On the value of the XOR monogamy-of-entanglement game

Krishna Agaram

July 2025

As done in [TFKW13], any malicious position verification strategy can be transformed into a strategy of the BB84 monogamy-of-entanglement game (albeit with ρ_{ABC} restricted to satisfy $\rho_A = I/2^n$), yielding parallel-repetition soundness for 2-verifier 1-prover PMIPs.

As remarked earlier, a natural choice of randomness given that each bit x_i of the challenge is known only partially to provers would be the exclusive-or or XOR of the bits x_i, and one might expect the exclusive-or to be almost uniformly random given only partial information about each x_i. However, we show that this is not the case. In particular, it turns out that in the BB84 monogamy game, the exclusive-or of the n bits $\{ x_i \}_{i=1}^n$ can be guessed with probability around 85% for *every* $n \in \mathbb{N}$. We establish this using the notion of ZX-compatibility, which we introduce in Section 2.2 and which may be of independent interest, especially in the context of Pauli algebras.

Remark. Before the authors could publish this result, it was rediscovered by Coladangelo, Liu and Xie [CLX25] using a different approach. However, our approach may still be of independent interest for the notion of ZX-compatibility and the recursive structure of the optimal strategy for the XOR game.

Contents

1 Monogamy-of-entanglement games

1.1 Preliminaries

Definition 1.1 (monogamy-of-entanglement game [TFKW13]). *A monogamy-of-entanglement game G consists of a finite-dimensional Hilbert space $\mathcal{H}_\mathcal{A}$ and a list of measurements $M_\theta = \{F_x^\theta\}_{x\in\mathcal{X}}$ on $\mathcal{H}_\mathcal{A}$, indexed by $\theta \in \Theta$, where X and Θ are finite sets.*

A monogamy game is interpreted as being played by three parties A, B, and C with B and C attempting to independently guess the outcome of A's measurement.

Definition 1.2 (allowed strategies in a monogamy-of-entanglement game). *A strategy s for a monogamy game F is a tuple*

$$s = (\rho_{ABC}, \{P_b^\theta\}_{b,\theta}, \{Q_c^\theta\}_{c,\theta}, \varphi_\mathcal{B}, \varphi_\mathcal{C})$$

with $\rho_{ABC} \in \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B} \otimes \mathcal{H}_\mathcal{C}$, $\{P_b^\theta\}_b$ (resp. $\{Q_c^\theta\}_c$) being a POVM on $\mathcal{H}_\mathcal{B}$ (resp. $\mathcal{H}_\mathcal{C}$) for each θ, and $\varphi_\mathcal{B}$ (resp. $\varphi_\mathcal{C}$) a function assigning each pair (θ, b) (resp. (θ, c)) an element $x \in \mathcal{X}$ representing the response of B (resp. C) upon receving measurement outcome b (resp. c) given θ.

Consider a strategy $s = (\rho_{ABC}, \{P_b^\theta\}_{b,\theta}, \{Q_c^\theta\}_{c,\theta}, \varphi_\mathcal{B}, \varphi_\mathcal{C})$. For each θ, we define

$$P_x^\theta = \sum_{\substack{b\in\mathcal{H}_\mathcal{B} \\ \varphi_\mathcal{B}(\theta,b)=x}} P_b^\theta \quad \text{and} \quad Q_x^\theta = \sum_{\substack{c\in\mathcal{H}_\mathcal{C} \\ \varphi_\mathcal{C}(\theta,c)=x}} Q_c^\theta.$$

(Note the overload of the subscript of P and Q; this is almost always unambiguous in our exposition and we shall point out the distinction when necessary.)

Remark. Notice that for each θ, the positive operators P_x^θ and Q_x^θ still sum over $x \in \mathcal{X}$ to the identity: they may be viewed as positive operators on a virtual Hilbert space isomorphic to $\mathcal{X}$.

