Qubit tests from classical codes

Thomas Vidick and Henry Yuen

January 17, 2025

WARNING: NOTES ON[1]

Abstract

We introduce a notion of *quantum presentation* for a classical linear error-correcting code over $\mathbb{F}_q$ that informally allows each character of the code to be replaced by a unitary of order q. We further introduce a notion of *quantum soundness* for the code that parallels the notion of local testability for linear codes.

The notions we introduce are motivated by the use of error-correcting codes to design efficient tests, in the form of non-local games, that single out high-dimensional quantum strategies. Such a test plays an important role in the recent proof of $\mathsf{MIP}^* = \mathsf{RE}$ [JNV+20a].

We suggest a general approach to designing such tests by combining a quantum sound linear code with commutation and anti-commutation tests. This approach is inspired from a similar approach introduced in [NV16], developed in [JNV+20a] and recently generalized in [dlS22]. As an application we recover a streamlined and simplified proof of the quantum low-degree test used in [JNV+20a], assuming the quantum soundness of the classical low-degree test shown in [JNV+22]

1 Introduction

(Thomas: Make the connection with LCS)

2 Preliminaries

2.1 Notation

When we write $\mathbb{E}_{i\in\mathcal{X}}$ where $\mathcal{X}$ is a finite set, we mean the expectation over i chosen uniformly at random from $\mathcal{X}$, i.e. $\frac{1}{|\mathcal{X}|}\sum_{i\in\mathcal{X}}$. For a vector $u \in \mathcal{X}^n$ and a subset $S \subseteq [n]$, we write u_S to denote the vector in $\mathcal{X}^S$ which is the restriction of u to S.

2.2 Algebra

A *tracial von Neumann algebra* is a pair $(\mathcal{M}, \tau)$ of a von Neumann algebra $\mathcal{M}$ together with a normal faithful tracial state τ on $\mathcal{M}$, which we often refer to as the *trace*. The main example of interest is $\mathcal{M} = M_n(\mathbb{C})$, the algebra $n \times n$ complex matrices, with τ the dimension-normalized trace, which we denote $\mathrm{tr}(M) = \frac{1}{n}\mathrm{Tr}(M)$. We write $\|x\|_2 = \tau(x^*x)^{1/2}$ for the 2-norm on $\mathcal{M}$.

Let $B(\ell_2)$ be the von Neumann algebra of bounded operators on ℓ_2, the Hilbert space of convergent sequences in $\mathbb{C}^{\mathbb{Z}}$ equipped with the usual Euclidean norm (for which we let $(e_i)_{i\in\mathbb{Z}}$ denote the standard basis). We denote $\mathcal{M}_\infty = \mathcal{M}\overline{\otimes}B(\ell_2)$, where the overline denotes closure for the operator topology. $\mathcal{M}_\infty$ is a von Neumann algebra equipped with the (infinite) trace $\tau_\infty = \tau \otimes \mathrm{Tr}$, with $\mathrm{Tr}(x) = \sum_{i\in\mathbb{Z}} e_i^T X e_i$ the trace on $B(\ell_2)$. We generally identify $\mathcal{M}$ with the "corner" $\mathcal{M} \otimes e_{1,1} \subset \mathcal{M}_\infty$.

We let $\mathbb{F}$ denote a finite field, and $\mathbb{F}_2$ the field with two elements. For $u \in \mathbb{F}^n$ for some n, we write $|u|$ for the Hamming weight of u, i.e. the number of nonzero coordinates. For $a, b \in \mathbb{F}^k$, we write $a \cdot b$ to denote the inner product $\sum_{i=1}^k a_i b_i$.

2.3 Measurements

A POVM in $\mathcal{M}$ with outcome set $\mathcal{A}$ is a finite collection of positive semidefinite operators $\{P_a\}_{a\in\mathcal{A}}$ such that $\sum_a P_a = I_{\mathcal{M}}$. A POVM is *projective* if for all a, P_a is a projection. Given a projective measurement $\{P_a\}_{a\in\mathbb{F}_2^k}$ and $b \in \mathbb{F}_2^k$ we define the corresponding *observable*

$$\widehat{P}(b) = \sum_a (-1)^{a\cdot b} P_a \;,$$

which is self-adjoint and unitary. If $k = 1$, we often use the shorthand $\widehat{P}$ for $\widehat{P}(1) = P_0 - P_1$.

