A monogamy-of-entanglement game for subspace coset states

Eric Culf* Thomas Vidick†

August 12, 2021

Abstract

We establish a strong monogamy-of-entanglement property for subspace coset states, which are uniform superpositions of vectors in a linear subspace of $\mathbb{F}_2^n$ to which has been applied a quantum one-time pad. This property was conjectured recently by [Coladangelo, Liu, Liu, and Zhandry, Crypto'21] and shown to have applications to unclonable decryption and copy-protection of pseudorandom functions. We present two proofs, one which directly follows the method of the original paper and the other which uses an observation from [Vidick and Zhang, Eurocrypt'20] to reduce the analysis to a simpler monogamy game based on BB'84 states. Both proofs ultimately rely on the same proof technique, introduced in [Tomamichel, Fehr, Kaniewski and Wehner, New Journal of Physics '13].

1 Introduction

Informally, a *monogamy game* is a game in which the maximum success probability is tied to the monogamy of entanglement, i.e. limitations on the strength of quantum multipartite correlations. The simplest such game goes as follows. Two players Bob and Charlie aim to prepare a tripartite state ρ_{ABC}, such that A is a single qubit and B and C are arbitrary, and the following holds: given a measurement of A in the standard or Hadamard basis yielding an outcome $x \in \{0,1\}$ it is possible to predict x both by making a measurement on B only *and* on C only, given the chosen basis as side information. Monogamy of entanglement expresses itself by the fact that while ignoring C it is possible to win in this game with probability 1 by choosing ρ_{AB} to be an EPR pair, as soon as C is present the maximum winning probability drops to $\frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.854$.

Monogamy games have played an important role in quantum cryptography since some of the first proofs of security of quantum key distribution, which make use of monogamy through uncertainty relations such as $H(Z|\mathsf{B}) + H(X|\mathsf{C}) \geq 1$, with X and Z classical random variables that denote the outcome of a measurement of A in the standard and Hadamard bases respectively [Koa06, TL17]. In this note we study a monogamy game introduced recently in [CLLZ21] and called "strong monogamy game" therein. Informally, in the game two players Bob and Charlie cooperate in an attempt to create two copies of a *coset subspace state*

$$|A_{s,s'}\rangle \;=\; \frac{1}{\sqrt{|A|}} \sum_{u \in A} (-1)^{u \cdot s'} |u + s\rangle \;,$$

where A is a linear subspace of $\mathbb{F}_2^n$ and $s, s' \in \mathbb{F}_2^n$ are arbitrary, such that given the first copy *and* a description of A it is possible to obtain a vector $u \in A + s$, while given the other copy *and* the description of A it is

*Department of Mathematics, University of Ottawa, Canada. eculf019@uottawa.ca
†Department of Computing and Mathematical Sciences, California Institute of Technology, USA. vidick@caltech.edu

possible to obtain a vector $v \in A^\perp + s'$, with $A^\perp = \{w : w \cdot u = 0 \forall u \in A\}$.[1] (We describe the game in detail in Section 2.) In [CLLZ21] the authors show a sub-exponentially decaying bound on the players' maximum success probability in a variant of this game where from each copy a pair $(u, v) \in (A + s) \times (A^\perp + s')$ has to be returned. While the original subspace coset game is more useful for their cryptographic applications they are unable to analyze it. In this paper we show an exponentially decaying bound on the players' maximum success probability in the original game; as shown in [CLLZ21] this implies constructions for uncloneable decryption and copy-protection of pseudorandom functions based on post-quantum indistinguishability obfuscation and one-way functions only. (In contrast, in [CLLZ21] the same applications are obtained under the additional, strong assumption of extractable witness encryption. We refer to [CLLZ21] for additional discussion.)

Our main result is stated as Theorem 2.1 in Section 2. We first show the theorem directly by following the template introduced in [TFKW13] and adapting it to subspace coset states using some of the arguments from [CLLZ21] as well as some new steps. Next, we revisit our proof by making a simple but useful connection between subspace coset states and BB'84 states. (This connection was first used in [VZ21] to analyze a proof of quantum knowledge for subspace coset states.) To explain the connection, let A be a subspace spanned by canonical vectors, $A = \text{Span}\{e_i, i \in \overline{T}\}$ for some set $T \subseteq \{1, \ldots, n\}$ with complement $\overline{T}$, and $s, s' \in \mathbb{F}_2^n$. Let $\theta \in \{0, 1\}^n$ be the indicator vector of $\overline{T}$, i.e. $\theta_i = 1$ if and only if $i \notin T$. Let $x \in \{0, 1\}^n$ be such that $x_i = s_i$ whenever $i \in T$ and $x_i = s'_i$ whenever $i \in \overline{T}$. Then it is easily verified that

$$|A_{s,s'}\rangle \;=\; |x\rangle_\theta \;,$$

where we write $|x\rangle_\theta = |x_1\rangle_{\theta_1} \cdots |x_n\rangle_{\theta_n}$ with $|x_i\rangle_{\theta_i} = H^{\theta_i}|x_i\rangle$, H the Hadamard gate. Thus coset subspace states for "basis-aligned" subspaces are exactly BB'84 states. This observation leads to a partition of subspace coset states such that subspace coset states in each element of the partition are in 1-to-1 correspondence with BB'84 states under a simple unitary permutation of the standard basis, see Claim 5.2 for a precise formulation. While this observation implicitly appears in some of the arguments from [CLLZ21], as well as in our direct proof of Theorem 2.1, making it explicit allows us to directly relate the strong monogamy game from [CLLZ21] (which we refer to as the "coset-monogamy game") to a simple variant of the monogamy game from [TFKW13] (which we refer to as the "basis-monogamy game") whose maximum success probability we bound using a similar technique to the one introduced in their paper. Ultimately this "proof by reduction" is very similar to the direct proof; we include it in the hope that the simple reduction pointed out here will find further uses in the analysis of monogamy games motivated by tasks in quantum cryptography.

In Section 2 we introduce the strong monogamy game (called coset-monogamy game here) and state our main result, Theorem 2.1. In Section 3 we prove our main result. In Section 4 we introduce and analyze our variant of the BB'84-based monogamy game from [TFKW13] (called basis-monogamy game here). Finally in Section 5 we show a reduction from the coset monogamy game to the basis monogamy game.

Acknowledgments. We thank Fatih Kaleoglu for pointing out an error in an earlier proof of Lemma 3.4. E.C. would like to thank Anne Broadbent. E.C.'s work is supported by a CGS M scholarship from Canada's NSERC. T.V. is supported by NSF CAREER Grant CCF-1553477, AFOSR YIP award number FA9550-16-1-0495, MURI Grant FA9550-18-1-0161 and the IQIM, an NSF Physics Frontiers Center (NSF Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-12500028).

[1] Here it is crucial that A is revealed only after the "copying" has taken place, as given A and $|A_{s,s'}\rangle$ itself it is possible to recover A and $s \mod A$, $s' \mod A^\perp$.