Given particular θ, the probability of B and C winning the game F is

$$\operatorname{tr}\left(\Pi^\theta \rho_{ABC}\right) \qquad \text{where} \qquad \Pi^\theta = \sum_{x\in\mathcal{X}} F_x^\theta \otimes P_x^\theta \otimes Q_x^\theta.$$

The overall probability of winning the game is then the expected win probability over the uniform distribution of θ:

$$\mathsf{p}_{\mathsf{win}}(G, \mathcal{S}) = \frac{1}{|\Theta|} \sum_{\theta\in\Theta} \operatorname{tr}\left(\Pi^\theta \rho_{ABC}\right).$$

In the BB84 monogamy game, the measurements on $\mathcal{H}_\mathcal{A}$ are given by

$$F_x^\theta = |x^\theta\rangle \langle x^\theta| \quad \text{for } x \in \{0,1\}, \theta \in \{0,1\}.$$

Parallel Repetition: The parallel repetition of a monogamy game is defined naturally by the measurements F_x^θ being replaced by $F_x^{\theta_1} \otimes F_x^{\theta_2} \otimes \cdots \otimes F_x^{\theta_n}$, and the state ρ_{ABC} now belonging to $\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. However, we do not require that the measurements P_x^θ and Q_x^θ be factorizable into tensor products of measurements based on individual θ_i.

1.2 The extractor game

An extractor game is a relaxed monogamy-of-entanglement game where parties B and C try to guess the value of a function (typically, non-injective) when applied to A's measurement result. The formal definition is as follows:

Definition 1.3 (extractor game)**.** *An extractor game is associated with a monogamy game G and an extractor function $f : \mathcal{X} \to \mathcal{Y}$, where $\mathcal{Y}$ is a finite set. The game consists of the same measurements as G, but the winning condition on θ is changed to*

$$\mathrm{tr}\left(\Pi^\theta \rho_{ABC}\right) \quad \textit{where } \Pi^\theta = \sum_{\substack{x_1,x_2,x_3\in\mathcal{X} \\ f(x_1)=f(x_2)=f(x_3)}} F^\theta_{x_1} \otimes P^\theta_{x_2} \otimes Q^\theta_{x_3}.$$

The probability of winning the game is identical to before, i.e.

$$\mathsf{p}_{\mathsf{win}}(G,\mathcal{S}) = \frac{1}{|\Theta|}\sum_{\theta\in\Theta} \mathrm{tr}\left(\Pi^\theta \rho_{ABC}\right).$$

Grouping by valuation, we can rewrite

$$\Pi^\theta = \sum_{y\in\mathcal{Y}} F^\theta_y \otimes P^\theta_y \otimes Q^\theta_y \quad \text{with } \Lambda^\theta_y = \sum_{x\in f^{-1}(y)} \Lambda^\theta_x \text{ for } \Lambda \in \{F,P,Q\}.$$

(Notice again the overload of the subscript of the measurement operators F, P and Q.)

The parallel-repetition xor-game, or xor-game for short, is defined as the extractor game on the parallel repetition of the BB84 game, with the extractor f being the exclusive-or function on $\mathcal{X} = \{0,1\}^n$, i.e. $f(x) := \oplus x \equiv x_1 \oplus \cdots \oplus x_n$.

In this work, we shall compute the value of the (parallely-repeated) xor-game. It is easy to see that the value is at most the value of the 1-qubit BB84 monogamy game: indeed, given a strategy s for the xor-game, consider the strategy s' for the single-qubit BB84 game where new adversary B' (resp. C') generates uniformly random bits $\theta_2,\ldots,\theta_n$ and $x_2,\ldots,x_n$, runs B (resp. C) internally, receiving output bit β (resp. γ) and outputs $x = \beta \oplus x_2 \oplus \cdots \oplus x_n$ (resp. $x = \gamma \oplus x_2 \oplus \cdots \oplus x_n$). This strategy may naturally be described all at once by a POVM, and it is easy to see that the win probability of s' for the BB84 game is equal to the win probability of s for the xor-game. Thus, we have

$$\mathsf{p}^{\mathrm{xor}}_{\mathsf{win}}(G,s) \leq \frac{1}{2} + \frac{1}{2\sqrt{2}} \equiv p_0.$$

We shall next establish a matching lower-bound by providing a family of strategies, one for each n, that achieves winning probability p.

2 Lower-bound on the value of the xor-game

2.1 Construction

It suffices for our purposes to consider deterministic, completely correlated strategies that may be described by a list of bits $p = (p_\theta)_{\theta\in\{0,1\}^n}$:

Definition 2.1 (Deterministic perfectly correlated strategy)**.** *To a string $p \in \{0,1\}^{2^n}$ indexed by $\theta \in \{0,1\}^n$, we associate the following strategy for the xor-game:*

- *The Hilbert spaces $\mathcal{H}_\mathcal{B}$ and $\mathcal{H}_\mathcal{C}$ are single-qubit spaces isomorphic to $\mathbb{C}^2$.*
- *The projectors P_b^θ are defined by*

$$P_0^\theta = (1 - p_\theta)\mathbb{I}_2 \equiv p_\theta^0 \mathbb{I}_2,$$
$$P_1^\theta = p_\theta \mathbb{I}_2 \equiv p_\theta^1 \mathbb{I}_2.$$