We define a specific family of projective measurements on $M_{2^k}(\mathbb{C})$ which are derived from the *Pauli observables*. Define

$$\sigma^X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \;, \qquad \sigma^Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \;,$$

and more generally for $a, b \in \mathbb{F}_2^k$ let $\sigma^X(a) = \bigotimes_{i=1}^t (\sigma^X)^{a_i}$ and $\sigma^Z(b) = \bigotimes_{i=1}^t (\sigma^Z)^{b_i}$, which are observables in $M_{2^k}(\mathbb{C})$. These are self-adjoint unitary operators called Pauli observables. Each observable $\sigma^X(a)$ (resp. $\sigma^Z(b)$) corresponds to the *Pauli measurement* $\{\sigma_a^X\}_{a\in\mathbb{F}_2^k}$ (resp. $\{\sigma_b^Z\}_{b\in\mathbb{F}_2^k}$) where (in a slight abuse of notation)

$$\sigma_a^X = \mathop{\mathbb{E}}_{\alpha\in\mathbb{F}_2^k} (-1)^{a\cdot\alpha}\sigma^X(\alpha) \qquad \text{and} \qquad \sigma_b^Z = \mathop{\mathbb{E}}_{\beta\in\mathbb{F}_2^k} (-1)^{b\cdot\beta}\sigma^Z(\beta).$$

It is easy to verify that $\{\sigma_a^X\}_a$ and $\{\sigma_b^Z\}_b$ are projections summing to identity.

2.4 Nonlocal games

We give standard definitions on nonlocal games.

Definition 2.1 (Game)**.** A game is a tuple $(\mathcal{X}, \mu, \mathcal{A}, D)$ where $\mathcal{X}$ is a finite set, μ a distribution on $\mathcal{X} \times \mathcal{X}$, $\mathcal{A} = (\mathcal{A}(x))_{x\in\mathcal{X}}$ a collection of finite sets, and

$$D : \big\{(x, y, a, b) : (x, y) \in \mathrm{supp}(\mu), a \in \mathcal{A}(x), b \in \mathcal{A}(y)\big\} \;\to\; \{0, 1\}$$

such that D is symmetric, i.e. $D(x, y, a, b) = D(y, x, b, a)$ whenever both terms are defined. We often abuse notation and write μ for the symmetrized marginal of μ, i.e.

$$\mu(x) := \sum_{x'\in\mathcal{X}} \frac{1}{2}\big(\mu(x, x') + \mu(x', x')\big) \;.$$

The interpretation of $G = (\mathcal{X}, \mu, \mathcal{A}, D)$ as a nonlocal game is the following. In the "game", a referee is imagined to sample a pair of "questions" $(x, y) \sim \mu$. The question x is sent to a first player, "Alice," and the question y is sent to a second player, "Bob." Each player is tasked with responding with an answer $a \in \mathcal{A}(x)$ for Alice, and $b \in \mathcal{A}(y)$ for Bob. The referee accepts the players' answers if and only if $D(x, y, a, b) = 1$.

Nonlocal games provide a framework to study different kinds of bipartite correlations: depending on the level of coordination allowed between Alice and Bob, they may have varying chances of success in the game.

In quantum mechanics, a local strategy for the players (meaning that each player is required to determine their answer locally, without exchanging information with the other player) is specified by the following.

Definition 2.2 (Synchronous strategy)**.** If $G = (\mathcal{X}, \mu, \mathcal{A}, D)$ is a game and $(\mathcal{M}, \tau)$ a tracial von Neumann algebra, a *synchronous strategy* $\mathscr{S}$ *for* G *on* $(\mathcal{M}, \tau)$ is, for every $x \in \mathcal{X}$, a projective measurement $(P^x_a)_{a \in \mathcal{A}(x)}$ on $\mathcal{M}$. The value of a strategy $\mathscr{S}$ in G is

$$\omega(G; \mathscr{S}) = \sum_{(x,y) \in \mathcal{X} \times \mathcal{X}} \frac{1}{2}\big(\mu(x,y) + \mu(y,x)\big) \sum_{(a,b) \in \mathcal{A}(x) \times \mathcal{A}(y)} D(x,y,a,b)\, \tau\big(P^x_a\, P^y_b\big)\,.$$[1]

We say that $\mathscr{S}$ is *perfect* if $\omega(G; \mathscr{S}) = 1$.

