Succinct analysis of the question-succinct Pauli braiding test

Angus Lowe* Quynh Nguyen†

October 31, 2024

Abstract

The Pauli braiding test is a nonlocal game in which a verifier interacts classically with two non-communicating but entangled provers in such a way that, in order to win the game, the provers essentially have no choice but to perform Pauli measurements. For many applications of this test, it is also important that some of the messages exchanged between the verifiers and provers be succinct, i.e., have length at most polylog(n) bits when testing n-qubit Paulis. In this note, we describe a recent simplification of the Pauli braiding test due to [Sal22] in which the questions are of length $\Theta(\log n)$, while the answers are of length $\Theta(n)$.

1 Introduction

Nonlocal games have featured prominently in many areas of quantum information science since the early days of the field. In particular, employing such games to rule out physical theories has a long history beginning with John Bell's seminal work on the subject [BA04]. That there exist nonlocal games which may also be used to test the presence of specific *states* or *behaviours* is a more modern, but equally compelling idea with wide-ranging applications in quantum complexity [Ji+22; MNZ24], cryptography [VV14; Gri20], and foundations [Bru+14]. Referred to as *self-testing* or *device-independent certification*, this class of tests grants a verifier the ability to certify properties of a system while making minimal assumptions about the details of that system.

In this note, we describe and analyze a specific example of a nonlocal game which can serve as a self-test of states and measurements, called the *Pauli braiding test* (PBT). Though several variations of the PBT have been proposed [NV17; Vid; Ji+22; Sal22], each has the same overall format. First, a verifier sends classical questions to the provers, Alice and Bob, who may share an entangled state but do not communicate with each other. The questions sent to the provers by the verifier may be interpreted as instructions to measure certain Pauli observables. If Alice and Bob are honest then their strategy is to perform the requested Pauli measurements and send the outcomes back to the verifier, passing the test with certainty.

Remarkably, the PBT is *robust* in the sense that any strategy adopted by Alice and Bob which succeeds with high probability must be proportionally close to the honest one, up to certain unimportant local transformations. As explained in [Vid], this is analogous to the classical linearity test of Blum, Luby, and Rubinfield [BLR93] in which a near-optimal strategy is necessarily derived from a function which is close to linear. In both cases, the robustness is ultimately a consequence of the stability of approximate group representations, as described in further detail in Section 2.5 and in the note by de la Salle [Sal22].

*alowe7@mit.edu
†qnguyen@g.harvard.edu

The PBT has a number of noteworthy applications, a few of which we now summarize. First, it can be used directly as a means to test high-dimensional entanglement in a robust manner. Namely, using classical messages of length $O(n)$, any strategy for the provers which succeeds with probability constantly close to 1 must involve measurements performed on a shared state which is constantly close to n EPR pairs [NV17]. This is significant as prior work required a success probability of at least $1 - 1/\mathrm{poly}(n)$ to reach the same conclusion [Vid].

The PBT can also serve as a subroutine within a larger protocol which "commands" Alice and Bob to perform measurements in the Pauli basis. Utilizing the test in this manner allows one to perform the remainder of the analysis for a given protocol assuming that Alice and Bob adopt the honest measurement strategy, effectively transforming untrustworthy parties into trusted measurement devices. For example, in the protocol for delegated quantum computation of Grilo [Gri20], the PBT is used in conjunction with an "energy test" to verify a BQP computation on a pair of remote servers which need only possess the computational power of a quantum computer in the honest case. In the language of interactive proofs, this gives a prover-efficient MIP^* protocol for BQP.

In quantum complexity, the PBT has been proposed as a tool to construct an MIP^* protocol with succinct questions and answers when the honest provers are required to be efficient (given copies of a QMA witness) and the problem being verified is QMA-Complete. Such a protocol would answer the games variant of the quantum PCP conjecture in the affirmative. Unfortunately, it is not known whether this conjecture is true at the time of writing [NN24]. However, a question-succinct PBT was employed successfully in recent work which constructs a succinct classical argument system for QMA from standard cryptographic assumptions [MNZ24]. Finally, we mention that a question-succinct PBT plays an important role in the proof that $\mathsf{MIP}^* = \mathsf{RE}$. (Here, MIP^* denotes protocols in which the provers are all-powerful.)

For some of the above applications, it is desirable to have the length of the questions and answers in the PBT be as short as possible. In particular, it was necessary to have a PBT with questions of length at most $\mathrm{polylog}(n)$ in [Ji+22] and at most $O(\log n)$ in [MNZ24]. To this end, a question-succinct PBT was derived in [Ji+22] and subsequently simplified in [Sal22]. The purpose of this note is to explain this construction of a PBT which has $\Theta(\log n)$-length questions and $\Theta(n)$-length answers in a mostly self-contained manner. We do, however, allow ourselves to defer some details regarding i) synchronous strategies and ii) the existence of small-biased sets. The latter of these, being quite standard, is perhaps excusable.

The rest of this note is organized as follows. In Section 2 we establish some preliminary notations and definitions, including those for two essential tools which appear later: small-biased sets (Section 2.4) and approximate representations (Section 2.5). Then in Section 3 we describe the PBT in detail, beginning with a non-succinct version before explaining how it leads naturally to the desired question-succinct PBT in Section 3.5.

2 Preliminaries

2.1 Notation

Sets and operators. The single-qubit Pauli operators are denoted in the standard way by $\sigma_X, \sigma_Y, \sigma_Z$. For any $a \in \{0,1\}^n$ we let $\sigma_Z(a) = \bigotimes_{i=1}^n \sigma_Z^{a_i}$ and $\sigma_X(a) = \bigotimes_{i=1}^n \sigma_X^{a_i}$. We use these notations interchangeably for both the operators themselves as well as abstract group elements. For any positive integer n we let $[n]$ denote the set $\{1, \ldots, n\}$. Let $\mathcal{H}$, $\mathcal{H}'$ be finite-dimensional Hilbert spaces. We denote by $\mathrm{L}(\mathcal{H}, \mathcal{H}')$ the set of linear maps from $\mathcal{H}$ to $\mathcal{H}'$, $\mathrm{L}(\mathcal{H})$ the set of linear maps from $\mathcal{H}$ to $\mathcal{H}$, $\mathrm{D}(\mathcal{H}) \subset \mathrm{L}(\mathcal{H})$ the set of quantum states (positive semidefinite operators of unit trace)

on $\mathcal{H}$, and $\mathrm{U}(\mathcal{H})$ the set of unitary operators on $\mathcal{H}$. We let $\mathbb{R}_+$ denote the set of nonnegative real numbers.