2 The coset-monogamy game

The following game is a monogamy game introduced in [CLLZ21], where it is called "strong monogamy game" (see Section 4.4 therein). For a linear subspace A of $\mathbb{F}_2^n$ and $s, s' \in \{0,1\}^n$ recall the notation

$$|A\rangle \;=\; \frac{1}{\sqrt{|A|}} \sum_{u \in A} |u\rangle \qquad \text{and} \qquad |A_{s,s'}\rangle \;=\; X^s Z^{s'} |A\rangle \;=\; \frac{1}{\sqrt{|A|}} \sum_{u \in A} (-1)^{u \cdot s'} |u+s\rangle \;,$$

where $X^s = X^{s_1} \otimes \cdots X^{s_n}$, $Z^{s'} = Z^{s'_1} \otimes \cdots Z^{s'_n}$ with $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

We formulate the game exactly as in [CLLZ21, Section 4.4]. The only difference is that we rename $\mathcal{A}_0$ into "the adversary", $\mathcal{A}_1$ into "Bob" and $\mathcal{A}_2$ into "Charlie". Thus the game is played between a trusted "challenger" and two untrusted, cooperating players Bob and Charlie. The game is parametrized by an even integer $n \geq 2$.

Coset-monogamy game.

1. *Preparation:* The challenger picks a uniformly random subspace $A \subseteq \mathbb{F}_2^n$ of dimension $\frac{n}{2}$ and two uniformly random elements $s, s' \in \mathbb{F}_2^n$. The challenger sends $|A_{s,s'}\rangle$ to the adversary.

2. The adversary applies a quantum channel $\Phi : \mathcal{H}_{\mathsf{A}} \to \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}}$, where $\mathcal{H}_{\mathsf{A}} = (\mathbb{C}^2)^{\otimes n}$ and $\mathcal{H}_{\mathsf{B}}$, $\mathcal{H}_{\mathsf{C}}$ are arbitrary. The adversary computes $\rho_{\mathsf{BC}} = \Phi(|A_{s,s'}\rangle\langle A_{s,s'}|)$. It sends registers B to Bob and C to Charlie, respectively.

3. *Question:* The challenger sends the description of A, in the form of a basis for it, to both Bob and Charlie.

4. *Answer:* Bob returns $s_1 \in \mathbb{F}_2^n$ and Charlie returns $s_2 \in \mathbb{F}_2^n$.

5. *Winning condition:* The adversary, Bob and Charlie win if and only if $s_1 \in A + s$ and $s_2 \in A^\perp + s'$, where $A^\perp = \{v \in \mathbb{F}_2^n : \; v \cdot u = 0 \, \forall u \in A\}$.

Our main result is a bound on the maximum winning probability of the adversary, Bob and Charlie in the coset-monogamy game.

Theorem 2.1. *Let $n \geq 1$ be an even integer. Let q_n be the adversary, Bob and Charlie's maximum probability of winning in the coset-monogamy game. Then*

$$q_n \;\leq\; \sqrt{e} \Big(\cos \frac{\pi}{8} \Big)^n \;.$$

We give two proofs of the theorem. Ultimately, both proofs rely on the technique from [TFKW13], and lead to the same numerical bound on the success probability. The difference is that the first proof is direct, while the second proof proceeds by a reduction to a variant of the monogamy game from [TFKW13]. Since the reduction is intuitively clear, and the monogamy game we reduce to, being based on BB'84 states, is easier to analyze, the second proof is conceptually simpler and potentially more general. However, it is less direct.

3 Direct proof

We give a direct proof of Theorem 2.1. The proof proceeds in two steps. In the first step we reduce to the analysis of an extended nonlocal game of the form considered in [JMRW16]. This step is standard in the analysis of monogamy games, and also appears as [CLLZ21, Lemma C.6]. We formulate it in Lemma 3.1 below. In the second step we bound the maximum success probability in the extended nonlocal game. This step relies on a technique introduced in [TFKW13] to bound the operator norm of a tripartite operator introduced to model the players' actions in the game. We describe this step in Section 3.2.

3.1 Reduction to an extended nonlocal game

Write $\mathsf{G}\big(\frac{n}{2}, n\big)$ for the set of linear subspaces of $\mathbb{F}_2^n$ of dimension $\frac{n}{2}$. For $A \in \mathsf{G}\big(\frac{n}{2}, n\big)$ write $\mathsf{CS}(A)$ for a fixed set of representatives of the cosets of A. In particular, $|\mathsf{CS}(A)| = 2^{\frac{n}{2}}$.

Lemma 3.1. *Fix a strategy for the coset-monogamy game, consisting of a channel $\Phi : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_C$ and for each $A \in \mathsf{G}\big(\frac{n}{2}, n\big)$ POVMs $\{B_s^A\}_{s \in \mathsf{CS}(A)}$ for Bob and $\{C_{s'}^A\}_{s' \in \mathsf{CS}(A^\perp)}$ for Charlie. Let q_n' be the probability that this strategy succeeds in the game. Then*

$$\begin{aligned} q_n' &= \mathop{\mathrm{E}}_{A \in \mathsf{G}\left(\frac{n}{2}, n\right)} \mathop{\mathrm{E}}_{\substack{s \in \mathsf{CS}(A) \\ s' \in \mathsf{CS}(A^\perp)}} \mathrm{Tr}\big((B_s^A \otimes C_{s'}^A)\Phi\big(|A_{s,s'}\rangle\langle A_{s,s'}|\big)\big) \\ &= \mathop{\mathrm{E}}_{A \in \mathsf{G}\left(\frac{n}{2}, n\right)} \sum_{\substack{s \in \mathsf{CS}(A) \\ s' \in \mathsf{CS}(A^\perp)}} \mathrm{Tr}\Big(\big(|A_{s,s'}\rangle\langle A_{s,s'}| \otimes B_s^A \otimes C_{s'}^A\big)\rho\Big) \ , \end{aligned}$$

where $\rho = (\mathrm{Id}_{\mathsf{A}} \otimes \Phi_{\mathsf{A}'})(|\phi^+\rangle\langle\phi^+|_{\mathsf{AA}'}^{\otimes n})$ with $|\phi^+\rangle$ the EPR pair, $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and all expectations are uniform averages.

While the first equality is by definition, the second equality is what we refer to as a "reduction to an extended nonlocal game." This is because the second line can be interpreted as the success probability in the following three-player game: (i) Bob and Charlie prepare a tripartite state ρ_{ABC} such that A is an n-qubit register. They give A to Alice and keep B and C respectively. (ii) Alice selects a uniformly random subspace $A \in \mathsf{G}\big(\frac{n}{2}, n\big)$ and gives A to Bob and Charlie. She measures A using the projective measurement $\{|A_{s,s'}\rangle\langle A_{s,s'}|\}$ with outcomes $(s, s') \in \mathsf{CS}(A) \times \mathsf{CS}(A^\perp)$. (iii) Bob and Charlie measure their registers using arbitrary POVM $\{B_s^A\}$ and $\{C_{s'}^A\}$ respectively. They win if and only if they obtain outcomes, s for Bob and s' for Charlie, that match Alice's.