The name *synchronous* stems from the fact that whenever an identical pair (x, x) is chosen, $\tau(P^x_a P^x_b) = 0$ for $a \neq b$ due to the requirement that $\{P^x_a\}_a$ is a projective measurement. Thus a synchronous strategy always returns the same answer to the same question. More general strategies, which allow different operators $\{P^x_a\}$ and $\{Q^y_b\}$, do not automatically enforce the synchronicity condition, but we do not consider such strategies here.

3 Quantum soundness of linear codes

(Thomas: added wrapper text throughout this section**)** In this section we introduce a notion of "quantum soundness" for a linear error-correcting code. We start with classical definitions around codes, then define quantum soundness and finally we provide an example.

3.1 Classical definitions

Definition 3.1 (Linear code)**.** For q a prime power and n, k, d integer a $[n, k, d]_q$ linear code is a k-dimensional subspace $\mathcal{C} \subseteq \mathbb{F}_q^n$ such that for every $u \in \mathcal{C}$ such that $u \neq 0$, $|u| \geq d$. Equivalently, we think of $\mathcal{C}$ as a linear map $\mathcal{C} : \mathbb{F}_q^k \to \mathbb{F}_q^n$. We write $E_{\mathcal{C}} \in \mathbb{F}_q^{k \times n}$ for the generator matrix defined by $E_{\mathcal{C}}^T e_i = \mathcal{C}(e_i)$ for all $i \in \{1, \dots, k\}$, where $\{e_1, \dots, e_k\}$ is the standard basis of $\mathbb{F}_q^k$.

When the subscript q is omitted, it is implicitly taken as $q = 2$, i.e. the code is assumed to be binary.

Some codes have the useful property that they can be *locally tested*. Informally, this means that it is possible to distinguish codewords from strings that are far from the code by examining only a randomly chosen constant-size subset of coordinates. We give one possible way to formalize this; for more on the topic see e.g. the book chapter by Goldreich [Gol17].

Definition 3.2 (Local tester)**.** Let $\mathcal{C}$ be an $[n, k, d]_q$ linear code, $\delta : [0, 1] \to [0, 1]$, and $r \in \mathbb{N}$. An *r-local δ-tester for* $\mathcal{C}$ is a pair $M = ((M_S)_{S \subseteq [n]}, \nu)$ where ν is a distribution over subsets $S \subseteq [n]$ of size at most r, and for each such subset $M_S : \mathbb{F}_q^S \to \{0, 1\}$ is a predicate such that the following hold:

- (Completeness:) For any $u \in \mathcal{C}$, $\Pr_{S \sim \nu}(M_S(u_S) = 1) = 1$.
- (Soundness:) For any $\varepsilon \geq 0$ and any $u \in \mathbb{F}_q^n$ that is within (Hamming) distance at least ε from $\mathcal{C}$, $\Pr_{S \sim \nu}(M_S(u_{|S}) = 0) \geq \delta(\varepsilon)$.

[1] Note the symmetrization of μ. This is to avoid explicitly requiring μ to be permutation-invariant in the definition of a game.

3.2 Quantum soundness

We now introduce our notion of quantum soundness. Informally, a code is quantum sound with respect to a specific tester for it if whenever a family of measurements locally satisfies the constraints imposed by the tester, then it globally returns a codeword.

To be more precise, we first introduce the notion of *code presentation*, which is the "global object" that we aim to test for.

Definition 3.3 (Code presentation)**.** Let $\mathcal{C}$ be an $[n,k,d]$ linear code. A *presentation* of $\mathcal{C}$ is a pair $(\mathcal{M}, A)$ of a tracial von Neumann algebra $\mathcal{M}$ and a collection of projective measurements $A = \{A^i_a\}_{a\in\mathbb{F}_q} \subseteq \mathcal{M}$ for $i \in \{1,\dots,n\}$ such that the $\{A^i_a\}$ pairwise commute and $\sum_{c\in\mathcal{C}} \prod_{i=1}^n A^i_{c_i} = I$.[2]

Since the $\{A^i\}$ that form a code presentation mutually commute, as quantum mechanical measurements they can be performed sequentially in any order; this will lead to the same distribution on outcomes $u = (u_1,\dots,u_n)$. The last condition in the definition implies that for any outcome u that has nonzero probability, $u \in \mathcal{C}$. In finite dimension D, a code presentation is equivalently specified by an orthonormal basis $\{f_1,\dots,f_D\}$ and an assignment of a codeword $u_j \in \mathcal{C}$ to each f_j. We then let $A^i_a = \sum_{j:\,(u_j)_i=a} f_j f_j^*$.