  Note that for each θ, one of the projectors is $\mathbf{0}$ and the other is $\mathbb{I}_2$. In particular, the outcome of the measurement is fully determined *by θ (hence the name deterministic strategy).*

- *The projectors Q_c^θ are equal to P_c^θ for each $c \in \{0,1\}$ and $\theta \in \{0,1\}^n$ (hence the name perfectly correlated).*
- *The state ρ_{ABC} is equal to $|v\rangle\langle v| \otimes \rho \otimes \rho$, where ρ is an arbitrary density matrix on $\mathcal{H}_\mathcal{B}$ and $|v\rangle = |v(p)\rangle$ is a carefully chosen vector in $\mathcal{H}_\mathcal{A}$ which we shall describe later.*
- *The function $\varphi_\mathcal{B}$ (resp. $\varphi_\mathcal{C}$) maps (θ, b) (resp. (θ, c)) to an arbitrarily chosen special element of $\mathcal{X} = \{0,1\}^n$ such that $b = \oplus x$ (resp. $c = \oplus x$). For example $x = 0^n$ when $b = 0$ and $x = 10^{n-1}$ when $b = 1$.*

We remark that much of the description of the strategy is quite arbitrarily chosen; the essential idea is that the adversaries B and C deterministically respond solely based on θ and rely on the state ρ_A to ensure that A's measurement outcome is very-likely the same as the deterministic response of B and C. Indeed, the choice of $|v\rangle$ in ρ_A is crucial to ensure that the win probability is maximized.

Denote $p_\theta^0 := 1 - p_\theta$ and $p_\theta^1 := p_\theta$. The projectors can then be succintly written

$$P_b^\theta = Q_b^\theta = p_\theta^b \mathbb{I}_2 \quad \text{for } b \in \{0,1\} \text{ and } \theta \in \{0,1\}^n.$$

The win probability for a strategy p is then given by:

,

$$\begin{aligned}
\mathsf{p}_{\mathsf{win}}^{\mathsf{xor}}(G,p) &= \frac{1}{2^n} \sum_{\theta \in \{0,1\}^n} \operatorname{tr}\left(\Pi^\theta \rho_{ABC}\right) \\
&= \frac{1}{2^n} \sum_{\theta \in \{0,1\}^n} \operatorname{tr}\left(\left(\sum_{x \in \{0,1\}^n} |x^\theta\rangle\langle x^\theta| \otimes p_\theta^{\oplus x}\mathbb{I}_2 \otimes p_\theta^{\oplus x}\mathbb{I}_2\right)(|v\rangle\langle v| \otimes \rho \otimes \rho)\right) \\
&= \frac{1}{2^n} \operatorname{tr}\left(\left(\sum_{\theta \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} p_\theta^{\oplus x} |x^\theta\rangle\langle x^\theta|\right)|v\rangle\langle v|\right). \qquad (1)
\end{aligned}$$

We shall simplify this further. Note that for each θ,

$$\sum_{x \in \{0,1\}^n} |x^\theta\rangle\langle x^\theta| = H^\theta \left(\sum_{x \in \{0,1\}^n} |x^\theta\rangle\langle x^\theta|\right) H^\theta = \mathbb{I}_{2^n}.$$

Multiplying both sides of Eq. (1) by 2 and subtracting $1 = \frac{1}{2^n}\mathrm{tr}\left(\mathbb{I}_{2^n}\right)$ yields

$$\begin{aligned}2\mathsf{p}_{\mathsf{win}}^{\mathrm{xor}}(G,p) - 1 &= \frac{1}{2^n}\mathrm{tr}\left(\left(\sum_{\theta\in\{0,1\}^n}\sum_{x\in\{0,1\}^n}\left(2p_\theta^{\oplus x}-1\right)|x^\theta\rangle\langle x^\theta|\right)|v\rangle\langle v|\right)\\ &= \frac{1}{2^n}\mathrm{tr}\left(\left(\sum_{\theta\in\{0,1\}^n}\sum_{x\in\{0,1\}^n}\sigma\left[2p_\theta^{\oplus x}\right]|x^\theta\rangle\langle x^\theta|\right)|v\rangle\langle v|\right),\end{aligned}$$

where $\sigma : \{0,1\} \to \{-1,+1\}$ is defined by $\sigma(0) = -1, \sigma(1) = 1$. Define

