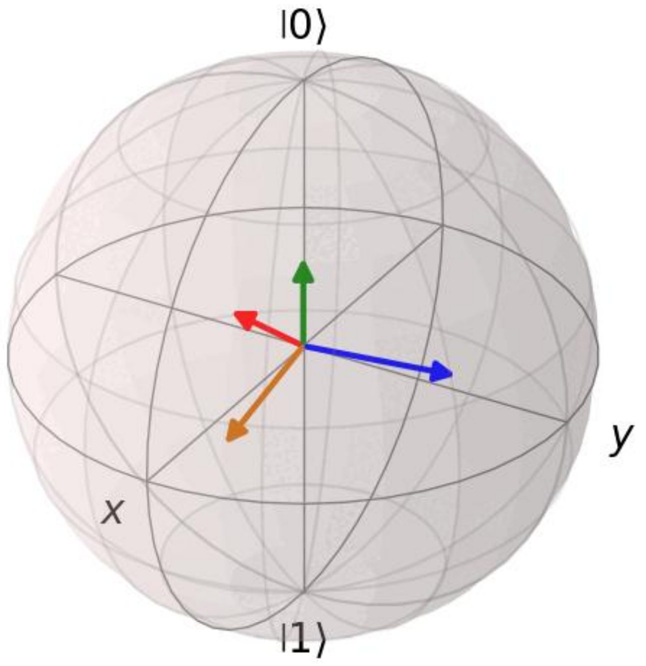
Where the parameterized POVM {|ψx (t)⟩⟨ψx (t)|}x , where t ∈ [1 2 , 1], is defined as:

$$|\psi_0(t)\rangle = \sqrt{\frac{1}{2t}}|0\rangle,$$

$$|\psi_1(t)\rangle = \sqrt{\frac{4t-1}{12t}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle,$$

$$|\psi_2(t)\rangle = \sqrt{\frac{4t-1}{12t}}|0\rangle + \frac{1}{\sqrt{3}}e^{\frac{2i\pi}{3}}|1\rangle,$$

$$|\psi_3(t)\rangle = \sqrt{\frac{4t-1}{12t}}|0\rangle + \frac{1}{\sqrt{3}}e^{\frac{4i\pi}{3}}|1\rangle.$$



RESULTS

Attack Strategy: Combining Trivial and Extremal POVMs

Combined State and Measurement:

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

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

$$\omega_{BF} = (1-p)|0\rangle\langle 0|_B \otimes |0\rangle\langle 0|_F + \frac{p}{4} I \otimes |1\rangle\langle 1|_F$$