To define the "local object" that the code tester will effectively test for, we first introduce a notion of distance on measurements. At first read it may be helpful to consider the case $\mathcal{M} = \mathcal{N}$ and $w = P = 1_{\mathcal{M}}$, in which case it simplifies significantly. **(Thomas:** moved the defn here; since it's quite important for the paper I prefer that it's not dumped in the preliminaries**)**

Definition 3.4 (Closeness)**.** Let $\{A^i_a\} \subseteq \mathcal{M}$ and $\{B^i_a\} \subseteq \mathcal{N}$ be two families of projective measurements on tracial algebras $(\mathcal{M}, \tau^{\mathcal{M}})$ and $(\mathcal{N}, \tau^{\mathcal{N}})$ respectively, indexed by the same set $i \in \mathcal{I}$ and with the same set of outcomes $a, b \in \mathcal{A}$. For $\delta \geq 0$ and μ a measure on $\mathcal{I}$ we say that $\{A^i\}$ and $\{B^i\}$ are (δ,μ)-close if there exists a projection $P \in \mathcal{M}_\infty$ of finite trace such that $\mathcal{N} = P\mathcal{M}_\infty P$ and $\tau^{\mathcal{N}} = \tau_\infty/\tau_\infty(P)$, and a partial isometry $w \in P\mathcal{M}_\infty I_{\mathcal{M}}$ such that

$$\mathop{\mathbb{E}}_{i\sim\mu} \sum_{a\in\mathcal{A}} \left\| A^i_a - w^* B^i_a w \right\|_2^2 \leq \delta$$

and

$$\max\left\{\tau^{\mathcal{M}}(I_{\mathcal{M}} - w^*w)\,,\ \tau^{\mathcal{N}}(P - ww^*)\right\} \leq \delta\,.$$

If the measure μ is omitted then it is understood to be the uniform measure on $\mathcal{I}$.

We now define the "local object." This local object depends on a local tester M for the code $\mathcal{C}$. Informally, a *local presentation* of a code $\mathcal{C}$ (with respect to M) specifies a family of measurements $\{A^i\}$, just like the global presentation, except that these measurements are not required to commute globally. Instead, it is only required that for every "local" set $S \subseteq \{1,\dots,n\}$ of size $|S| \leq r$ the $\{A^i\}$ for $i \in S$ are close, according to the preceding definition, to a family of commuting measurements $\{B^i\}$ for $i \in S$ such that furthermore measuring all B_i lead to an outcome $a \in \mathbb{F}_2^S$ that would be accepted by the local tester M, i.e. $M(S,a) = 1$.

Definition 3.5 (ε-local presentation)**.** Let $\mathcal{C}$ be an $[n,k,d]_q$ linear code and M be an r-local tester for $\mathcal{C}$. An *ε-local presentation of* $(\mathcal{C}, M)$ is a pair $((\mathcal{M},\tau), A)$ of a tracial von Neumann algebra $(\mathcal{M},\tau)$ and a collection of projective measurements $A = \{A^i_a\}_{a\in\mathbb{F}_q} \subseteq \mathcal{M}$ for $i \in \{1,\dots,n\}$ such that for any $S \subseteq \{1,\dots,n\}$ of size $|S| \leq r$ there are $|S|$ pairwise commuting projective measurements $\{B^{S,i}\}_{i\in S} \subset \mathcal{M}_\infty$, with $B^{S,i} = \{B^{S,i}_b\}_{b\in\mathbb{F}_q}$, such that

[2] This implies that whenever $u \notin \mathcal{C}$, $\prod_i A^i_{u_i} = 0$.

- $\sum_{a\in\mathbb{F}^S} M(S,a)\prod_{i\in S} B^{S,i}_{a_i} = I$
- For any S such that $|S| \leq r$ and $i \in S$, let $A^{S,i} = S^i$. Then the two measurement families $\{A^{S,i}\}_{S,i\in S}$ and $\{B^{S,i}\}_{S,i\in S}$ are (ε,ν')-close, where $\nu'((S,i)) = \nu(S)1_{i\in S}\frac{1}{|S|}$.