$$Z_p := \sum_{\theta\in\{0,1\}^n}\sum_{x\in\{0,1\}^n}\sigma\left[p_\theta^{\oplus x}\right]|x^\theta\rangle\langle x^\theta|$$

so that $2\mathsf{p}_{\mathsf{win}}^{\mathrm{xor}}(G,p) - 1 = \frac{1}{2^n}\langle v|Z_p|v\rangle$. Recall that the strategy gets to choose ρ_{ABC} and hence $|v\rangle$. Choosing $|v\rangle$ to be the normalized top-eigenvector of Z_p gives

$$2\mathsf{p}_{\mathsf{win}}^{\mathrm{xor}}(G,p) - 1 = \frac{1}{2^n}\|Z_p\|.$$

We shall show that for every n, there exists a strategy p (in fact, at least 2^{n+1} such strategies) such that $\|Z_p\| = 2^n/\sqrt{2}$, which yields the desired lower bound

$$\sup_s \mathsf{p}_{\mathsf{win}}^{\mathrm{xor}}(G,s) \geq \frac{1+\frac{1}{\sqrt{2}}}{2} = \frac{1}{2} + \frac{1}{2\sqrt{2}}.$$

We shall do this recursively.

Given strategies p_0 and p_1 for the $(n-1)$-fold xor-game, define the strategy $p = p_0p_1$ for the n-fold xor-game to be the strategy induced by the concatenation of the strategies p_0 and p_1 treated as strings. In particular, for each $\theta \in \{0,1\}^n$,

$$p_\theta = \begin{cases}(p_0)_{\theta_1} & \text{if } \theta = 0\theta_1\\ (p_1)_{\theta_1} & \text{if } \theta = 1\theta_1\end{cases}$$

We have the following easy claim:

Claim 2.2. *Let p_0 and p_1 be bitstrings of the same length 2^{n-1}. Define $p := p_0p_1$ (concatenation). Then*

$$Z_p = Z \otimes Z_{p_0} + X \otimes Z_{p_1} = \begin{bmatrix}Z_{p_0} & Z_{p_1}\\ Z_{p_1} & -Z_{p_0}\end{bmatrix}.$$

Proof. Define $Z_p^\theta := \sum_{x\in\{0,1\}^n}(-1)^{p_\theta^{\oplus x}}|x^\theta\rangle\langle x^\theta|$ so $Z_p = \sum_{\theta\in\{0,1\}^n} Z_p^\theta$. For $\theta \in \{0,1\}^{n-1}$, we can write

$$\begin{aligned}Z_p^{0\theta} &= \sum_{x\in\{0,1\}^n}\sigma\left[(p_0)_\theta^{\oplus x}\right]|x^{0\theta}\rangle\langle x^{0\theta}|\\ &= |0\rangle\langle 0| \otimes Z_{p_0}^\theta - |1\rangle\langle 1| \otimes Z_{p_0}^\theta,\end{aligned}$$

so that $\sum_{\theta\in\{0,1\}^{n-1}} Z_p^{0\theta} = Z \otimes Z_{p_0}$. Similarly, for $\theta \in \{0,1\}^{n-1}$,

$$\begin{aligned} Z_p^{1\theta} &= \sum_{x\in\{0,1\}^n} \sigma\left[(p_1)_\theta^{\oplus x}\right] |x^{1\theta}\rangle \langle x^{1\theta}| \\ &= |+\rangle\langle +| \otimes Z_{p_1}^\theta - |-\rangle\langle -| \otimes Z_{p_1}^\theta, \end{aligned}$$

so that $\sum_{\theta\in\{0,1\}^{n-1}} Z_p^{1\theta} = X \otimes Z_{p_1}$. The result follows by adding the two equations. □

The crux of the argument lies in the linear-algebraic property of ZX-compatibility and consequent structure of their spectra. We define and analyze ZX-compatibility in the next section.

2.2 ZX-compatibility

Definition 2.3. *We say that a pair of same-order symmetric matrices (A, B) is ZX-compatible if $AB+BA = 0$ and $A^2 = B^2$.*

Remark. The name comes from the easy observation that the Pauli matrices Z and X are ZX-compatible.