State-dependent norm. For any two square linear operators $A, B \in \mathrm{L}(\mathcal{H})$ and quantum state $\rho \in \mathrm{D}(\mathcal{H})$ acting on a Hilbert space $\mathcal{H}$ of dimension d define the state-dependent semi-inner-product[1] $\langle A, B\rangle_\rho := \mathrm{Tr}\big(A^\dagger B \rho\big)$. We denote by $\|\cdot\|_\rho$ the norm induced by this inner product, $\|A\|_\rho = \sqrt{\langle A, A\rangle_\rho}$. In the special case where $\rho = I/d$ is the maximally mixed state, the state-dependent norm is equivalent to a *normalized Frobenius norm*, $\|A\|_f := \sqrt{\mathrm{Tr}(A^\dagger A)/d}$. The following fact will later be useful.

Fact 2.1. *For any $\rho \in \mathrm{L}(\mathcal{H})$, the squared state-dependent norm $\|\cdot\|_\rho^2 : \mathrm{L}(\mathcal{H}) \to \mathbb{R}_+$ is a convex function.*

Proof. The state-dependent semi-inner-product satisfies the Cauchy-Schwarz Inequality, and therefore the state-dependent norm satisfies the Triangle Inequality. Since $x \mapsto x^2$ is a non-decreasing function on $[0, \infty)$ and is convex, the composition of this function with the state-dependent norm is also convex. □

2.2 Nonlocal games and synchronous correlations

Nonlocal game definitions. Given finite sets of questions $\mathcal{X}$, $\mathcal{Y}$ along with finite sets of answers $\mathcal{A}$, $\mathcal{B}$, a *nonlocal game* is specified by choosing a distribution ν over the questions as well as a *decision predicate* $D(ab|xy) \in \{0, 1\}$ for all $(x, y, a, b) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B}$. Here, $\mathcal{X}$ and $\mathcal{Y}$ should be interpreted as possible questions a verifier may ask Alice and Bob, respectively, while $\mathcal{A}$ and $\mathcal{B}$ denote their possible answers. The decision predicate D represents the winning condition of the game: upon receiving x and y as questions, Alice and Bob win whenever they respond with answers a, b such that $D(ab|xy) = 1$. In the game, Alice and Bob reply with answers according to some *correlation* $C = (C_{x,y,a,b})_{x,y,a,b} \subset [0, 1]$ which, for each restriction to a fixed x and y, defines a valid joint distribution over answers a and b. The winning probability, or *value* of the nonlocal game is then

$$\omega(C) := \sum_{x,y} \nu(x, y) \sum_{a,b} D(ab|xy)\ C_{x,y,a,b} \tag{1}$$

In the MIP^* setting, Alice and Bob are further assumed to be unable to communicate while playing the game[2]. The game is therefore one of incomplete information, where correlations induced by the strategy in which Alice simply sends Bob her question x are not *a priori* valid. Instead, their strategy must comprise local measurements performed on a shared quantum state.

Formally, a *quantum strategy* for a game of the above form is specified by a tuple of $\mathfrak{S} = (|\psi\rangle, A, B)$, where $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a bipartite quantum state shared between Alice and Bob, $A = \{A_a^x\} \subset \mathrm{L}(\mathcal{H}_A)$ and $B = \{B_b^y\} \subset \mathrm{L}(\mathcal{H}_B)$ are collections (indexed by x and y) of PVMs (indexed by a and b) performed by Alice and Bob, respectively. The correlation induced by the strategy is

$$C_{x,y,a,b} = \langle\psi|\, A_a^x \otimes B_b^y\, |\psi\rangle \tag{2}$$

for every $(x, y, a, b) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B}$. Of particular importance in this note are *synchronous correlations* which are defined to be those correlations which are induced by convex combinations

[1] "Semi" because it is not conjugate symmetric.

[2] This can be enforced through the postulates of special relativity by making them play far enough apart from each other, hence the name "nonlocal".

of strategies on maximally entangled states[3]. More precisely, a correlation $C = (C_{x,y,a,b})_{x,y,a,b}$ is synchronous if there exists a family of quantum strategies $\{(|\psi_\lambda\rangle, A^\lambda, B^\lambda)\}_\lambda$ with $A^\lambda = \{A_a^{\lambda,x}\}$, $B^\lambda = \{B_b^{\lambda,y}\}$ denoting collections of PVMs such that

$$C_{x,y,a,b} = \mathbb{E}_\lambda \langle\psi_\lambda| A_a^{\lambda,x} \otimes B_b^{\lambda,y} |\psi_\lambda\rangle \tag{3}$$

where the expectation is with respect to some measure over λ, and for each λ it holds that $|\psi_\lambda\rangle$ is a maximally entangled state on some tensor product Hilbert space $\mathcal{H}_\lambda \otimes \mathcal{H}_\lambda$.

Synchronous strategies are w.l.o.g. We now provide a sketch as to why we assume Alice and Bob share an EPR state in our analysis. The main result of [Vid22] shows that there exist games for which a synchronous strategy wins the game with probability 1, and any strategy which wins the game with probability at least $1 - \varepsilon$ must induce a correlation which is $O(\varepsilon)$-close to a synchronous correlation, in a certain sense. By playing such a game with probability 1/2, and any other game of interest — e.g., the PBT — with probability 1/2, we can construct a new game for which the winning probability of any far-from-synchronous strategy is constantly far from the optimum, essentially "enforcing" that Alice and Bob adopt a near-synchronous strategy. Moreover, since synchronous strategies involve a convex combination of EPR states, the soundness of a test against arbitrary strategies is guaranteed by its soundness against strategies where Alice and Bob share an EPR state in some number of dimensions. Hence, in the rest of the note we assume that Alice and Bob adopt a strategy comprising PVMs performed on a shared EPR state.

Intuition for Vidick's result. The precise statement and the proof of the above result are technical and fall outside the intended scope of this note. However, we can provide a high level explanation for why the result is plausible. Let $|\psi\rangle$ be the entangled state in a near-optimal strategy and ρ be its reduced state on Bob. An observation in Vidick's proof (see also [Pau+16]) is the following simple decomposition of any density matrix into a convex combination of projectors

$$\rho = \int_0^{\lambda_{\max}(\rho)} d\lambda \Pi_{\geq\lambda}(\rho),$$

where $\Pi_{\geq\lambda}(\rho)$ is the projector onto the eigenvectors with eigenvalues at least λ and $\lambda_{\max}(\rho)$ is the top eigenvalue of ρ. Let the maximally entangled state $|\psi_\lambda\rangle$ be the canonical purification of $\Pi_{\geq\lambda}(\rho)$. Notice that $\int_\lambda d\lambda \operatorname{Tr}(\Pi_{\geq\lambda}(\rho)) = 1$, so $d\lambda \operatorname{Tr}(\Pi_{\geq\lambda}(\rho))$ forms a probability measure. Then Vidick's analysis essentially shows that the strategy can be viewed as a convex combination over $|\psi_\lambda\rangle$ under this measure. This analysis does rely on the fact that the original near-optimal strategy is almost-synchronous.