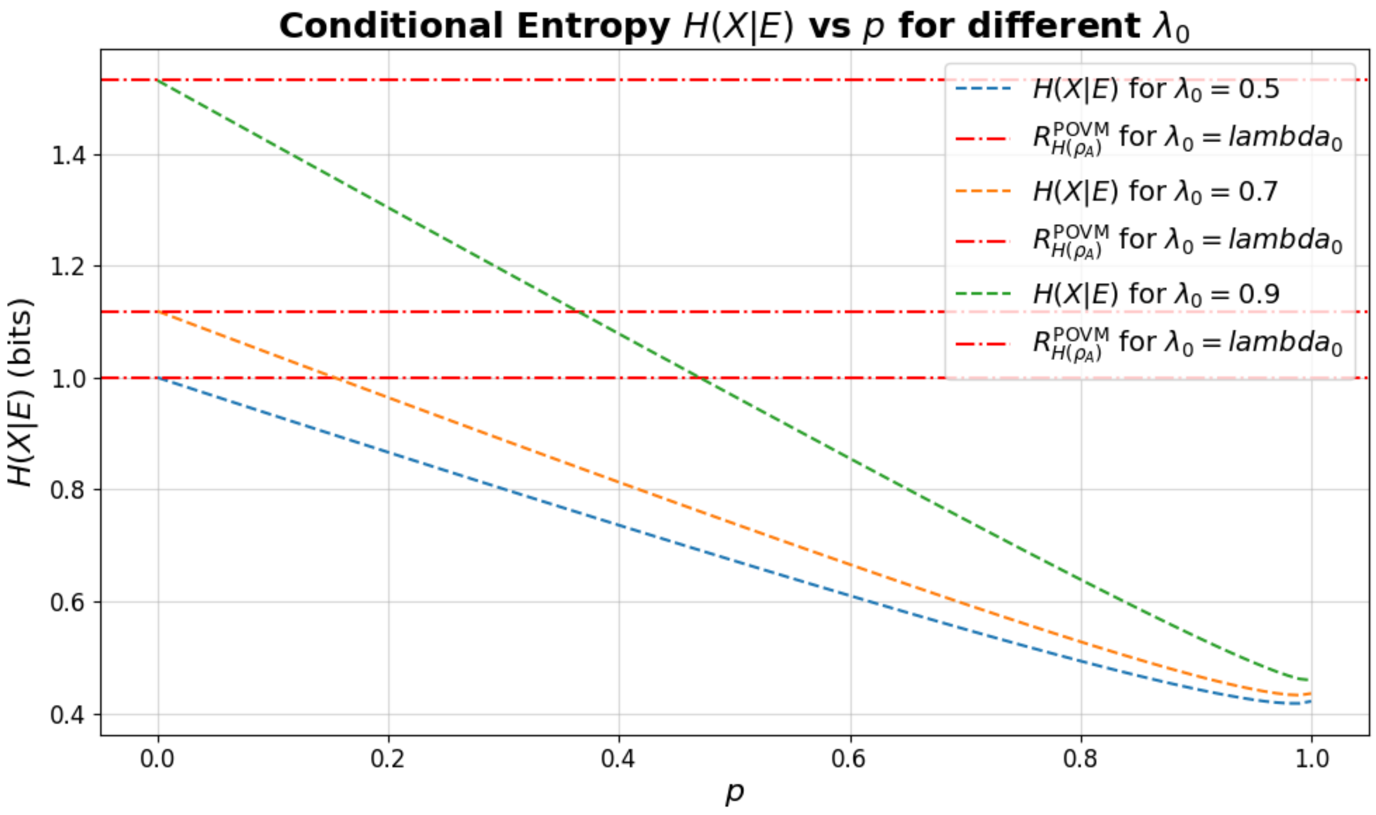
Purification and Final State:

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

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

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

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



RESULTS

POVM Decomposition into Extremal Rank-One POVMs

1. **Problem Setup**
   - Given a rank-1 POVM $\{a_i E_i\}$
   - **Goal:** decompose as

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

2. **Formulating the decomposition**
   - Start with n arbitrary rank-1 operators $\{E_i\}$
   - Find coefficients $\{a_i\}$ such that:

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

3. **Linear Programming**
   - Solve a linear program to determine a_i under two constraints:
     - **Identity condition**: Weighted sum equals I.
     - **Bloch sphere representation**: Ensures E_i remain valid quantum elements
4. **Iterative Refinement**
   - Adjust the linear program at each step to satisfy constraints.
   - Repeat until decomposition reaches a unique solution.

RESULTS

POVM Decomposition into Extremal Rank-One POVMs

Example: Pentagonal POVM on the Bloch Sphere's Equator

Consider the POVM with five outcomes: P $= \{\frac{2}{5}E_1, \frac{2}{5}E_2, \frac{2}{5}E_3, \frac{2}{5}E_4, \frac{2}{5}E_5\}$

The E_i are rank-1 projectors located on the Bloch sphere's equator.

First step gives the following outcome:

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

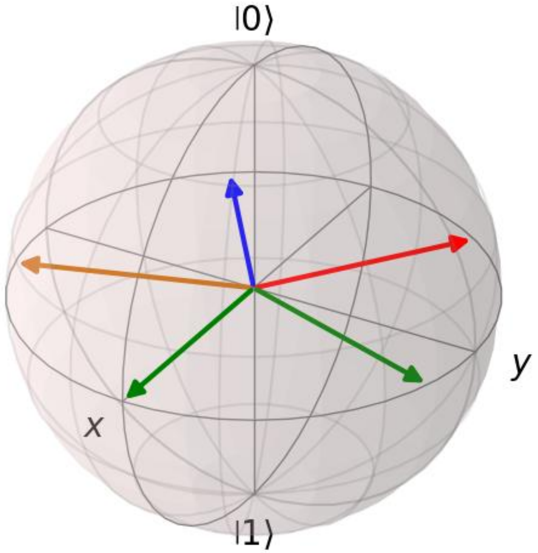
where

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

and

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

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



RESULTS

POVM Decomposition into Extremal Rank-One POVMs

Example: Pentagonal POVM on the Bloch Sphere's Equator

Consider the POVM with five outcomes: P $= \{\frac{2}{5}E_1, \frac{2}{5}E_2, \frac{2}{5}E_3, \frac{2}{5}E_4, \frac{2}{5}E_5\}$

The E_i are rank-1 projectors located on the Bloch sphere's equator.