Proof. To show the second equality we expand using the definition of ρ

$$\begin{aligned} \mathrm{Tr}\Big(\big(|A_{s,s'}\rangle\langle A_{s,s'}| \otimes B_s^A \otimes C_{s'}^A\big)\rho\Big) &= \frac{1}{2^n} \sum_{r,r' \in \mathbb{F}_2^n} \mathrm{Tr}\Big(\big(|A_{s,s'}\rangle\langle A_{s,s'}| \otimes B_s^A \otimes C_{s'}^A\big)\big(|r\rangle\langle r'| \otimes \Phi(|r\rangle\langle r'|)\big)\Big) \\ &= \frac{1}{2^n} \sum_{r,r' \in \mathbb{F}_2^n} \langle r'|A_{s,s'}\rangle\langle r|A_{s,s'}\rangle \mathrm{Tr}\big(\big(B_s^A \otimes C_{s'}^A\big)\Phi(|r\rangle\langle r'|)\big) \\ &= \frac{1}{2^n} \mathrm{Tr}\Big(\big(B_s^A \otimes C_{s'}^A\big)\Phi\Big(\sum_{r \in \mathbb{F}_2^n} |r\rangle\langle r|A_{s,s'}\rangle\langle A_{s,s'}| \sum_{r' \in \mathbb{F}_2^n} |r'\rangle\langle r'|\Big)\Big) \\ &= \frac{1}{2^n} \mathrm{Tr}\big(\big(B_s^A \otimes C_{s'}^A\big)\Phi\big(|A_{s,s'}\rangle\langle A_{s,s'}|\big)\big) \ , \end{aligned}$$

which gives the result. ∎

3.2 Analysis of extended nonlocal game

We need two preliminary lemmas. The first bounds the overlap of operators constructed as sums of coset state projections. We use $\|\cdot\|$ to denote the operator norm, i.e. the largest singular value.

Lemma 3.2. *For any $A, B \in \mathsf{G}\big(\frac{n}{2}, n\big)$, $s' \in \mathsf{CS}(A^\perp)$ and $t \in \mathsf{CS}(B)$ we have that the overlap*

$$\Big\| \sum_{s\in \mathsf{CS}(A)} |A_{s,s'}\rangle\langle A_{s,s'}| \sum_{t'\in \mathsf{CS}(B^\perp)} |B_{t,t'}\rangle\langle B_{t,t'}| \Big\| \leq \sqrt{2^{\dim(A\cap B)-\frac{n}{2}}} \,. \tag{1}$$

Proof. First, note that

$$\begin{aligned}
\sum_{t'\in \mathsf{CS}(B^\perp)} |B_{t,t'}\rangle\langle B_{t,t'}| &= \frac{1}{2^{\frac{n}{2}}} \sum_{t'\in\mathbb{F}_2^n} |B_{t,t'}\rangle\langle B_{t,t'}| \\
&= \frac{1}{2^n} \sum_{t'\in\mathbb{F}_2^n} \sum_{b,b'\in B} (-1)^{(b+b')\cdot t'} |b+t\rangle\langle b'+t| \\
&= \sum_{b,b'\in B} \delta_{b,b'} |b+t\rangle\langle b'+t| \\
&= \sum_{b\in B+t} |b\rangle\langle b| \,,
\end{aligned} \tag{2}$$

a projection onto the subspace spanned by the vectors given by the elements of the coset $B+t$. Let $\Pi_{B+t} = \sum_{b\in B+t} |b\rangle\langle b|$. Then

$$\begin{aligned}
\Big\| \sum_{s\in \mathsf{CS}(A)} |A_{s,s'}\rangle\langle A_{s,s'}| \sum_{t'\in \mathsf{CS}(B^\perp)} |B_{t,t'}\rangle\langle B_{t,t'}| \Big\| &= \Big\| \sum_{s\in \mathsf{CS}(A)} |A_{s,s'}\rangle\langle A_{s,s'}| \Pi_{B+t} \Big\| \\
&= \Big\| \Pi_{B+t} \Big(\sum_{s\in \mathsf{CS}(A)} |A_{s,s'}\rangle\langle A_{s,s'}| \Big) \Pi_{B+t} \Big\|^{1/2} \,,
\end{aligned} \tag{3}$$

where the second equality uses that $\{|A_{s,s'}\rangle\langle A_{s,s'}|\}_{s\in\mathsf{CS}(A)}$ are orthogonal projectors. Since we have that $|A_{s,s'}\rangle$ is a superposition of basis elements in $A+s$, so $\Pi_{B+s}|A_{s,s'}\rangle$ is a superposition of basis elements in $(A+s)\cap(B+t)$, giving that the set of $\Pi_{B+t}|A_{s,s'}\rangle$ over s is orthogonal. Thus,

$$\begin{aligned}
\Big\| \Pi_{B+t} \Big(\sum_{s\in \mathsf{CS}(A)} |A_{s,s'}\rangle\langle A_{s,s'}| \Big) \Pi_{B+t} \Big\| &\leq \max_{s\in\mathsf{CS}(A)} \big\| \Pi_{B+t} |A_{s,s'}\rangle\langle A_{s,s'}| \Pi_{B+t} \big\| \\
&= \max_{s\in\mathsf{CS}(A)} \langle A_{s,s'}| \Pi_{B+t} |A_{s,s'}\rangle \,,
\end{aligned} \tag{4}$$

which uses $\|\sum_s X_s\| \leq \max_s \|X_s\|$ for X_i Hermitian with orthogonal range. Now, for any $s \in \mathsf{CS}(A)$,

$$\begin{aligned}
\langle A_{s,s'}| \Pi_{B+t} |A_{s,s'}\rangle &= \frac{1}{2^{\frac{n}{2}}} \big|(A+s)\cap(B+t)\big| \\
&\leq \frac{1}{2^{\frac{n}{2}}} \big|A\cap B\big| \,.
\end{aligned}$$

Plugging this back into (4) completes the proof. ∎

The second lemma is a key bound used in [TFKW13].

Lemma 3.3 (Lemma 2 in [TFKW13])**.** *Let $P_1, ..., P_n$ be positive semidefinite operators on a Hilbert space. Then*

$$\left\| \sum_{i=1}^{n} P_i \right\| \leq \sum_{i=1}^{n} \max_{j=1,...,n} \left\| \sqrt{P_j} \sqrt{P_{\pi_i(j)}} \right\| ,$$

where $\pi_1, ..., \pi_n$ is any set of mutually orthogonal permutations of $\{1, ..., n\}$, i.e. $\pi_i \circ \pi_j^{-1}$ only has a fixed point if $i = j$.