The second constraint of ZX-compatibility yields the following nice property:

Claim 2.4. *Suppose A and B are symmetric matrices with $A^2 = B^2$. Then the ranges/column spaces of A and B are identical.*

Proof. Let n denote the common order of A and B. Since A and B are real symmetric, we may write $A = \sum_{i=1}^r \lambda_i |v_i\rangle\langle v_i|$ and $B = \sum_{i=1}^s \mu_i |w_i\rangle\langle w_i|$, where $\{|v_i\rangle\}_{i=1}^r$ and $\{|w_i\rangle\}_{i=1}^s$ are orthonormal vectors in $\mathbb{R}^n$ and $\lambda_i, \mu_i \in \mathbb{R}\setminus\{0\}$ are the nonzero eigenvalues of A and B. Note that the range of A is spanned by $\{|v_i\rangle\}_{i=1}^r$ and the that of B by $\{|w_i\rangle\}_{i=1}^s$. We shall show that each $v_i \in \text{span}(\{w_j\}_{j=1}^s)$ and vice versa, which implies the result.

The condition $A^2 = B^2$ is equivalent to

$$\sum_{i=1}^r \lambda_i^2 |v_i\rangle\langle v_i| = \sum_{i=1}^s \mu_i^2 |w_i\rangle\langle w_i|.$$

Fix $i \in \{1,\ldots,r\}$. Right-multiplying both sides by $|v_i\rangle$ gives (note $\lambda_i \neq 0$)

$$|v_i\rangle = \sum_{j=1}^s \frac{\mu_j^2}{\lambda_i^2} |w_j\rangle \in \text{span}(\{w_j\}_{j=1}^s).$$

Similarly, each $|w_j\rangle \in \text{span}(\{v_i\}_{i=1}^r)$. The result follows. □

Lemma 2.5. *Suppose A and B are ZX-compatible. Suppose also that the nonzero eigenvalues of A and B are $\{\lambda, -\lambda\}$ (with multiplicity 1 each) for some $\lambda > 0$. Then the nonzero eigenvalues of*

$$C = \begin{bmatrix} A & B \\ B & -A \end{bmatrix}$$

are $\{2\lambda, -2\lambda\}$ (with multiplicity 1 each).

Proof. Let n denote the common order of A and B. Suppose v and $\bar{v}$ are orthonormal eigenvectors of A corresponding to the nonzero eigenvalues, i.e. $Av = \lambda v$ and $A\bar{v} = -\lambda\bar{v}$. We claim that $v \perp Bv$: indeed, note that

$$A(Bv) - B(Av) = -\lambda Bv$$

and so $Bv \parallel \bar{v} \perp v$. Consider the four nonzero vectors in $\mathbb{R}^{2n}$ defined by

$$\begin{aligned} \boldsymbol{x}_1 &= \begin{bmatrix} Av \\ Bv \end{bmatrix}, & \boldsymbol{x}_2 &= \begin{bmatrix} Av \\ -Bv \end{bmatrix} \\ \boldsymbol{x}_3 &= \begin{bmatrix} Bv \\ Av \end{bmatrix}, & \boldsymbol{x}_4 &= \begin{bmatrix} Bv \\ -Av \end{bmatrix} \end{aligned}$$

We can compute

$$\begin{aligned} C\boldsymbol{x}_1 &= \begin{bmatrix} A & B \\ B & -A \end{bmatrix} \begin{bmatrix} Av \\ Bv \end{bmatrix} = \begin{bmatrix} (A^2+B^2)v \\ (BA-AB)v \end{bmatrix} = 2\begin{bmatrix} A(Av) \\ B(Av) \end{bmatrix} = 2\lambda\boldsymbol{x}_1, \\ C\boldsymbol{x}_2 &= \begin{bmatrix} A & B \\ B & -A \end{bmatrix} \begin{bmatrix} Av \\ -Bv \end{bmatrix} = \begin{bmatrix} (A^2-B^2)v \\ (BA+AB)v \end{bmatrix} = \mathbf{0}, \\ C\boldsymbol{x}_3 &= \begin{bmatrix} A & B \\ B & -A \end{bmatrix} \begin{bmatrix} Bv \\ Av \end{bmatrix} = \begin{bmatrix} (AB+BA)v \\ (B^2-A^2)v \end{bmatrix} = \mathbf{0}, \\ C\boldsymbol{x}_4 &= \begin{bmatrix} A & B \\ B & -A \end{bmatrix} \begin{bmatrix} Bv \\ -Av \end{bmatrix} = \begin{bmatrix} (AB-BA)v \\ (B^2+A^2)v \end{bmatrix} = -2\begin{bmatrix} B(Av) \\ -A(Av) \end{bmatrix} = -2\lambda\boldsymbol{x}_4. \end{aligned}$$