(Henry: question about the name: why "presentation"? the object here is a pair $(\mathcal{M}, A)$ which looks syntactically the same as a code representation... should it be "representation"?**)** **(Thomas:** Yeah...should we use "presentation" for both? This avoids confusion with language from representation theory. I did this above, what do you think?**)** **(Henry:** I actually like the term representation for its allusion to representation theory. But we should be consistent with both; you pick.**)**

Now we define *quantum soundness*, which requires any "local object" to be close to a "global object."

Definition 3.6 (Quantum soundness)**.** Let $\mathcal{C}$ be an $[n,k,d]_q$ linear code and M a r-local tester for $\mathcal{C}$. Let $\delta : [0,1] \to [0,1]$ be such that $\delta(0) = 0$. We say that $(\mathcal{C}, M)$ has *quantum soundness* $\delta(\varepsilon)$ if the following holds. For any ε-local presentation $(\mathcal{M}, A)$ of $(\mathcal{C}, M)$ there is a presentation $(\mathcal{N}, B)$ of $\mathcal{C}$ such that the measurement families A and B are $\delta(\varepsilon)$-close.

Remark 3.7. *Definition 3.6 can be reformulated in the language of nonlocal games, see Proposition 4.3.*

Remark 3.8. *A necessary condition for a code to be quantum sound is that any* 0*-local quantum presentation* $((\mathcal{M},\tau), A)$ *is a presentation of* $\mathcal{C}$*. Not all codes satisfy this condition, see e.g. [PRSS22, Example 2.16]. If* $(\mathcal{C}, M)$ *satisfies this condition, then we say that it is* Abelian*. Thus, Abelian codes have, by definition, quantum soundness* $\overline{\delta}$ *where* $\overline{\delta}(0) = 0$ *and* $\overline{\delta}(x) = 1$ *for* $x \in (0,1]$.

3.3 Example: the Hadamard code

We give an example of quantum sound code, the *Hadamard code*. This code can be defined for any $t \geq 1$ and it is an $[T, t, T/2]_2$ linear code, where $T = 2^t$. For simplicity we write $\mathcal{C}_{\mathrm{HAD}}$ to denote this code, omitting t. As a linear map, for $i \in \{1,\ldots,t\}$, $\mathcal{C}_{\mathrm{HAD}}(e_i) = (x_i)_{x\in\mathbb{F}_2^t} \in \mathbb{F}_2^T$, where we identify the index set $\{1,\ldots,T\}$ with the set $\mathbb{F}_2^t$ in an arbitrary way.

It is shown in [BLR90] that there is a 3-local δ-tester M_{HAD} for $\mathcal{C}_{\mathrm{HAD}}$, where $\delta(\varepsilon) = 6\varepsilon$. The distribution ν_{HAD} is uniform over subsets $\{x, y, x+y\} \subset \mathbb{F}_2^t$ where $x, y \in \mathbb{F}_2^t$ are uniformly and independently chosen. For all $u \in \mathbb{F}_2^T$, the predicate $M_{\mathrm{HAD},S}(u|_S) = 1$ if and only if $u_x + u_y = u_{x+y}$ (where we think of the coordinates of u as being indexed by elements of $\mathbb{F}_2^t$).

In [NV16] show that the Hadamard code is quantum sound. They show this using the language of nonlocal games, but it is straightforward to adapt the argument to the definitions introduced here**(Thomas:** should we do it "for completeness"?**)** .[3]

Theorem 3.9 (Theorem 10 in [NV16])**.** *There is a universal constant* $c > 0$ *such that for any* $t \geq 1$*, the pair* $(\mathcal{C}_{\mathrm{HAD}}, M_{\mathrm{HAD}})$ *has quantum soundness* $\delta(\varepsilon) = c\,\varepsilon$.

4 A formulation of quantum soundness in terms of nonlocal games

In this section we give an equivalent (up to a mild slack in parameters) definition of quantum soundness of a linear code in terms of *robustness* of a nonlocal game associated with the code. This formulation will be important for the statement of our main result.