We give the permutations we will use to apply Lemma 3.3. For $n \geq 2$ even let

$$C_{n,n/2} = \left\{ \gamma \in \{0,1\}^n : |\gamma| = \frac{n}{2} \right\} ,$$

where for a string γ, $|\gamma|$ denotes its Hamming weight (number of nonzero entries).

Lemma 3.4. *Let n be an even integer. Then there are $N = \binom{n}{n/2}$ mutually orthogonal permutations $\pi_1, \ldots, \pi_N$ of $C_{n,n/2}$ such that the following holds. For each $k \in \{0, \ldots, \frac{n}{2}\}$ there are exactly $\binom{\frac{n}{2}}{k}^2$ permutations π_j such that the number of positions at which γ and $\pi_j(\gamma)$ are both 1 is $\frac{n}{2} - k$.*

Proof. Fix $n \geq 2$ an even integer, and let $k \in \{1, \ldots, \frac{n}{2}\}$. Let $G_{n,k}$ be the graph with vertex set $C_{n,n/2}$ and an edge between any $\gamma, \gamma' \in C_{n,n/2}$ such that the number of positions at which γ and γ' are both 1 is exactly $\frac{n}{2} - k$.

We claim that the minimum degree d_k of $G_{n,k}$ is at least $\binom{\frac{n}{2}}{k}^2$. Indeed, for any $\gamma \in C_{n,n/2}$ we can define distinct γ' that are connected to it in $G_{n,k}$ by choosing k locations among the $\frac{n}{2}$ 1 positions of γ, k locations among the $\frac{n}{2}$ 0 positions, and flipping those values.

For each edge in $G_{n,k}$ create two directed edges to obtain a directed graph $\tilde{G}_{n,k}$. In $\tilde{G}_{n,k}$ each vertex has in-degree at least d_k, and out-degree at least d_k. Thus we can find d_k non-overlapping oriented vertex cycle covers of $\tilde{G}_{n,k}$, call them $c_{k,1}, \ldots, c_{k,d_k}$.[2] To each such oriented vertex cycle cover associate a permutation $\pi_{k,i}$ of $C_{n,n/2}$ in the natural way. By construction for any $i \neq i'$, $\pi_{k,i}$ and $\pi_{k,i'}$ are orthogonal.

For $k = 0$, set $\pi_{0,1}$ to be the identity permutation of $C_{n,n/2}$.

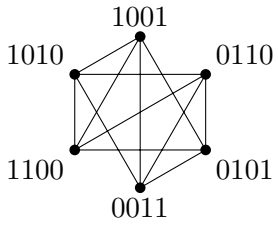
We observe that for $k \neq k'$ and any i, i' it must be that $\pi_{k,i}$ and $\pi_{k',i'}$ are orthogonal permutations. This is because two elements of $C_{n,n/2}$ can be connected by an edge in at most one $G_{n,k}$. To conclude, use that by the Vandermonde identity we have found a total of

$$N = \binom{n}{n/2} = \sum_{k=0}^{n/2} \binom{n/2}{k}^2$$

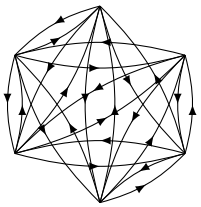
mutually orthogonal permutations, as desired. □

Remark 3.5. Instead of permutations of $C_{n,n/2}$ we can consider the π_j as permutations on the set of subsets of size $\frac{n}{2}$ of a universe of size n by fixing an ordering of the elements of the universe and, for any subset, considering the binary string to be the indicator function of the subset.

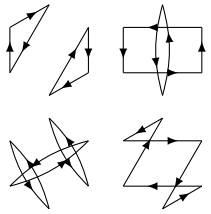
[2] To show this, find a first cycle cover in an arbitrary way and remove all edges used. This reduces both the out- and in-degrees by exactly 1. Repeat until the minimum degree reaches zero.



(a) The graph $G_{4,1}$.



(b) The graph $\tilde{G}_{4,1}$.



(c) A set of cycle covers.

Figure 1: Graph construction from Lemma 3.4 in the case of $n = 4, k = 1$.

We are ready to complete our proof of the upper bound on the winning probability of the coset-monogamy game.

Proof of Theorem 2.1. Fix a strategy for the coset-monogamy game, consisting of a channel $\Phi : \mathcal{H}_{\mathsf{A}} \to \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}}$ and, for each $A \in \mathsf{G}\big(\frac{n}{2}, n\big)$, POVMs $\{B_s^A\}_{s\in\mathsf{CS}(A)}$ for Bob and $\{C_{s'}^A\}_{s'\in\mathsf{CS}(A^\perp)}$ for Charlie. Let q'_n be the probability that this strategy succeeds in the game. Without loss of generality, assume that the POVMs are projective. Using Lemma 3.1,

$$\begin{aligned} q'_n &= \mathop{\mathrm{E}}_{A\in\mathsf{G}\left(\frac{n}{2},n\right)} \sum_{\substack{s\in\mathsf{CS}(A)\\ s'\in\mathsf{CS}(A^\perp)}} \mathrm{Tr}\Big(\big(|A_{s,s'}\rangle\langle A_{s,s'}| \otimes B_s^A \otimes C_{s'}^A\big)\rho\Big) \\ &\leq \Big\| \mathop{\mathrm{E}}_{A\in\mathsf{G}\left(\frac{n}{2},n\right)} \Pi^A \Big\| , \end{aligned}$$

where

$$\Pi^A = \sum_{\substack{s\in\mathsf{CS}(A)\\ s'\in\mathsf{CS}(A^\perp)}} |A_{s,s'}\rangle\langle A_{s,s'}| \otimes B_s^A \otimes C_{s'}^A \ .$$

As in [CLLZ21] we decompose the average over the subspaces followed by an average over bases of $\mathbb{F}_2^n$, and then over subspaces that may be spanned by $\frac{n}{2}$ vectors from the basis. Using the triangle inequality we can bound the winning probability as

$$q'_n \leq \mathop{\mathrm{E}}_{\beta \text{ basis of } \mathbb{F}_2^n} \Big\| \mathop{\mathrm{E}}_{\substack{\gamma\subseteq\beta\\ |\gamma|=\frac{n}{2}}} \Pi^{\mathrm{span}(\gamma)} \Big\| . \tag{5}$$

We apply Lemma 3.3 using the permutations $\pi_1, \ldots, \pi_N$ from Lemma 3.4, where $N = \binom{n}{n/2}$. Applying the lemma,

$$q'_n \leq \mathop{\mathrm{E}}_{\beta \text{ basis of } \mathbb{F}_2^n} \frac{1}{N} \sum_{j=1}^{N} \max_{\substack{\gamma\subseteq\beta\\ |\gamma|=\frac{n}{2}}} \big\| \Pi^{\mathrm{span}(\gamma)} \Pi^{\mathrm{span}(\pi_j(\gamma))} \big\| . \tag{6}$$