Thus the four vectors $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4$ are eigenvectors of C. Further, they are orthogonal: noting that $\langle Av, Bv\rangle = \langle Bv, Av\rangle = \lambda\langle v, Bv\rangle = 0$, we have

$$\begin{aligned} \langle \boldsymbol{x}_1, \boldsymbol{x}_3\rangle &= \langle Av, Bv\rangle + \langle Bv, Av\rangle = 0, \\ \langle \boldsymbol{x}_1, \boldsymbol{x}_4\rangle &= \langle Av, Bv\rangle - \langle Bv, Av\rangle = 0, \\ \langle \boldsymbol{x}_2, \boldsymbol{x}_3\rangle &= \langle Av, Bv\rangle - \langle Bv, Av\rangle = 0, \\ \langle \boldsymbol{x}_2, \boldsymbol{x}_4\rangle &= \langle Av, Bv\rangle + \langle Bv, Av\rangle = 0, \\ \langle \boldsymbol{x}_1, \boldsymbol{x}_2\rangle &= \langle Av, Av\rangle - \langle Bv, Bv\rangle = \langle v, (A^2-B^2)v\rangle = 0, \\ \langle \boldsymbol{x}_3, \boldsymbol{x}_4\rangle &= \langle Bv, Bv\rangle - \langle Av, Av\rangle = \langle v, (B^2-A^2)v\rangle = 0. \end{aligned}$$

Finally, we shall show that any vector $\boldsymbol{x} \in \operatorname{span}(\{\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4\})^\perp$ is sent to $\mathbf{0}$ by C; this yields $2n-4$ more orthonormal eigenvectors of C with eigenvalue 0, completing the proof. Suppose then that $\boldsymbol{x} = \begin{bmatrix} y & z \end{bmatrix}^\top \perp \boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4$. Then $\boldsymbol{x} \perp (\boldsymbol{x}_1 + \boldsymbol{x}_2)/2$ and $\boldsymbol{x} \perp (\boldsymbol{x}_3 + \boldsymbol{x}_4)/2$, so that $y \perp Av, Bv$ or $y \perp v, \bar{v}$. Since A maps $\operatorname{span}(\{v, \bar{v}\})^\perp$ to $\mathbf{0}$, $Ay = \mathbf{0}$. Also, Claim 2.4 implies that B has the same null space $\operatorname{span}(\{v, \bar{v}\})^\perp$ as A, and so $By = \mathbf{0}$ as well. In perfectly analogous fashion, $\boldsymbol{x} \perp (\boldsymbol{x}_1 - \boldsymbol{x}_2)/2$ and $\boldsymbol{x} \perp (\boldsymbol{x}_3 - \boldsymbol{x}_4)/2$ imply $Az = Bz = \mathbf{0}$. It follows that

$$C\boldsymbol{x} = \begin{bmatrix} Ay + Bz \\ By - Az \end{bmatrix} = \begin{bmatrix} \mathbf{0} \\ \mathbf{0} \end{bmatrix}.$$

Thus, the only two nonzero eigenvalues of C are 2λ and -2λ, each with multiplicity 1. The proof is complete. □

A few additional properties of ZX-compatibility not needed for the proof of the lemma:

- The vectors $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4$ defined in the proof are actually just the images of x_1 under the four Pauli operators I, Z, X and Y.
- Further, notice that one has $\lambda^2 = \langle v, A^2 v\rangle = \langle Bv, Bv\rangle$, so that $\|Bv\| = \lambda$. Since $Bv \parallel \bar{v}$, we must have $Bv = \pm\lambda\bar{v}$. It follows that the vectors $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4$ when divided by λ are simply (upto sign of $\bar{v}$) $\begin{bmatrix} v \\ \pm\bar{v}\end{bmatrix}$ and $\begin{bmatrix} \bar{v} \\ \pm v\end{bmatrix}$ and hence are trivially orthogonal.
- Suppose that w and $\bar{w}$ are the orthonormal eigenvectors of B corresponding to eigenvalues λ and $-\lambda$ respectively. Then A, B being ZX-compatible implies that the pairwise inner products $\langle v, w\rangle, \langle v, \bar{w}\rangle, \langle \bar{v}, w\rangle, \langle \bar{v}, \bar{w}\rangle$ are all $\pm 1/\sqrt{2}$, generalizing the case of Pauli matrices Z and X.
- The proof of the lemma does not require any condition on the spectrum of B: it is enough that A has the spectrum $\{\lambda, 0, \ldots, 0, -\lambda\}$ and that A and B are ZX-compatible.