[3] While [NV16] only show the result for finite-dimensional $\mathcal{M}$, the same proof works for any tracial von Neumann algebra $(\mathcal{M}, \tau)$.

4.1 The code game

Informally, the game $G_{\mathcal{C},M}$ associated to a code $\mathcal{C}$ and a local tester M for $\mathcal{C}$ is the "oracularized" version of the test executed by M. That is, one player in the game is asked to provide an assignment to all variables in the set S queried by the tester, that will satisfy its test, while the other player is asked to provide an assignment to a single $i \in S$ and checked for consistency—this will ensure that the first players' answers are consistent across different sets S. The formal definition follows.

Definition 4.1. Let $\mathcal{C}$ be an $[n,k,d]_q$ linear code and M an r-local tester for $\mathcal{C}$. The game $G_{\mathcal{C},M}$ is defined as follows. We set

$$\mathcal{X} = \{S \subseteq \{1,\dots,n\}, |S| \leq r\} \sqcup \{1,\dots,n\} \quad \text{and} \quad \mu(S,i) = \frac{1_{i\in S}}{|S|}\nu(S) ,$$

and for any $S, i \in \mathcal{X}$, $\mathcal{A}(S) = \mathbb{F}_q^S$ and $\mathcal{A}(i) = \mathbb{F}_q$, and finally $D(S,i,a,b) = M(S,a)1_{a_i=b}$.

To state the sense in which this nonlocal game is equivalent to quantum soundness of $\mathcal{C}$ we need to introduce a notion of *robustness* of a nonlocal game. This definition is standard in the literature on self-testing**(Thomas:** is it; give a ref?) .

Definition 4.2 (Robust game)**.** Given a game G, a function $\delta : [0,1] \to [0,1]$, and a distribution ν on $\mathcal{X}$ we say that G is (δ,ν)-*robust* if any synchronous strategy for G that succeeds with probability at least $1-\varepsilon$ in G, for some $\varepsilon \geq 0$, is $(\delta(\varepsilon),\nu)$-close to a perfect strategy.

Note that in the definition ν need not be the marginal of the game distribution μ. In particular, we will often consider ν that is supported on a strict subset of the support of μ.

We now state the main result of the section.

Proposition 4.3. *Let $\mathcal{C}$ be an $[n,k,d]_q$ linear code and M an r-local tester for $\mathcal{C}$ with distribution ν. Let $\delta,\delta' : [0,1] \to [0,1]$. Then the following hold:*

1. *If $G_{\mathcal{C},M}$ is (δ',ν)-robust for ν the uniform distribution on $\{1,\dots,n\} \subseteq \mathcal{X}$, and $(\mathcal{C},M)$ is Abelian, then M has quantum soundness δ'', for some $\delta''(\varepsilon) = O(\delta'(\sqrt{\varepsilon}))$.*
2. *If M has quantum soundness δ then $G_{\mathcal{C},M}$ is (δ'',ν)-robust, for some $\delta''(\varepsilon) = O(\delta(2\varepsilon))$ and ν the uniform distribution on $\{1,\dots,n\} \subseteq \mathcal{X}$.*

We prove the proposition in Section 4.3. Before doing so, we introduce some simple tools.

4.2 Preliminary lemmas

We give some lemma that will be used in the proof of Proposition 4.3. The lemma are well-known; we include proofs for the specific statements that we use.

In Definition 3.4 closeness is measured in the L_2 sense. The first lemma gives a consequence for distance measured in an L_1 sense.

Lemma 4.4. *Let $\{P_a^i\}$ and $\{Q_a^i\}$ be two families of projective measurements that are (ε,μ)-close. Then*

$$\mathop{\mathbb{E}}_{i\in\mathcal{I}} \sum_{a\in\mathcal{A}(i)} \tau\big(|P_a - w^*Q_a w|\big) \leq \varepsilon + 2\sqrt{\varepsilon}\,. \tag{1}$$

Proof. Using the triangle inequality,

$$\begin{aligned}\mathop{\mathbb{E}}_i \sum_a \tau\big(|P^i_a - w^* Q^i_a w|\big) \leq \mathop{\mathbb{E}}_i \sum_a \Big(&\tau\big(|(P^i_a - (P^i_a)^2)|\big) + \tau\big(|P_a(P^i_a - w^* Q^i_a w)|\big) \\ &+ \tau\big(|(P^i_a - w^* Q^i_a w) w^* Q^i_a w|\big) \\ &+ \tau\big(|(w^* Q^i_a w^* w Q^i_a w - w^* Q^i_a w)|\big)\Big) \,. \end{aligned} \tag{2}$$