For any subspaces $A, B \in \mathsf{G}\big(\frac{n}{2}, n\big)$ define the projectors

$$P = \sum_{\substack{s\in\mathsf{CS}(A)\\ s'\in\mathsf{CS}(A^\perp)}} |A_{s,s'}\rangle\langle A_{s,s'}| \otimes \mathrm{Id}_{\mathsf{B}} \otimes C_{s'}^A \qquad \text{and} \qquad Q = \sum_{\substack{s\in\mathsf{CS}(B)\\ s'\in\mathsf{CS}(B^\perp)}} |B_{s,s'}\rangle\langle B_{s,s'}| \otimes B_s^B \otimes \mathrm{Id}_{\mathsf{C}} \ , \tag{7}$$

which satisfy $\Pi^A \le P$ and $\Pi^B \le Q$. Thus

$$\left\|\Pi^A\Pi^B\right\|^2 = \sup_{|v\rangle}\langle v|\Pi^B\Pi^A\Pi^B|v\rangle = \sup_{|v\rangle\in\textsc{Supp}(\Pi_B)}\langle v|\Pi^A|v\rangle \le \sup_{|v\rangle\in\textsc{Supp}(Q)}\langle v|P|v\rangle = \|PQ\|^2 \ , \qquad (8)$$

and using Lemma 3.2,

$$\begin{aligned}\left\|\Pi^A\Pi^B\right\| &\le \Big\| \sum_{\substack{(s,s')\in \mathsf{CS}(A)\times\mathsf{CS}(A^\perp)\\(t,t')\in\mathsf{CS}(B)\times\mathsf{CS}(B^\perp)}} |A_{s,s'}\rangle\langle A_{s,s'}|\cdot|B_{t,t'}\rangle\langle B_{t,t'}| \otimes B_t^B \otimes C_{s'}^A \Big\| \\ &= \max_{\substack{s'\in\mathsf{CS}(A^\perp)\\ t\in\mathsf{CS}(B)}} \Big\| \sum_{s\in\mathsf{CS}(A)} |A_{s,s'}\rangle\langle A_{s,s'}| \sum_{t'\in\mathsf{CS}(B^\perp)} |B_{t,t'}\rangle\langle B_{t,t'}| \Big\| \\ &\le \sqrt{2^{\dim(A\cap B)-\frac{n}{2}}} \ . \end{aligned} \qquad (9)$$

By Lemma 3.4 for $k \in \{0,\dots,\frac{n}{2}\}$ there are $\binom{\frac{n}{2}}{k}^2$ permutations π_j such that the dimension of $\mathrm{span}(\gamma)\cap\mathrm{span}(\pi_j(\gamma))$ is $\frac{n}{2}-k$. Plugging (9) back into (6) we thus get

$$\begin{aligned} q_n' &\le \mathop{\mathrm{E}}_{\beta \text{ basis of } \mathbb{F}_2^n} \frac{1}{N}\sum_{j=1}^{N} \max_{\substack{\gamma\subseteq\beta\\|\gamma|=\frac{n}{2}}} \sqrt{2^{\dim(\mathrm{span}(\gamma)\cap\mathrm{span}(\pi_j(\gamma)))-\frac{n}{2}}} \\ &\le \frac{1}{\binom{n}{\frac{n}{2}}}\sum_{k=0}^{\frac{n}{2}}\binom{\frac{n}{2}}{k}^2\sqrt{2^{-k}} \ . \end{aligned}$$

The final bound is provided by Lemma 3.6 stated below. □

Lemma 3.6. *For any even integer $n \ge 2$,*

$$\frac{1}{\binom{n}{\frac{n}{2}}}\sum_{k=0}^{\frac{n}{2}}\binom{\frac{n}{2}}{k}^2\sqrt{2^{-k}} \ \le \ \sqrt{e}\Big(\cos\frac{\pi}{8}\Big)^n \ .$$

Proof. We bound $\binom{\frac{n}{2}}{k} \le \binom{\frac{n}{2}}{\frac{n}{4}}$ for any $k \in \{0,\dots,\frac{n}{2}\}$ and

$$\begin{aligned}\frac{\binom{\frac{n}{2}}{\frac{n}{4}}}{\binom{n}{\frac{n}{2}}} &= \frac{1}{2^{\frac{n}{2}}}\Big(1+\frac{1}{n-1}\Big)\Big(1+\frac{1}{n-3}\Big)\cdots\Big(1+\frac{1}{\frac{n}{2}+1}\Big) \le \frac{1}{2^{\frac{n}{2}}}\Big(1+\frac{1}{\frac{n}{2}+1}\Big)^{\frac{n}{4}} \\ &\le \frac{\sqrt{e}}{2^{\frac{n}{2}}} \ , \end{aligned}$$

which gives

$$\begin{aligned}\frac{1}{\binom{n}{\frac{n}{2}}}\sum_{k=0}^{\frac{n}{2}}\binom{\frac{n}{2}}{k}^2\sqrt{2^{-k}} &\le \frac{\binom{\frac{n}{2}}{\frac{n}{4}}}{\binom{n}{\frac{n}{2}}}\sum_{k=0}^{\frac{n}{2}}\binom{\frac{n}{2}}{k}\sqrt{2^{-k}} \\ &\le \frac{\sqrt{e}}{2^{\frac{n}{2}}}\Big(1+\frac{1}{\sqrt{2}}\Big)^{\frac{n}{2}} \\ &= \sqrt{e}\Big(\cos\frac{\pi}{8}\Big)^n \ , \end{aligned}$$

as claimed. □

4 The basis-monogamy game

In this section we introduce a monogamy game which we call the *basis-monogamy game*. While this game is conceptually simpler than the coset-monogamy game introduced in Section 2, in the next section we will show that the latter can be reduced to the former. In this section we focus on the basis-monogamy game, which may be of independent interest, and its analysis.

We formulate the game directly as an extended nonlocal game, that can be seen as a variant of a game introduced in [TFKW13]. Informally, in the game from [TFKW13] two players Bob and Charlie are trying to both be maximally entangled with Alice: they are required to prepare a tripartite state ρ_{ABC}, where A is an n-qubit register handed over to Alice and B and C are arbitrary registers kept by Bob and Charlie respectively, such that when Alice measures her n qubits in a randomly chosen basis $\theta \in \{0,1\}^n$ (where as usual $\theta_i = 0$ denotes a measurement in the standard basis, and $\theta_i = 1$ a measurement in the Hadamard basis) to obtain a string of outcomes $x \in \{0,1\}^n$, given θ as side information Bob and Charlie are able to return strings $y, z \in \{0,1\}^n$ respectively such that $x = y = z$. Our variant of the game introduces two simple modifications: first, n is even and θ is chosen such that $|\theta| = \frac{n}{2}$, and second, Bob and Charlie are only asked to predict measurement outcomes associated with the standard basis ($\theta_i = 0$) and Hadamard basis ($\theta_i = 1$), respectively. More formally, for n an even integer the basis-monogamy game proceeds as follows.