2.3 The proof of the lower bound

For the induction, we shall also need a few simple observations addressing ZX-compatibility of the operators Z_p. In what follows, we shall use $\overline{p}$ to denote the bitwise negation of p, i.e. $\overline{p}_\theta = 1 - p_\theta$ for each $\theta \in \{0,1\}^n$. As a strategy, it corresponds to the adversaries guessing exactly the opposite of what they would have guessed in the strategy p, at each value of θ.

Lemma 2.6. *The following are true for each $n \in \mathbb{N}$ and $p, p_0, p_1 \in \{0,1\}^{2^n}$.*

1. $Z_{\overline{p}} = -Z_p$.
2. (Z_{p_0}, Z_{p_1}) *is ZX-compatible iff* (Z_{p_1}, Z_{p_0}) *is ZX-compatible.*
3. $(Z_{p_0 p_1}, Z_{p_1 \overline{p}_0})$ *is ZX-compatible.*
4. $(Z_{p_0 p_1}, Z_{\overline{p}_1 p_0})$ *is ZX-compatible.*

Proof.

1. This follows from the definition of Z_p:

$$Z_{\overline{p}} := \sum_{\theta\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} \sigma\left[\overline{p}_\theta^{\oplus x}\right] |x^\theta\rangle\langle x^\theta| = \sum_{\theta\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} -\sigma\left[p_\theta^{\oplus x}\right] |x^\theta\rangle\langle x^\theta| = -Z_p.$$

2. Trivial: the definition of (A, B) being ZX-compatible is symmetric in A and B.
3. From Claim 2.2, we have the expressions

$$Z_{p_0 p_1} = \begin{bmatrix} Z_{p_0} & Z_{p_1} \\ Z_{p_1} & -Z_{p_0}\end{bmatrix} \quad \text{and} \quad Z_{p_1\overline{p}_0} = \begin{bmatrix} Z_{p_1} & -Z_{p_0} \\ -Z_{p_0} & -Z_{p_1}\end{bmatrix}.$$

For notational convenience, denote $A := Z_{p_0}$ and $B := Z_{p_1}$. We compute

$$Z^2_{p_0p_1} = \begin{bmatrix} A & B \\ B & -A \end{bmatrix} \begin{bmatrix} A & B \\ B & -A \end{bmatrix} = \begin{bmatrix} A^2+B^2 & AB-BA \\ BA-AB & A^2+B^2 \end{bmatrix} = \begin{bmatrix} B & -A \\ -A & -B \end{bmatrix} \begin{bmatrix} B & -A \\ -A & -B \end{bmatrix} = Z^2_{p_1\overline{p}_0}.$$

Further,

$$Z_{p_0p_1} Z_{p_1\overline{p}_0} = \begin{bmatrix} A & B \\ B & -A \end{bmatrix} \begin{bmatrix} B & -A \\ -A & -B \end{bmatrix} = \begin{bmatrix} AB-BA & -A^2-B^2 \\ B^2+A^2 & AB-BA \end{bmatrix} = - \begin{bmatrix} B & -A \\ -A & -B \end{bmatrix} \begin{bmatrix} A & B \\ B & -A \end{bmatrix} = -Z_{p_1\overline{p}_0} Z_{p_0p_1},$$

as needed.

4. Note that (A, B) is ZX-compatible iff $(A, -B)$ is. We finish by noting $Z_{\overline{p}_1p_0} = -Z_{p_1\overline{p}_0}$.

□

Finally, we note that the base-case operators Z_{00} and Z_{01} corresponding to $n = 1$ are ZX-compatible.

Observation 2.7. *Z_{00} and Z_{01} are ZX-compatible. Further,*

$$\|Z_{00}\| = \|Z_{01}\| = \frac{2}{\sqrt{2}}.$$

Proof. For $p = 00$ and $x \in \{0, 1\}$, note $p_\theta^{\oplus x} = 1 \oplus x$. We compute

$$Z_{00} = \sum_{\theta\in\{0,1\}} \sum_{x\in\{0,1\}} \sigma[1 \oplus x] \left|x^\theta\right\rangle \left\langle x^\theta\right| = (|0\rangle\langle 0| - |1\rangle\langle 1|) + (|+\rangle\langle +| - |-\rangle\langle -|) = Z + X.$$

Similarly, note $p = 01$ satisfies $p_\theta^{\oplus x} = 1 \oplus \theta \oplus x$. This gives

$$Z_{00} = (|0\rangle\langle 0| - |1\rangle\langle 1|) - (|+\rangle\langle +| - |-\rangle\langle -|) = Z - X.$$

It is easy to see that the eigenvalues of Z_{00} and Z_{01} are $\pm\sqrt{2}$, from which. the norm claim follows. ZX-compatibility follows from the calculations

$$(Z + X)^2 = Z^2 + X^2 = (Z - X)^2$$

(where we use $ZX + XZ = 0$) and

$$(Z + X)(Z - X) = Z^2 - X^2 + XZ - ZX = -(Z^2 - X^2) + XZ - ZX = -(Z - X)(Z + X)$$

(where we use $Z^2 = X^2$). The observation follows. □

We are now ready to prove the main lower bound.