We repeat until we find :

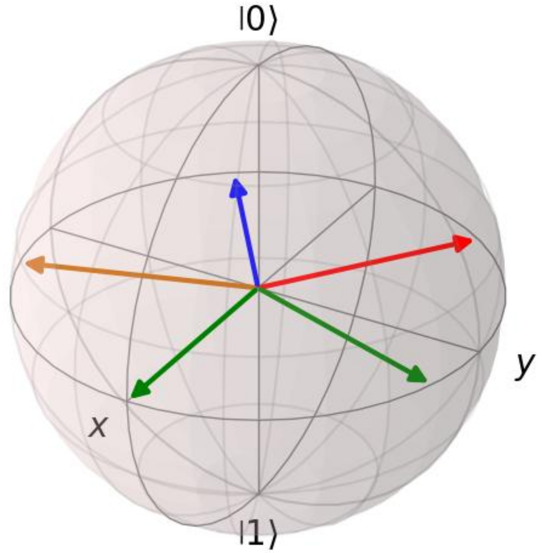
$$P = p_1 P^{(1)} + p_2 P^{(2)} + p_3 P^{(3)},$$

where

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

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

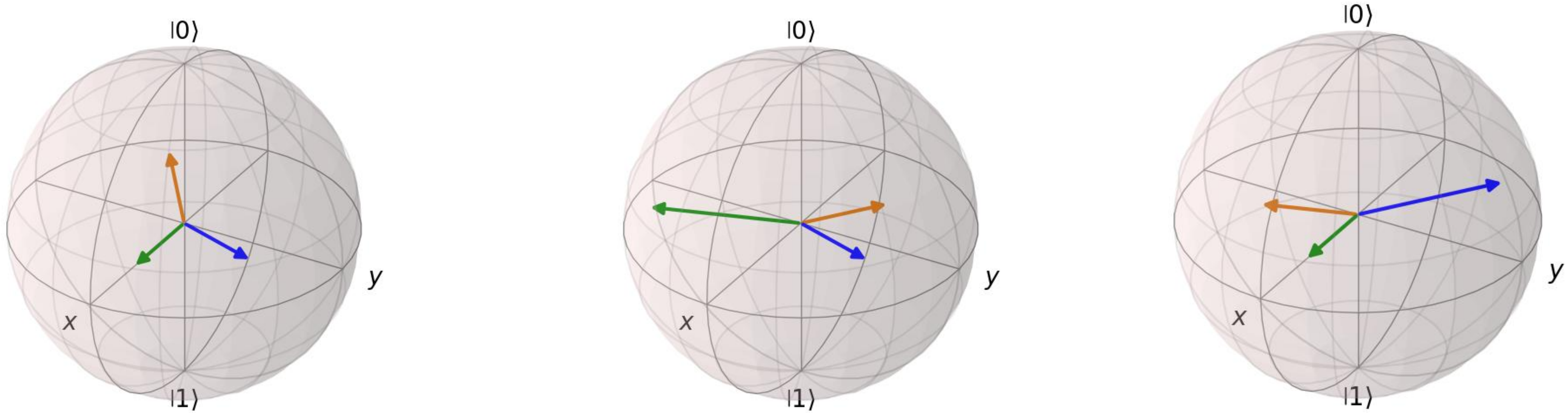
and p_1, p_2, p_3 are appropriate weights for the 3-outcome POVMs.



RESULTS

POVM Decomposition into Extremal Rank-One POVMs

Example: Pentagonal POVM on the Bloch Sphere's Equator



(a) The POVM elements {E1, E3, E4} are chosen with probability p1 = 0.4472,
(b) The POVM elements {E2, E4, E5} are chosen with probability p2 = 0.2764,
(c) The POVM elements {E2, E3, E5} are chosen with probability p2 = 0.2764.

CONCLUSION

- Used convex combinations of trivial and extremal rank-1 projectors to analyze POVM structures.
- Implemented an algorithm to decompose POVMs while maintaining completeness and positivity.
- Numerical instabilities in complex cases affected result reliability.
- Future work could improve the algorithm for general POVMs and explore stronger adversaries especially for Naimark's dilation.

THANK YOU FOR YOUR ATTENTION