2.3 The magic square game

One of the prototype nonlocal games is the Mermin-Peres magic square game. In this game, Alice and Bob need to come up with 9-bit assignments to the cells in a 3 by 3 square that are consistent with each other. Alice is asked to report the assignment of a random row/column, while Bob is asked to report that of a random cell. They win iff the assignments are compatible. However, not all assignments are allowed. Each row or column, labelled by $\ell \in [6]$, has a set of valid bit assignments $V(\ell) \subseteq \{0,1\}^3$. In particular, we require the bits in each row to have even Hamming weight (i.e., the parity is even $\mathsf{Par}(\ell) = 1$) and in each column to have odd Hamming weight ($\mathsf{Par}(\ell) = -1$).

[3]This definition differs from the standard one in which a correlation is synchronous if $C_{x,x,a,b} = 0$ whenever $a \neq b$. That the two definitions are equivalent was shown in [Pau+16].

This game has a winning quantum strategy where Alice and Bob share a 2-qubit EPR state, and perform the measurements indicated in the table below.

$\sigma_Z \otimes \mathrm{I}$	$\mathrm{I} \otimes \sigma_Z$	$\sigma_Z \otimes \sigma_Z$
$\mathrm{I} \otimes \sigma_X$	$\sigma_X \otimes \mathrm{I}$	$\sigma_X \otimes \sigma_X$
$-\sigma_Z \otimes \sigma_X$	$-\sigma_X \otimes \sigma_Z$	$-\sigma_Z\sigma_X \otimes \sigma_X\sigma_Z$

Table 1: Winning strategy for the magic square game.

A fundamental result in nonlocal games is that if they win with probability 1, then their strategy must be equivalent to the aforementioned strategy, up to local isometries. Furthermore, this fact is 'rigid' (or self-testing): a strategy with winning probability $1-\varepsilon$ must be $O(\varepsilon)$-close to the optimal strategy, under certain notion of closeness. This property can be used as a test for the anticommutation of two operators (corresponding to the top center and middle left cells). This anticommutation test will be as subroutine in the Pauli braiding test. A proof of self-testing for general stategies can be found in [Wu+16]. We here give a simple proof assuming the strategy is synchronous.

Lemma 2.2 (Self-testing)**.** *Let $\{Q^j, \mathrm{I}-Q^j\}$ be Bob's PVM upon receiving question $j \in [9]$. Let $B^j = 2Q^j - \mathrm{I}$ (the Q^j outcome means Bob assigns 0 to cell j). If they win the magic square game with probability $1-\varepsilon$, then $\|B^2B^4 + B^4B^2\|_f^2 \le O(\varepsilon)$.*

Proof. Let Alice strategy be the PVMs $\{P^\ell_{a_1a_2a_3}\}_{a_1a_2a_3\in\{0,1\}^3}$ for each $\ell \in [6]$ labeling a row/column. So if Alice is asked for an assignment for a row/column ℓ, she perform the corresponding PVM and return the outcome (a_1, a_2, a_3). If $\ell = (i_1, i_2, i_3)$, we denote the marginals of the PVM as $P^\ell_{i_1} = \sum_{a_2,a_3:(0,a_2,a_3)\in V(\ell)} P^\ell_{0a_2a_3}$, and $P^\ell_{i_2}$, $P^\ell_{i_3}$ are similarly defined. Define the unitaries $A^\ell_j = 2P^\ell_j - \mathrm{I}$. By construction, it holds that

$$A^\ell_{i_1} = \mathsf{Par}(\ell) A^\ell_{i_2} A^\ell_{i_3}. \tag{4}$$

Suppose a line $\ell = (i_1, i_2, i_3)$ and a cell $j \in \{i_1, i_2, i_3\}$ is sampled (which happens with probability $1/18$). Then, the probability that Alice and Bob pass is

$$\begin{aligned}
1 - 18\varepsilon &\le \mathrm{Tr}\Big((P^\ell_j \otimes Q^j)\psi\Big) + \mathrm{Tr}\Big(((\mathrm{I}-P^\ell_j)\otimes(\mathrm{I}-Q^j))\psi\Big) \\
&= \mathrm{tr}\Big(Q^j (P^\ell_j)^\top\Big) + \mathrm{tr}\Big((\mathrm{I}-Q^j)(\mathrm{I}-P^\ell_j)^\top\Big) && (\psi \text{ is EPR state}) \\
&= 1 - \|(P^\ell_j)^\top - Q^j\|_f^2.
\end{aligned}$$

So we have

$$\|B^j - (A^\ell_j)^\top\|_f^2 \le 4\varepsilon, \qquad \forall j \in \ell. \tag{5}$$

Combining Eq. (4) and Eq. (5) we obtain

$$\|B^{i_1} - \mathsf{Par}(\ell) B^{i_2} B^{i_3}\|_f \le 6\sqrt{\varepsilon} \qquad \forall \ell = (i_1, i_2, i_3) \tag{6}$$

Therefore,

$$\begin{aligned}
B^2B^4 &\approx_{O(\sqrt{\varepsilon})} (B^1B^3)B^4 \approx_{O(\sqrt{\varepsilon})} -(B^4B^7)B^3B^4 \\
&\approx_{O(\sqrt{\varepsilon})} B^4B^7(B^9B^6)B^4 \approx_{O(\sqrt{\varepsilon})} B^4B^7B^9B^6(B^6B^5) \\
&\approx_{O(\sqrt{\varepsilon})} B^4B^7B^9B^5 \approx_{O(\sqrt{\varepsilon})} B^4B^8B^5 \\
&\approx_{O(\sqrt{\varepsilon})} -B^4B^2.
\end{aligned}$$

□

2.4 Small-biased sets

Later in the question-succint Pauli braiding test we will use a combinatorial tool called ϵ-biased sets. So we introduce them and their construction here.

Definition 2.3 (ϵ-biased set)**.** *A subset of n-bit strings $S \subseteq \mathbb{Z}_2^n$ is ϵ-biased if for any nonzero bit string $y \in \{0,1\}^n$ we have $|\mathbb{E}_{x\in S}(-1)^{x\cdot y}| \leq \epsilon$.*

A way to construct biased sets is via good error-correcting codes. Given a linear code C with parameters $[n,k,d]$ and bias ϵ, i.e., all codewords have normalized Hamming weight in $[(1-\epsilon)/2,(1+\epsilon)/2]$. To obtain a constant biased ϵ set with minimal size, we use a constant-biased code family with constant rate and linear distance, e.g., we can use the code in [TS17]. Given such code we construct an ϵ-biased set for $\mathbb{Z}_2^k$ of cardinality n as follows. Let $\{b^{(1)},\ldots,b^{(k)}\} \subseteq \mathbb{Z}_2^n$ be a basis for the code C. We define the set $S = \{x^{(i)} | x^{(i)} \in \mathbb{Z}_2^k, 1 \leq i \leq n, x^{(i)}_j = b^{(j)}_i\} \subseteq \mathbb{Z}_2^k$. Indeed, for any nonzero $y \in \mathbb{Z}_2^k$ we have

$$\begin{aligned}\left|\frac{1}{n}\sum_{i\in[n]}(-1)^{y\cdot x^{(i)}}\right| &= \left|\frac{1}{n}\sum_{i\in[n]}(-1)^{\sum_{j\in[k]} y_j b_i^{(j)} \mod 2}\right| \\ &= \left|\frac{1}{n}\sum_{i\in[n]}(-1)^{c_i}\right| \\ &= \left|1-2\frac{|c|}{n}\right| \leq \epsilon,\end{aligned}$$

where we noticed that $c \triangleq \sum_{j\in[k]} y_j b^{(j)} \in \mathbb{Z}_2^n$ is a nonzero codeword of C.