Basis-monogamy game.

1. *Preparation:* Bob and Charlie together prepare a state ρ_{ABC} such that A is an n-qubit register and B and C are arbitrary. They pass A to Alice and keep registers B and C to themselves, respectively.

2. *Question:* Alice chooses $\theta \in \{0,1\}^n$ uniformly at random conditioned on $|\theta| = \frac{n}{2}$. Alice measures each qubit of A in the basis indicated by θ to obtain a string of outcomes $x \in \{0,1\}^n$. She sends θ to Bob and Charlie. Let $T = \{i \in \{1,\ldots,n\} : \theta_i = 0\}$.

3. *Answer:* Bob returns a string $y \in \{0,1\}^T$. Charlie returns a string $z \in \{0,1\}^{\overline{T}}$.

4. *Winning condition:* Bob and Charlie win if and only if $y = x_T$ and $z = x_{\overline{T}}$.

Naturally this game is slightly easier than the one considered in [TFKW13]. Nevertheless we can use the same proof technique to bound the maximum success probability and obtain the following result.

Theorem 4.1. *Let $n \geq 1$ be an even integer. Let p_n be Bob and Charlie's maximum probability of winning in the basis-monogamy game. Then*

$$p_n \leq \sqrt{e}\Big(\cos\frac{\pi}{8}\Big)^n .$$

Remark 4.2. We have that $\cos\frac{\pi}{8} \approx 0.924$, whereas in [TFKW13] the bound $(1/2 + 1/(2\sqrt{2}))^n \approx 0.854^n$ is obtained on the success probability for the variant of the game where Bob and Charlie both have to answer a complete string of measurement outcomes $y, z \in \{0,1\}^n$. Since our version of the game is easier, the bound is slightly weaker. We did not attempt to check if the bound we obtain is optimal.

Proof. The proof follows very closely the proof of [TFKW13, Theorem 3]. Fix an arbitrary strategy for the game that succeeds with probability p'_n. The strategy consists of a state ρ_{ABC} and for each $\theta \in C_{n,n/2} = \{\gamma \in \{0,1\}^n : |\gamma| = \frac{n}{2}\}$ two POVM $\{B_y^\theta\}_{y\in\{0,1\}^T}$ and $\{C_z^\theta\}_{z\in\{0,1\}^{\overline{T}}}$ respectively. Applying Naimark's

dilation theorem if needed, assume without loss of generality that both families of measurements are projective. For any $\theta \in \{0,1\}^n$ such that $|\theta| = \frac{n}{2}$ define

$$\Pi^\theta \;=\; \sum_{x\in\{0,1\}^n} |x\rangle\langle x|_\theta \otimes B^\theta_{x_T} \otimes C^\theta_{x_{\overline{T}}}\,.$$

Then Π^θ is a projector. Furthermore we can express the strategy's success probability as

$$\begin{aligned} p'_n &= \mathop{\mathrm{E}}_{\theta\in C_{n,n/2}} \mathrm{Tr}\big(\Pi^\theta\,\rho_{\mathsf{ABC}}\big) \\ &\leq \Big\| \mathop{\mathrm{E}}_{\theta\in C_{n,n/2}} \Pi^\theta \Big\| \\ &\leq \frac{1}{N}\sum_{k=1}^{N} \max_\theta \big\|\Pi^\theta \Pi^{\pi^k(\theta)}\big\|\,, \end{aligned} \tag{10}$$

where the first inequality follows by linearity and the definition of the operator norm and the second inequality follows from 3.3. In the third line we set $N = \binom{n}{n/2}$ and $\pi^1,\ldots,\pi^N$ are the N mutually orthogonal permutations promised by Lemma 3.4.

Note that at this stage we are in a situation that is very similar to the situation at Eq. (6) in the proof of Theorem 2.1. The only difference is that there is a single basis β that is the standard basis of $\mathbb{F}_2^n$ (i.e. the coordinate vectors). We make the correspondence between the two situations more explicit in Section 5. Here, for clarity we complete the proof without at all resorting to the notation of subspaces.

Fix an arbitrary pair (θ,θ') and let R be the set of indices in which θ and θ' differ. Without loss of generality, assume that θ_R has Hamming weight at most $|R|/2$; if not we exchange the roles of θ and θ'. Let $S = \{i \in R :\, \theta_i = 0\}$, so that $S \subseteq R$ and $|S| > |R|/2$. Let

$$T = \{i :\, \theta_i = 0\} \qquad \text{and} \qquad T' = \{i :\, \theta'_i = 0\}\,,$$

so that $S \subseteq T \cap \overline{T'}$. Let

$$\overline{P} \;=\; \sum_{x_T\in\{0,1\}^T} \big(|x_S\rangle\langle x_S| \otimes \mathrm{Id}_{\overline{S}}\big) \otimes B^\theta_{x_T} \otimes \mathrm{Id}_{\mathsf{C}}\,,$$

where $\mathrm{Id}_{\overline{S}}$ denotes the identity on qubits of register A that do not lie in the set S. Similarly, let

$$\overline{Q} \;=\; \sum_{x_{\overline{T'}}\in\{0,1\}^{\overline{T'}}} \big(H^S|x_S\rangle\langle x_S|H^S \otimes \mathrm{Id}_{\overline{S}}\big) \otimes \mathrm{Id}_{\mathsf{B}} \otimes C^{\theta'}_{x_{\overline{T'}}}\,,$$

where H^S denotes a Hadamard on each of the qubits in S. We compute

$$\begin{aligned} \overline{P}\,\overline{Q}\,\overline{P} &= \sum_{x_T, y_{\overline{T'}}, z_T} |x_S\rangle\langle x_S|H^S|y_S\rangle\langle y_S|H^S|z_S\rangle\langle z_S| \otimes \mathrm{Id}_{\overline{S}} \otimes P^\theta_{x_T} P^\theta_{z_T} \otimes Q^{\theta'}_{y_{\overline{T'}}} \\ &= \sum_{x_T, y_{\overline{T'}}} |x_S\rangle\langle x_S|H^S|y_S\rangle\langle y_S|H^S|x_S\rangle\langle x_S| \otimes \mathrm{Id}_{\overline{S}} \otimes P^\theta_{x_T} \otimes Q^{\theta'}_{y_{\overline{T'}}} \\ &= 2^{-|S|} \sum_{x_T} |x_S\rangle\langle x_S| \otimes \mathrm{Id}_{\overline{S}} \otimes P^\theta_{x_T} \otimes \mathrm{Id}_{\mathsf{C}}\,, \end{aligned}$$