Theorem 2.8. *Let $n \in \mathbb{N}$. There exists a strategy $p \in \{0, 1\}^{2^n}$ such that $\|Z_p\| = 2^n/\sqrt{2}$. Infact, there exist 2^{n+1} strategies $p_0, \overline{p}_0, p_1, \overline{p}_1, \ldots p_{2^n-1}, \overline{p}_{2^n-1} \in \{0, 1\}^{2^n}$ such that for each such strategy p $\|Z_p\| = 2^n/\sqrt{2}$. Further, p_{2k} and p_{2k+1} are ZX-compatible for every $k \in \{0, 1, \ldots, 2^{n-1} - 1\}$.*

Proof. We proceed by induction on n. The basecase $n = 1$ follows from Observation 2.7 with $p_0 = 00$ and $p_1 = 01$.

Suppose now that we have 2^{n+1} strategies for the n-fold xor-game. For each $k \in \{0, \ldots, 2^{n-1} - 1\}$, construct the two strategies $p := p_{2k}p_{2k+1}$ and $q := p_{2k}\overline{p}_{2k+1}$. Lemma 2.5 implies that $\|Z_p\| = \|Z_q\| = 2^{n+1}/\sqrt{2}$ and Lemma 2.6 (3) implies that p and q are ZX-compatible. Noting that (A, B) are ZX-compatible iff $(-A, -B)$ are ZX-compatible, we note from Lemma 2.6 (1) that $\overline{p}_{2k}$ and $\overline{p}_{2k+1}$ are ZX-compatible too. Using Lemma 2.6(3) again yields two more ZX-compatible strategies $\overline{p}$ and $\overline{q}$ that satisfy $\|Z_{\overline{p}}\| = \|Z_{\overline{q}}\| = 2^{n+1}/\sqrt{2}$. Finally, note that one may switch the roles of p_{2k} and p_{2k+1} to obtain another four distinct strategies. In particular, the four strategies $p_{2k}, \overline{p}_{2k}, p_{2k+1}, \overline{p}_{2k+1}$ give rise to the eight strategies

$$\begin{aligned} q_{4k} &:= p_{2k}p_{2k+1}, & \overline{q}_{4k} &= \overline{p}_{2k}\overline{p}_{2k+1}, \\ q_{4k+1} &:= p_{2k}\overline{p}_{2k+1}, & \overline{q}_{4k+1} &= \overline{p}_{2k}p_{2k+1}, \\ q_{4k+2} &:= p_{2k+1}p_{2k}, & \overline{q}_{4k+2} &= \overline{p}_{2k+1}\overline{p}_{2k}, \\ q_{4k+3} &:= p_{2k+1}\overline{p}_{2k}, & \overline{q}_{4k+3} &= \overline{p}_{2k+1}p_{2k} \end{aligned}$$

with each q_i satisfying $\|Z_{q_i}\| = 2^{n+1}/\sqrt{2}$. Further, $q_{2\ell}$ and $q_{2\ell+1}$ are ZX-compatible for $\ell = 2k, 2k+1$. The result follows by induction on n. □

Theorem 2.8 coupled with the trivial upper bound above proves that for every n, the value of the n-fold xor-game is $1/2 + 1/2\sqrt{2}$, as needed. ■

References

[CLX25] Andrea Coladangelo, Qipeng Liu, and Ziyi Xie. *The curious case of "XOR repetition" of monogamy-of-entanglement games*. 2025. arXiv: 2509.01831 [quant-ph]. URL: https://arxiv.org/abs/2509.01831.

[TFKW13] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. "A monogamy-of-entanglement game with applications to device-independent quantum cryptography". In: *New Journal of Physics* 15.10 (Oct. 2013), p. 103002. ISSN: 1367-2630. DOI: 10.1088/1367-2630/15/10/103002. URL: http://dx.doi.org/10.1088/1367-2630/15/10/103002.