This notion of having a bounded bias is a special case of the *spectral gap* property defined in [Sal22]. More generally, the spectral gap of a measure over a countable group is defined to be the maximal second eigenvalue of the group Fourier transform of the measure. The current section corresponds to the special case of the abelian group $\mathbb{Z}_2^n$.

2.5 Approximate representations

In this section we introduce the concept of rounding approximate representations, which underlies the proof that the PBT serves as a robust self-test of measurements.

Definition 2.4 ((ϵ,σ)-approximate representation)**.** *Let $\sigma \in \mathrm{D}(\mathcal{H})$ be a quantum state, G be a finite group, and $f : G \to \mathrm{U}(\mathcal{H})$ be a function from the group to unitary operators. We say that f is an* (ϵ,σ)-approximate representation *of G if it holds that*

$$\mathbb{E}_{g,h\sim G} \|f(g)f(h) - f(gh)\|_\sigma^2 \leq \epsilon. \tag{7}$$

We mostly focus on $(\epsilon, I/d)$-approximate representations throughout this note, i.e., representations which are close on average with respect to the normalized Frobenius norm introduced in Section 2.1.

Theorem 2.5 (Gowers-Hatami (weaker version))**.** *If $f : G \to \mathrm{U}(\mathcal{H})$ is an (ϵ,σ)-approximate representation of the group G then there exists an isometry $V : \mathcal{H} \to \mathcal{H}'$ and a (true) representation $\pi : G \to \mathrm{U}(\mathcal{H})$ of G such that*

$$\mathbb{E}_{g\sim G} \|f(g) - V^\dagger \pi(g) V\|_\sigma^2 \leq \epsilon.$$

Proof. We give an abridged proof here, following the proof of Theorem 3.1 in [MNZ24]. Consider the regular representation of G on $\mathrm{span}\{|g\rangle : g \in G\}$,

$$\pi(g) = \sum_{g \in G} |h\rangle\langle hg| \quad \forall g \in G. \tag{8}$$

Define the convolution of f with itself

$$f^\star(g) := \mathbb{E}_{h \sim G}\, f(h)^\dagger f(hg) \tag{9}$$

and a linear map $\phi : \mathrm{L}(\mathcal{H}_G) \to \mathrm{L}(\mathcal{H})$ with the action $\phi : |g\rangle\langle h| \mapsto f^\star(g^{-1}h)/|G|$. Plugging in, it is easy to show ϕ is unital, and by looking at the Choi state one can show it is completely positive. By Theorem 2.26 in [Wat18], $\phi^\dagger$ is trace-preserving . By Stinespring dilation, this means there exists an isometry $V : \mathcal{H} \to \mathcal{H}_G \otimes \mathcal{Z}$ such that $\phi^\dagger$ has the action $\phi^\dagger : X \mapsto \mathrm{Tr}_{\mathcal{Z}}(VXV^\dagger)$, or equivalently,

$$\phi(Y) = V^\dagger(Y \otimes \mathbb{1}_{\mathcal{Z}})V \quad \forall Y \in \mathrm{L}(\mathcal{H}_G). \tag{10}$$

Noting that $f^\star(g) = \phi(\pi(g))$, we have

$$\mathbb{E}_{g \sim G} \|f(g) - V^\dagger(\pi(g) \otimes \mathbb{1}_{\mathcal{Z}})V\|_\sigma^2 = \mathbb{E}_{g \sim G} \|\mathbb{E}_{h \sim G}[f(g) - f(h)^\dagger f(hg)]\|_\sigma^2 \tag{11}$$

$$\leq \mathbb{E}_{g,h \sim G} \|f(g)f(h) - f(gh)\|_\sigma^2 \tag{12}$$

where the inequality follows from Fact 2.1 and Jensen's Inequality. Making use of Definition 2.4 concludes the proof. □

2.6 The Weyl-Heisenberg group

The Gowers-Hatami theorem can be applied to the the n-qubit Weyl-Heisenberg group. This is essentially the n-qubit Pauli group without complex numbers, and we define it precisely as follows . The single-qubit Weyl-Heisenberg group H_1 has 8 elements $\{\pm\sigma_I, \pm\sigma_X, \pm\sigma_Z, \pm\sigma_W\}$, with relations $\sigma_I = \sigma_X^2 = \sigma_Z^2$ and $\sigma_W = \sigma_X\sigma_Z = -\sigma_Z\sigma_X$. This group has four 1-dimensional irreps, which are specified by the image of σ_X and σ_Z onto $\{\pm 1\}$. Note that for such 1-dimensional irreps, $-\sigma_I$ must be mapped to 1, in order for the relation $\sigma_X\sigma_Z = -\sigma_Z\sigma_X$ to hold. On the other hand, H_1 has a unique 2-dimensional irrep, given by the usual 1-qubit Pauli matrices. The n-qubit Weyl-Heisenberg group H_n is the n-fold tensor product of H_1. It turns out that the only irrep that satisfies $\rho(-\sigma_I) = -\rho(\sigma_I)$ has dimension 2^n and is given by the defining matrix representation. All other irreps are 1-dimensional.

3 Pauli braiding test

3.1 Overview

Here we describe at a high level a PBT [Sal22; MNZ24] that uses $\Theta(n)$-bit questions and $\Theta(n)$-bit answers. The PBT involves two subtests, called the commutation test and the anticommutation test, whose details are explained in the next subsections. The precise statement of full PBT is provided in Section 3.4. The question-succint version of the PBT, with $\Theta(\log n)$-bit questions is described in Section 3.5.

The idea of the PBT is as follows. Consider an MIP^* protocol, where the questions to Bob are either "Z" or "X" (the precise description of the test will involve other question types to Bob, but let's ignore them for now, and also let's for the moment not worry about what happens on the

Alice's side). We expect Bob to responds with an n-bit string which he obtains by performing a 2^n-element PVM, either $\{\tau_a^Z\}_{a\in\{0,1\}^n}$ or $\{\tau_b^X\}_{b\in\{0,1\}^n}$, depending on what question he is asked. For example, if he is asked "Z", he performs the PVM $\{\tau_a^Z\}_{a\in\{0,1\}^n}$ and answers a if he obtains the corresponding measurement outcome. We can extract the following unitary operators from Bob's PVMs: $\hat{Z}(a) \triangleq \sum_{s\in\{0,1\}^n}(-1)^{s\cdot a}\tau_s^Z$ and $\hat{X}(b) \triangleq \sum_{s\in\{0,1\}^n}(-1)^{s\cdot b}\tau_s^X$. Although the verifier doesn't have direct access to these operators, he can still 'measure' $\hat{Z}(a)$ by aggregating the relevant bits in Bob's answer bitstring s, $\prod_{i:a_i=1} s_i$, the same procedure applies to $\hat{X}(b)$. These operators are suggestively named as Pauli operators, and indeed we will design the PBT to certify that they (approximately) satisfy the Pauli group relations.