where for the second line we used that $P^\theta_{x_T} P^\theta_{z_T} = \delta_{x_T,z_T} P^\theta_{x_T}$ and for the third line that $|\langle x_S|H^S|y_S\rangle|^2 = 2^{-|S|}$ for all x, y and $\sum_{y_{\overline{T'}}} Q^{\theta'}_{y_{\overline{T'}}} = \mathrm{Id}_{\mathsf{C}}$ for all θ'. Using that $\sum_{x_T} P^\theta_{x_T} = \mathrm{Id}$ it follows that

$$\|\overline{PQP}\| \leq 2^{-|S|} \;\leq\; 2^{-|R|/2}\;,$$

where the second inequality is because $|S| \geq |R|/2$. Hence for all (θ, θ'),

$$\begin{aligned}
\left\|\Pi^\theta \Pi^{\theta'}\right\|^2 &= \left\|\Pi^{\theta'} \Pi^\theta \Pi^{\theta'}\right\| \\
&\leq \left\|\Pi^{\theta'}\, \overline{P}\, \Pi^{\theta'}\right\| \\
&= \left\|\overline{P}\, \Pi^{\theta'}\, \overline{P}\right\| \\
&\leq \left\|\overline{P}\, \overline{Q}\, \overline{P}\right\| \\
&\leq 2^{-|R|/2}\;, \qquad (11)
\end{aligned}$$

where in the first equality we used that Π^θ is a projection, the first inequality uses $\Pi^\theta \leq \overline{P}$ because $C^\theta_{x_{\overline{T}}} \leq \mathrm{Id}$ for all $x_{\overline{T}}$, the second equality uses that $\overline{P}$ and $\Pi^{\theta'}$ are projections and the last inequality that $\Pi^{\theta'} \leq \overline{Q}$.

By Lemma 3.4 for any $k \in \{0, \ldots, \frac{n}{2}\}$ there are $\binom{n/2}{k}^2$ permutations π_j such that θ and $\pi_j(\theta)$ differ in $2k$ positions, i.e. such that $|R| = 2k$. Returning to (10) and using (11) we obtain

$$p'_N \leq \frac{1}{N} \sum_{k=0}^{n/2} \binom{n/2}{k}^2 2^{-k/2}\;. \qquad (12)$$

We conclude using Lemma 3.6. □

5 Reduction to the coset-monogamy game

In this section we show a reduction from the coset-monogamy game to the basis-monogamy game. This gives a second proof of Theorem 2.1, by reduction to Theorem 4.1.

Proposition 5.1. *Let $n \geq 2$ be an even integer. Let p_n be the maximum probability of winning for Bob and Charlie in the basis-monogamy game. Let q_n be the maximum probability of winning for the adversary, Bob and Charlie in the coset-monogamy game. Then*

$$q_n \;\leq\; p_n\;.$$

Proof. Let $n \geq 2$ be even. Fix a strategy for the adversary that succeeds with some probability $q'_n \leq q_n$ in the coset-monogamy game. This strategy is specified by a channel Φ and families of POVM $\{B^A_s\}_{s\in\mathbb{F}_2^n}$ and $\{C^A_s\}_{s\in\mathbb{F}_2^n}$ for Bob and Charlie respectively. Here, the POVMs are indexed by subspaces A and return outcomes $s \in \mathbb{F}_2^n$.

We define a strategy for Bob and Charlie in the basis-monogamy game that succeeds with probability $p'_n = q'_n$. The strategy is as follows:

1. Bob and Charlie prepare n EPR pairs, $\rho_{\mathsf{AA'}} = |\phi^+\rangle\langle\phi^+|^{\otimes n}$ where $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and registers A and $\mathsf{A'}$ are n qubits each, containing the n first halves and the n second halves of the EPR pairs

respectively. They select a uniformly random basis $\mathcal{B} = \{u_1, \ldots, u_n\}$ of $\mathbb{F}_2^n$ which they each keep a copy of. Let $U_\mathcal{B}$ be the unitary of $(\mathbb{C}^2)^{\otimes n}$ which permutes standard basis vectors as

$$\forall x \in \{0,1\}^n \,, \qquad U_\mathcal{B}|x\rangle \,=\, \Big|\sum_i x_i u_i\Big\rangle \,. \tag{13}$$

They apply U_B to register A' and then compute

$$\rho_{\mathsf{ABC}} \,=\, \big(\mathrm{Id}_\mathsf{A} \otimes \Phi_{\mathsf{A'}\to\mathsf{BC}}\big)\big((\mathrm{Id}_\mathsf{A} \otimes U_\mathcal{B})[\rho_{\mathsf{AA'}}]\big) \,, \tag{14}$$

where for any linear maps X, Y on $\mathcal{H}$ we write $X[Y]$ for $XYX^\dagger$. They send register A to the challenger. Bob keeps register B and Charlie keeps register C.

2. Let $\theta \in \{0,1\}^n$ be the question selected by the challenger. Upon receipt of θ, Bob and Charlie each set

$$A = \mathrm{Span}\{u_i : \theta_i = 1\} \tag{15}$$

and $T = \{i : \theta_i = 0\}$. Bob measures the qubits in B using $\{B_s^A\}$ to obtain an outcome s_1. Charlie measures the qubits in C using $\{C_s^A\}$ to obtain an outcome s_2. Let $s_1 = \sum_i y_i u_i$ and $s_2 = \sum_i z_i u_i$, where $y, z \in \{0,1\}^n$, be the unique decomposition of each vector in the basis $\{u_i\}$ of $\mathbb{F}_2^n$. Bob returns y_T and Charlie returns $z_{\overline{T}}$.

We introduce notation to express the winning probability of this strategy in the basis-monogamy game. For a basis $\mathcal{B} = \{u_1, \ldots, u_n\}$ of $\mathbb{F}_2^n$ and $\theta \in \{0,1\}^n$, $T = \{i : \theta_i = 0\}$ and $y \in \{0,1\}^T, z \in \{0,1\}^{\overline{T}}$ we let A be the space spanned by $\{u_i : \theta_i = 1\}$ and

$$B_y^{(\mathcal{B},\theta)} \,=\, \sum_{y' \colon y' \cdot u_i = y_i \forall i \in T} B_{y'}^A \,, \qquad C_z^{(\mathcal{B},\theta)} \,=\, \sum_{z' \colon z' \cdot u_i = z_i \forall i \in \overline{T}} C_{z'}^A \,. \tag{16}$$