In fact, they by definition satisfy the commutation relations within the Z-type operators and X-type operators. This can be easily derived using the definition of PVMs.

Claim 3.1. *The operators $\{\hat{Z}(a)\}_{a\in\{0,1\}^n}$ form a unitary representation of $\mathbb{Z}_2^n$. The same holds for the operators $\{\hat{X}(b)\}_{b\in\{0,1\}^n}$.*

Proof. We consider the Z case. The X case follows analogously. The operators $\hat{Z}(a)$ are unitaries because $\sum_s \tau_s^Z = \mathrm{I}$. In addition,

$$\begin{aligned}\hat{Z}(a)\hat{Z}(b) &= \sum_{s\in\{0,1\}^n}(-1)^{s\cdot a}\tau_s^Z \sum_{s'\in\{0,1\}^n}(-1)^{s'\cdot b}\tau_{s'}^Z \\ &= \sum_{s\in\{0,1\}^n}(-1)^{s\cdot(a+b)}\tau_s^Z \qquad \text{(using } \tau_s^Z\tau_{s'}^Z = \delta_{s,s'}\text{)} \\ &= \hat{Z}(a+b). \end{aligned}$$

□

Therefore, all we need to do is to certify that $\{\hat{Z}(a)\}$ and $\{\hat{X}(b)\}$ 'braid' correctly according to the Pauli group relations. We have two cases:

- $\hat{Z}(a)\hat{X}(b) = \hat{X}(b)\hat{Z}(a)$ when $a\cdot b = 0$,
- $\hat{Z}(a)\hat{X}(b) = -\hat{X}(b)\hat{Z}(a)$ when $a\cdot b = 1$.

The first case will be handled by the commutation test and the second is by the anticommutation test. Altogether, the PBT guarantees that $\{\hat{Z}(a)\}$ and $\{\hat{X}(b)\}$ forms an approximate representation for the Weyl-Heisenberg group. Then we can apply the Gowers-Hatami theorem to conclude that Bob's strategy is, up to isometry, close to n-qubit Pauli measurements.

3.2 Commutation test

This subsection gives a test for $\hat{Z}(a)\hat{X}(b) = \hat{X}(b)\hat{Z}(a)$ when $a\cdot b = 0$.

Commutation test: For fixed $a, b \in \{0,1\}^n$ such that $a\cdot b = 0$.

1. Verifier sends (a, b) to Alice. Alice responds with 2 bits (u_a, u_b). (Honest Alice measures $\sigma_Z(a)$ and $\sigma_X(b)$ on her n qubits, and returns the results as u_a and u_b respectively.)
2. Verifier selects randomly $W \in \{Z, X\}$ and sends to Bob. Bob responds with a bitstring $v \in \{0,1\}^n$. (Honest Bob measures each of his n qubits in the W basis and reports outcome.)
3. Verifier checks $\prod_{i:a_i=1} v_i = u_a$ if Z was sent to Bob and $\prod_{i:b_i=1} v_i = u_b$ otherwise.

Note that the test as described above still makes sense if we remove a, b from the questions/answers and ask Bob to only respond with 1 bit (this, accordingly, remove the need for the aggregation step 3). Doing so gives the vanilla commutation game: Alice receives no question and answers with 2 bits (u_0, u_1), and Bob receives a 1-bit question y and answers with a bit v_y, they pass if $v_y = u_y$. All we are doing is attaching labels 'a', 'b' to the operators that we're certifying the commutation relation against, so that we can use this test as a subroutine in PBT. Importantly, Bob doesn't know which operators he is being tested agains since a, b were never sent to Bob.

Lemma 3.2. *Consider a fixed $a, b \in \{0,1\}^n$ and the commutation game described earlier. Let the PVMs $\{\tau_v^W\}_{v\in\{0,1\}^n}$ for $W \in \{Z, X\}$ be Bob's strategy as described in the previous subsection. Suppose Alice and Bob pass the commutation test with probability $1-\varepsilon$. Define $\hat{W}(c) = \sum_{v\in\{0,1\}^n}(-1)^{c\cdot v}\tau_v^W$ for $W \in \{Z, X\}$. Then the following holds:*

$$\|[\hat{Z}(a), \hat{X}(b)]\|_f^2 \leq O(\varepsilon).$$

Proof. Let $O \triangleq \frac{\mathrm{I}+\hat{Z}(a)}{2}$ and $P \triangleq \frac{\mathrm{I}+\hat{X}(b)}{2}$ be Bob's PVMs associated to $\hat{Z}(a)$ and $\hat{X}(b)$. Let the PVM $\{M_{u_a,u_b}\}_{u_a,u_b\in\{0,1\}^2}$ be Alice's strategy and let $M_{u_a *} \triangleq \sum_{u_b\in\{0,1\}} M_{u_a u_b}$ and $M_{* u_b} \triangleq \sum_{u_a\in\{0,1\}} M_{u_a u_b}$ be Alice's marginalized PVM operators. Suppose $W = Z$, the probability they pass the test is

$$\begin{aligned}
1-\varepsilon_Z &\leq \mathrm{Tr}((M_{0*}\otimes O)\psi) + \mathrm{Tr}(((\mathrm{I}-M_{0*})\otimes(\mathrm{I}-O))\psi) \\
&= \mathrm{tr}\Big(M_{0*}^\top O\Big) + \mathrm{tr}\Big((\mathrm{I}-M_{0*}^\top)(\mathrm{I}-O)\Big) \\
&= 1 - \Big\|M_{0*}^\top - O\Big\|_f^2,
\end{aligned}$$

where we used the synchronous strategy assumption, taking ψ to be the EPR state in the compatible Hilbert space. Hence, $\big\|M_{0*}^\top - O\big\|_f^2 \leq \varepsilon_Z$. Similarly let we obtain $\big\|M_{*0}^\top - P\big\|_f^2 \leq \varepsilon_X$.