Note that here T is determined by θ, and for all $(\mathcal{B}, \theta)$, both $\{B_y^{(\mathcal{B},\theta)}\}_{y \in \{0,1\}^T}$ and $\{C_z^{(\mathcal{B},\theta)}\}_{z \in \{0,1\}^{\overline{T}}}$ is a POVM. With this notation we can write

$$p'_n \,=\, \mathop{\mathrm{E}}_{\theta \in \{0,1\}^n} \mathop{\mathrm{E}}_{\mathcal{B}} \sum_{x \in \{0,1\}^n} \mathrm{Tr}\Big(\big(|x\rangle\langle x|_\theta \otimes B_{x_T}^{(\mathcal{B},\theta)} \otimes C_{x_{\overline{T}}}^{(\mathcal{B},\theta)}\big)\rho_{\mathsf{ABC}}\Big) \,,$$

where ρ_{ABC} is the state defined in (14) and the expectation is over a uniformly random $\theta \in \{0,1\}^n$ (as chosen by the challenger) and basis $\mathcal{B} = \{u_1, \ldots, u_n\}$ for $\mathbb{F}_2^n$ (as chosen by Bob and Charlie). Using Claim 5.2,

$$(|x\rangle\langle x|_\theta \otimes U_\mathcal{B})|\phi^+\rangle^{\otimes n} \,=\, \frac{1}{\sqrt{2^n}}|x\rangle_\theta \otimes U_\mathcal{B}|x\rangle_\theta \,=\, \frac{1}{\sqrt{2^n}}|x\rangle_\theta \otimes |A_{s,s'}\rangle \,,$$

where A is defined from x, θ and $\mathcal{B}$ as in (15), $s = \sum_{i \in T} x_i u_i$ and $s' = \sum_{i \in \overline{T}} x_i u_i$. Thus

$$\begin{aligned} p'_n &= \mathop{\mathrm{E}}_{\theta \in \{0,1\}^n} \mathop{\mathrm{E}}_{\mathcal{B}} \sum_{x \in \{0,1\}^n} \langle A_{s,s'}|B_{x_T}^{(\mathcal{B},\theta)} \otimes C_{x_{\overline{T}}}^{(\mathcal{B},\theta)}|A_{s,s'}\rangle \\ &= \mathop{\mathrm{E}}_{A} \mathop{\mathrm{E}}_{(s,s')A^\perp \times A} \sum_{u \in A,\, v \in A^\perp} \langle A_{s,s'}|B_u^A \otimes C_v^A|A_{s,s'}\rangle \\ &= \mathop{\mathrm{E}}_{A} \mathop{\mathrm{E}}_{(s,s') \in \{0,1\}^n \times \{0,1\}^n} \sum_{u \in A,\, v \in A^\perp} \langle A_{s,s'}|B_u^A \otimes C_v^A|A_{s,s'}\rangle \,, \end{aligned} \tag{17}$$

where the second equality is by definition of $B_{x_T}^{\mathcal{B},\theta}$ and $C_{x_{\overline{T}}}^{(\mathcal{B},\theta)}$ in (16) and the expectation is over a uniformly random subspace $A \subseteq \mathbb{F}_2^n$ of dimension $\frac{n}{2}$. Here we used that choosing such an A uniformly at random and returning $(A, A^\perp)$ yields the same distribution as choosing a basis $\mathcal{B} = \{u_1, \ldots, u_n\}$ and $\theta \in \{0,1\}^n$ such that $|\theta| = \frac{n}{2}$ uniformly at random and returning $(\text{Span}\{u_i : \theta_i = 1\}, \text{Span}\{u_i : \theta_i = 0\})$. In the second line above, the expectation over s, s' is uniform over $s \in A^\perp$ and $s' \in A$, and in the third line it is uniform over $s, s' \in \{0,1\}^n$; equality between the second and third lines follows from the definition of $|A_{s,s'}\rangle$. The expression in (17) is precisely q'_n, hence we have shown that $p'_n = q'_n$. Taking the supremum over all strategies in the coset-monogamy game proves the lemma. □

The following claim is used in the proof of Proposition 5.1.

Claim 5.2. *Let $\{u_1, \ldots, u_n\}$ be a basis of $\mathbb{F}_2^n$ and $U_\mathcal{B}$ defined as in* (13)*. Let $T \subseteq \{1, \ldots, n\}$ be such that $|T| = n/2$ and $A = \text{Span}\{u_i : i \in \overline{T}\}$. Let $\theta \in \{0,1\}^n$ be the indicator of $\overline{T}$ and $x \in \{0,1\}^n$. Let $s = \sum_{i \in T} x_i u_i$ and $s' = \sum_{i \in \overline{T}} x_i u_i$. Then*

$$|A_{s,s'}\rangle \;=\; U_\mathcal{B}|x\rangle_\theta \;.$$

Proof. First observe that

$$|x\rangle_\theta = X^{x_T}|0\rangle_\theta = X^{x_T} Z^{x_{\overline{T}}}|0\rangle_\theta \;. \tag{18}$$

Next we verify that for any $x, x' \in \{0,1\}^n$,

$$U_\mathcal{B} X^x U_\mathcal{B}^\dagger \;=\; X^t \qquad \text{and} \qquad U_\mathcal{B} Z^{x'} U_\mathcal{B}^\dagger \;=\; Z^{x'} \;, \tag{19}$$

where $t = \sum_i x_i u_i$ and $t' = \sum_i x'_i u_i$. This completes the proof of the claim as

$$\begin{aligned} U_\mathcal{B}|x\rangle_\theta &= U_\mathcal{B} X^{x_T} Z^{x_{\overline{T}}}|0\rangle_\theta \\ &= X^s Z^{s'} U_\mathcal{B}|0\rangle_\theta \\ &= X^s Z^{s'}|A\rangle \\ &= |A_{s,s'}\rangle \;, \end{aligned}$$

where the first line is by (18), the second by (19), the third by definition of $|A\rangle$, $U_\mathcal{B}$, and $|0\rangle_\theta = \sum_{b \in \{0,1\}^{\overline{T}}} |\sum_i b_i e_i\rangle$, and the last is by definition of $|A_{s,s'}\rangle$.

It remains to show (18). We show the first relation, the second is analogous. Writing $X^x = \sum_y |x + y\rangle\langle x|$ and using the definition of $U_\mathcal{B}$ we get

$$U_\mathcal{B} X^x U_\mathcal{B}^\dagger \;=\; \sum_y |y' + t\rangle\langle y'| \;,$$

where we defined $y' = \sum_i y_i u_i$ and used linearity. The right-hand side is precisely X^t. □

References

[CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. *arXiv preprint arXiv:2107.05692*, 2021.

[JMRW16] Nathaniel Johnston, Rajat Mittal, Vincent Russo, and John Watrous. Extended non-local games and monogamy-of-entanglement games. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 472(2189):20160003, 2016.

[Koa06] Masato Koashi. Unconditional security of quantum key distribution and the uncertainty principle. In *Journal of Physics: Conference Series*, volume 36, page 016. IOP Publishing, 2006.

[TFKW13] Marco Tomamichel, Serge Fehr, Jedrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, 2013.

[TL17] Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, 2017.

[VZ21] Thomas Vidick and Tina Zhang. Classical proofs of quantum knowledge. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 630–660. Springer, 2021.