Therefore,

$$\begin{aligned}
\frac{1}{4}\|[\hat{Z}(a), \hat{X}(b)]\|_f &= \|[O, P]\|_f \\
&\leq \|[O - M_{0*}^\top, P]\|_f + \|[M_{0*}^\top, P - M_{*0}^\top\|_f + \|[M_{0*}^\top, M_{*0}^\top]\|_f \\
&\leq 2(\sqrt{\varepsilon_Z} + \sqrt{\varepsilon_X}) \leq 4\sqrt{\varepsilon}, \qquad \text{(using } \varepsilon_Z + \varepsilon_X = 2\varepsilon\text{)}
\end{aligned}$$

where the last inequality uses that $[M_{0*}^\top, M_{*0}^\top] = 0$ because $\{M_{u_a,u_b}\}_{u_a,u_b}$ is a PVM. □

3.3 Anticommutation test

This subsection gives a test for $\hat{Z}(a)\hat{X}(b) = \hat{X}(b)\hat{Z}(a)$ when $a \cdot b = 1$, which is based on the magic square game. Similar to the commutation test, all we are doing is attaching labels 'a', 'b' to the operators that we're certifying the anticommutation relation against, so that we can use the magic square as a subroutine in PBT.

Anti-commutation test: For fixed $a, b \in \{0,1\}^n$ such that $a \cdot b = 1$.

1. The verifier chooses a cell index $j \in [9]$ at random, and choosing a random line (row/-column) $\ell \in [6]$ containing the cell j. Let the cell indices in ℓ be (i_1, i_2, i_3) (one of them is j).

The magic square (MS) game is played with both provers, with the following modifications:

2. The verifier 'attaches' the label (a, b) to his MS question to Alice (so Alice always knows which Pauli operators she is being tested against). The expected answer is 3 bits (u_1, u_2, u_3) corresponding to the assignment in the corresponding cells.

3. If the MS question to Bob is cell 2 or cell 4, the verifier sends 'Z' or 'X' to Bob instead (in which case Bob doesn't know which operators he is being tested againts), Bob is expected to answer with an n-bit string v; in all other cases the verifier attaches the strings (a, b) to the original MS question and Bob answers with a bit assignment to the corresponding cell.

4. The verifier accepts iff the answers would have been accepted in the MS game, with a small modification. If the question to Bob is Z or X, the verifier aggregates his answer to extract the bit assignment to the corresponding cell (2 or 4): he computes $\prod_{i:a_i=1} v_i$ if Z was sent to Bob and $\prod_{i:b_i=1} v_i$ otherwise.

Lemma 3.3. *Consider a fixed $a, b \in \{0,1\}^n$ and the anticommutation game described earlier. Let the PVMs $\{\tau_v^W\}_{v\in\{0,1\}^n}$ for $W \in \{Z, X\}$ be Bob's strategy as described in the previous subsection. Suppose Alice and Bob pass the anticommutation test with probability $1-\varepsilon$. Define $\hat{W}(c) = \sum_{v\in\{0,1\}^n}(-1)^{c\cdot v}\tau_v^W$ for $W \in \{Z, X\}$. Then the following holds:*

$$\|\{\hat{Z}(a), \hat{X}(b)\}\|_f^2 \leq O(\varepsilon).$$

Proof. Directly follows from Lemma 2.2. □

3.4 Combining the subtests

We can now combine the two tests in the previous subsections to obtain the desired PBT. It can be seen that the questions and answers are $\Theta(n)$-bit long[4].

Pauli braiding test (non-succint)
Sample random $a, b \in \{0,1\}^n$.

- If $a \cdot b = 0$, perform the **commutation test**,
- If $a \cdot b = 1$, perform the **anticommutation test**.

Theorem 3.4. *Let the self-adjoint unitaties $\{\hat{Z}(a)\}_{a\in\{0,1\}^n}, \{\hat{X}(b)\}_{b\in\{0,1\}^n} \subset \mathbb{C}^{d\times d}$ be defined from Bob's strategy as described in Section 3.1. If Alice and Bob pass the test with probability $1-\varepsilon$, then there exists a representation $R : H_n \mapsto \mathrm{U}(\mathbb{C}^{d'})$ of H_n, and an isometry $V : \mathbb{C}^d \mapsto \mathbb{C}^{d'}$ such that*

$$\mathbb{E}_{a,b\in\{0,1\}^n, c\in\{0,1\}}\|(-1)^c\hat{Z}(a)\hat{X}(b) - V^\dagger R((-1)^c\sigma_X(a)\sigma_Z(b))V\|_f^2 \leq O(\varepsilon). \tag{13}$$

Proof. Consider the map $f : H_n \mapsto \mathrm{U}(\mathbb{C}^d)$ defined as $f((-1)^c\sigma_Z(a)\sigma_X(b)) = (-1)^c\hat{Z}(a)\hat{X}(b)$. We claim that succeeding in the PBT with probability $1-\varepsilon$ implies f is a $(O(\varepsilon), \frac{\mathrm{I}}{d})$-approximate

[4]We contrast this with the original PBT by Natarajan and Vidick [Vid] that has $\Theta(n)$-bit questions and $\Theta(1)$-bit answers. The PBT presented in the current paper has a shorter analysis, and admits a simple question-succint variant.

representation for the n-qubit Weyl-Heisenberg group. I.e.,

$$\mathbb{E}_{g,h\sim H_n}\|f(g)f(h)-f(gh)\|_f^2\leq O(\varepsilon). \tag{14}$$

Indeed, consider fixed a,b and let $1-\varepsilon_{a,b}$ be the probability the provers pass the PBT in this marginalized case. Note that $\mathbb{E}_{a,b}\varepsilon_{a,b}=\varepsilon$. According to Lemma 3.2 and Lemma 3.3, success with probability $1-\varepsilon_{a,b}$ in the relevant test implies

$$\|\hat{Z}(a)\hat{X}(b)-(-1)^{a\cdot b}\hat{X}(b)\hat{Z}(a)\|_f^2\leq O(\varepsilon_{a,b}) \tag{15}$$

This in turn implies

$$\begin{aligned}
&\|f(\sigma_Z(a)\sigma_X(b))f(\sigma_Z(a')\sigma_X(b'))-f((-1)^{b\cdot a'}\sigma_Z(a+a')\sigma_X(b+b'))\|_f^2\\
=&\|\hat{Z}(a)\hat{X}(b)\hat{Z}(a')\hat{X}(b')-(-1)^{b\cdot a'}\hat{Z}(a+a')\hat{X}(b+b')\|_f^2\\
\leq&\|(-1)^{b\cdot a'}\hat{Z}(a)\hat{Z}(a')\hat{X}(b)\hat{X}(b')-\hat{Z}(a+a')\hat{X}(b+b')\|_f^2+O(\varepsilon_{a',b})\\
=&O(\varepsilon_{a',b}),
\end{aligned}$$

where the first equality uses definition of f, the inequality uses Eq. (15), and the last equality uses Claim 3.1. Averaging the above and using $\mathbb{E}_{a',b}\varepsilon_{a',b}=\varepsilon$ gives Eq. (14) as claimed.

Finally, we invoke Theorem 2.5 to conclude that there exists a nearby true representation and an isometry as in the theorem statement. □

Removing 1-dimensional irreps. We can further restrict Eq. (13) to the irrep blocks correponding to the matrix defining irrep within the representation R. I.e., we can remove the 1-dimensional irreps as follows[5]. Notice that Eq. (13) implies

$$\mathbb{E}_{a,b\in\{0,1\}^n}\|\hat{Z}(a)\hat{X}(b)-\frac{1}{2}V^\dagger(\mathrm{I}-R(-\sigma_I))VV^\dagger R((\sigma_X(a)\sigma_Z(b))V\|_f^2\leq O(\varepsilon),$$

which, combining with Eq. (13) itself, in turn implies

$$\mathbb{E}_{a,b\in\{0,1\}^n}\|V^\dagger(\mathrm{I}+R(-\sigma_I))VV^\dagger R((\sigma_X(a)\sigma_Z(b))V\|_f^2\leq O(\varepsilon).$$

Since all the 1-dimensional irreps map $-\sigma_I$ to 1 (cf. Section 2.5), the above inequality means those irreps only constitutes a $O(\varepsilon)$ fraction of the representation R. So we assume all of those 1-dimensional irreps to be the trivial 1-dim irrep (mapping everything to the scalar 1) while incurring only a $O(\varepsilon)$ error. In other words, there exist a representation $R'((-1)^c\sigma_X(a)\sigma_Z(b))=((-1)^c\sigma_X(a)\sigma_Z(b))^{\otimes m}\oplus\mathrm{I}_{d_1}$, where m is the multiplicity of the defining irrep and d_1 is the total dimension of the 1-dimensional irreps from R, and an isometry V' such that

$$\mathbb{E}_{a,b\in\{0,1\}^n,c\in\{0,1\}}\|(-1)^c\hat{Z}(a)\hat{X}(b)-V'^\dagger R'((-1)^c\sigma_X(a)\sigma_Z(b))V'\|_f^2\leq O(\varepsilon). \tag{16}$$

Remark 3.5. *By symmetrizing the game, i.e. with probability 1/2 we instead treat the first prover as Bob, we can command both provers to perform Pauli measurements.*

[5]Lemma 3.3 of [MNZ24] gives another way to do this.

3.5 Question-succinct PBT

This section describes the recent simplified approach to a succint PBT due to de la Salle [Sal22], drawing heavily from the exposition in the recent paper by Metger, Natarajan, and Zhang [MNZ24]. Using the results established in the previous sections, we have all the ingredients necessary to construct a modified version of the PBT with succinct questions. These ingredients are as follows.

- If we play the PBT non-local game using questions drawn from an ϵ-biased set $S \subseteq \{0,1\}^n$ then a high probability of success in that game implies that approximate commutation relations on the operators in the strategy hold with respect to an average taken over S.
- By Lemma 3.6 below, approximate commutation relations with respect to averages over S imply that those same relations approximately hold on average over $\{0,1\}^n$.
- By Gowers-Hatami (for the Weyl-Heisenberg group, **??**), approximate commutation relations on average over $\{0,1\}^n$ imply that the operators are close to Paulis on an n-qubit EPR state.

Working backwards through this chain of logic, if we can design a game as described above then we will have a new PBT that works just as well as the non-succinct PBT presented in the previous sections. Moreover, since (as described in Section 2.4) there exist constructions of ϵ-biased sets of size $\mathrm{poly}(n)$ [TS17], this game has questions of size $\Theta(\log n)$. Also note that we have already covered the first and third ingredients, in Section 3.4 and Section 2.5, respectively. Hence, it remains to show the second item, which is referred to as "lifting commutation to small-bias sets" in [MNZ24]. This is the content of the following lemma.

Lemma 3.6 (similar to Corollary 3.6 in [MNZ24])**.** *Fix an $\epsilon \in (0,1)$ and let $X, Z : \mathbb{Z}_2^n \to \mathrm{L}(\mathcal{H})$ be group representations of $\mathbb{Z}_2^n$, where for each $a \in \mathbb{Z}_2^n$ it holds that $X(a)$ and $Z(a)$ are binary observables. If $S \subseteq \mathbb{Z}_2^n$ is an ϵ-biased set then*

$$\mathbb{E}_{a,b\sim\mathbb{Z}_2^n} \|Z(a)X(b) - (-1)^{a\cdot b}X(b)Z(a)\|_f^2 \leq \frac{1}{(1-\epsilon)^2}\, \mathbb{E}_{a,b\sim S} \|Z(a)X(b) - (-1)^{a\cdot b}X(b)Z(a)\|_f^2. \quad (17)$$

Proof. Let $C(a,b) = Z(a)X(b) - (-1)^{a\cdot b}X(b)Z(a)$ for all $a, b \in \mathbb{Z}_2^n$. This means that if $Z(a) = \sigma_Z(a)$ and $X(b) = \sigma_X(b)$ for some $a, b \in \mathbb{Z}_2^n$ then it holds that $C(a,b) = 0$. Thus, one should think of this operator as reflecting a deviation from the commutation relations of Pauli operators. Defining $\widetilde{W}(a) := W(a) \otimes \sigma_W(a) \in \mathrm{L}(\mathcal{H} \otimes \mathbb{C}^{\{0,1\}^n})$ for $W \in \{X, Z\}$ one may verify that $[\widetilde{Z}(a), \widetilde{X}(b)] = C(a,b) \otimes \sigma_Z(a)\sigma_X(b)$ and $\|C(a,b) \otimes \sigma_Z(a)\sigma_X(b)\|_f^2 = \|C(a,b)\|_f^2$ for all $a, b \in \mathbb{Z}_2^n$. Hence,

$$\mathbb{E}_{a,b\sim\mathbb{Z}_2^n} \|C(a,b)\|_f^2 = \mathbb{E}_{a,b\sim\mathbb{Z}_2^n} \|[\widetilde{Z}(a), \widetilde{X}(b)]\|_f^2. \quad (18)$$

Furthermore, as shown below, for $W \in \{\widetilde{X}, \widetilde{Z}\}$ and M an arbitrary binary observable we have the inequality

$$\mathbb{E}_{a\sim S} \|[M, W(a)]\|_f^2 \geq (1-\epsilon)\, \mathbb{E}_{a\sim\mathbb{Z}_2^n} \|[M, W(a)]\|_f^2. \quad (19)$$

Applying this inequality twice to the right-hand side of Eq. (18) we have

$$\mathbb{E}_{a,b\sim S} \|C(a,b)\|_f^2 \geq (1-\epsilon)^2\, \mathbb{E}_{a,b\sim\mathbb{Z}_2^n} \|C(a,b)\|_f^2 \quad (20)$$

which proves the theorem. It remains to show Eq. (19). To this end, let $d := \dim(\mathcal{H})$ and consider the "overlap" quantity $f(a) := \mathrm{Tr}(MW(a)MW(a)) \in \mathbb{R}$ for each $a \in \mathbb{Z}_2^n$. (That this quantity is always real will be apparent from the rest of the proof.) Since $W : \mathbb{Z}_2^n \to \mathrm{L}(\mathcal{H} \otimes \mathbb{C}^{\{0,1\}^n})$ is a

representation of the finite group $\mathbb{Z}_2^n$, it decomposes into a direct sum of irreducible representations as $W(a) = \oplus_\lambda \chi_\lambda(a)$ where the index in the decomposition is over bit strings $\lambda \in \mathbb{Z}_2^n$, each appearing with some multiplicity, and $\chi_\lambda(a) := (-1)^{\lambda \cdot a}$ is the character corresponding to the bit string λ. Let $M_{\lambda\mu}$ denote the matrix elements of the observable M in this basis. We then have

$$f(a) = \sum_{\lambda\mu} M_{\lambda\mu}\chi_\mu(a) M_{\mu\lambda}\chi_\lambda(a) \tag{21}$$

$$= \sum_{\lambda\mu} |M_{\lambda\mu}|^2 (-1)^{a\cdot(\lambda+\mu)}. \tag{22}$$

for all $a \in \mathbb{Z}_2^n$. Taking the expectation with respect to uniformly random $a \in \mathbb{Z}_2^n$ we have

$$\mathbb{E}_{a\sim\mathbb{Z}_2^n} f(a) = \sum_{\lambda=\mu} |M_{\lambda\mu}|^2 =: \kappa \tag{23}$$

where we split the sum in Eq. (22) into terms where $\lambda = \mu$ and terms where $\lambda \neq \mu$ and made use of the fact that $\mathbb{E}_{a\in\mathbb{Z}_2^n}(-1)^{a\cdot y} = 0$ for any nonzero y. On the other hand,

$$\mathbb{E}_{a\sim S} f(a) = \kappa + \sum_{\lambda\neq\mu} |M_{\lambda\mu}|^2 \, \mathbb{E}_{a\sim S}(-1)^{a\cdot(\lambda+\mu)} \tag{24}$$

$$\leq \kappa + \epsilon \sum_{\lambda\neq\mu} |M_{\lambda\mu}|^2 \tag{25}$$

$$= \kappa + \epsilon \left(d - \sum_{\lambda=\mu} |M_{\lambda\mu}|^2 \right) \tag{26}$$

$$= \kappa + \epsilon(d - \kappa) \tag{27}$$

Therefore

$$\mathbb{E}_{a\sim S} \|[M, W(a)]\|_f^2 - \mathbb{E}_{a\sim\mathbb{Z}_2^n} \|[M, W(a)]\|_f^2 = \frac{2}{d} \left(\mathbb{E}_{a\sim\mathbb{Z}_2^n} f(a) - \mathbb{E}_{a\sim S} f(a) \right) \tag{28}$$

$$\geq -\epsilon \left(2 - \frac{2\kappa}{d} \right) \tag{29}$$

$$= -\epsilon \, \mathbb{E}_{a\sim\mathbb{Z}_2^n} \|[M, W(a)]\|_f^2 \tag{30}$$

where the second line makes use of Eqs. (23) and (24), while the final line follows from expanding the expectation and noting that M and $W(a)$ are binary observables for any $a \in \mathbb{Z}_2^n$ and therefore have unit normalized Frobenius norm. Finally, Eq. (19) follows upon rearranging the above inequality. □

Acknowledgements

We thank the teaching staff for an enjoyable class and valuable feedback on this final project. We also thank Tony Metger for useful discussions.

References

[BA04] J. S. Bell and Alain Aspect. *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy*. 2nd ed. Cambridge University Press, 2004.

[BLR93] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. "Self-testing/correcting with applications to numerical problems". In: *Journal of Computer and System Sciences* 47.3 (1993), pp. 549–595. ISSN: 0022-0000. DOI: https://doi.org/10.1016/0022-0000(93)90044-W. URL: https://www.sciencedirect.com/science/article/pii/002200009390044W.

[Bru+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. "Bell nonlocality". In: *Rev. Mod. Phys.* 86 (2 2014), pp. 419–478. DOI: 10.1103/RevModPhys.86.419. URL: https://link.aps.org/doi/10.1103/RevModPhys.86.419.

[Gri20] Alex B. Grilo. *A simple protocol for verifiable delegation of quantum computation in one round*. 2020. arXiv: 1711.09585 [quant-ph].

[Ji+22] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. *MIP*=RE*. 2022. arXiv: 2001.04383 [quant-ph].

[MNZ24] Tony Metger, Anand Natarajan, and Tina Zhang. *Succinct arguments for QMA from standard assumptions via compiled nonlocal games*. 2024. arXiv: 2404.19754 [quant-ph].

[NN24] Anand Natarajan and Chinmay Nirkhe. *The status of the quantum PCP conjecture (games version)*. 2024. arXiv: 2403.13084 [quant-ph].

[NV17] Anand Natarajan and Thomas Vidick. "A quantum linearity test for robustly verifying entanglement". In: *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*. STOC '17. ACM, June 2017. DOI: 10.1145/3055399.3055468. URL: http://dx.doi.org/10.1145/3055399.3055468.

[Pau+16] Vern I. Paulsen, Simone Severini, Daniel Stahlke, Ivan G. Todorov, and Andreas Winter. "Estimating quantum chromatic numbers". In: *Journal of Functional Analysis* 270.6 (2016), pp. 2188–2222. ISSN: 0022-1236. DOI: https://doi.org/10.1016/j.jfa.2016.01.010. URL: https://www.sciencedirect.com/science/article/pii/S0022123616000203.

[Sal22] Mikael de la Salle. *Spectral gap and stability for groups and non-local games*. 2022. arXiv: 2204.07084 [math.OA].

[TS17] Amnon Ta-Shma. "Explicit, almost optimal, epsilon-balanced codes". In: *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*. 2017, pp. 238–251.

[VV14] Umesh Vazirani and Thomas Vidick. "Fully Device-Independent Quantum Key Distribution". In: *Phys. Rev. Lett.* 113 (14 2014), p. 140501. DOI: 10.1103/PhysRevLett.113.140501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.113.140501.

[Vid] Thomas Vidick. *Simplified analysis on robust test for EPR pairs*. URL: http://users.cms.caltech.edu/~vidick/notes/pauli_braiding_1.pdf.

[Vid22] Thomas Vidick. "Almost synchronous quantum correlations". In: *Journal of Mathematical Physics* 63.2 (Feb. 2022), p. 022201. ISSN: 0022-2488. DOI: 10.1063/5.0056512. eprint: https://pubs.aip.org/aip/jmp/article-pdf/doi/10.1063/5.0056512/19799256/022201_1_online.pdf. URL: https://doi.org/10.1063/5.0056512.

[Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018. DOI: 10.1017/9781316848142.

[Wu+16] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. "Device-independent parallel self-testing of two singlets". In: *Physical Review A* 93.6 (2016), p. 062121.