The first term on the right-hand side is zero, because P^i is assumed projective. The terms in the middle are bounded using Hölder's inequality:

$$\begin{aligned}\mathop{\mathbb{E}}_i \sum_a \tau\big(|P^i_a(P^i_a - w^* Q^i_a w)|\big) &\leq \mathop{\mathbb{E}}_i \sum_a \|P^i_a\|_2 \; \|P^i_a - w^* Q^i_a w\|_2 \\ &\leq \Big(\mathop{\mathbb{E}}_i \sum_a \|P^i_a\|_2^2\Big)^{1/2} \Big(\mathop{\mathbb{E}}_i \sum_a \|P^i_a - w^* Q^i_a w\|_2^2\Big)^{1/2} \\ &\leq \sqrt{\varepsilon}\end{aligned}$$

by closeness. The second term of (2) is bounded in a similar fashion. Finally the last term of (2) can be bounded as

$$\begin{aligned}\mathop{\mathbb{E}}_i \sum_a \tau\big(|w^* Q^i_a w^* w Q^i_a w - w^* Q^i_a w|\big) &= \mathop{\mathbb{E}}_i \sum_a \tau\big((w^* Q^i_a (I - w^* w) Q^i_a w)\big) \\ &= \tau\Big((I - w^* w)\Big(\mathop{\mathbb{E}}_i \sum_a Q^i_a w w^* Q^i_a\Big)\Big) \\ &\leq \tau(I - w^* w) \, \Big\|\mathop{\mathbb{E}}_i \sum_a Q^i_a w w^* Q^i_a\Big\| \\ &\leq \varepsilon \,.\end{aligned}$$

□

The next lemma shows that two strategies for the same game G that are close according to Definition 3.4 have a close value.

Lemma 4.5. *Let $G = (\mathcal{X}, \mu, \mathcal{A}, D)$ be a game and $\mathscr{S} = \{P^x_a\}$ and $\mathscr{S}' = \{Q^x_a\}$ strategies on $\mathcal{M}$ and $\mathcal{N}$ respectively such that $\{P^x_a\}$ and $\{Q^x_a\}$ are (ε, μ)-close. Then*

$$\big|\omega(G; \mathscr{S}) - \omega(G; \mathscr{S}')\big| \leq 8\sqrt{\varepsilon} \,.$$

Proof. By definition, there exists a projection $P \in \mathcal{M}_\infty$ and a partial isometry $w \in P\mathcal{M}_\infty I_{\mathcal{M}}$ such that $\mathcal{N} = P\mathcal{M}_\infty P$ and

$$\begin{aligned}\omega(G; \mathscr{S}') &= \mathop{\mathbb{E}}_{(x,y)\sim\mu} \sum_{a,b} D(a,b,x,y)\tau\big(Q^x_a Q^y_b\big) \\ &= \mathop{\mathbb{E}}_{(x,y)\sim\mu} \sum_{a,b} D(a,b,x,y)\tau\big(w^* Q^x_a w \, w^* Q^y_b w\big) \\ &\quad + \mathop{\mathbb{E}}_{(x,y)\sim\mu} \sum_{a,b} D(a,b,x,y)\tau\big(w^* Q^x_a (P - w\, w^*) Q^y_b w\big) \\ &\quad + \mathop{\mathbb{E}}_{(x,y)\sim\mu} \sum_{a,b} D(a,b,x,y)\tau\big(Q^x_a Q^y_b (P - w w^*)\big) \,.\end{aligned}$$

Here we used the fact that $Q_a^x \in \mathcal{N}$ so $PQ_a^xP = Q_a^x$ for all x, a. The second and third term on the right-hand side can be bounded as

$$
\begin{aligned}
\Big| \mathop{\mathbb{E}}_{(x,y)\sim\mu} \sum_{a,b} D(a,b,x,y)\tau\big(w^* Q_a^x (P - w\,w^*) Q_b^y w\big) \Big| & \\
&\leq \mathop{\mathbb{E}}_{(x,y)\sim\mu} \Big| \tau\big(\sum_{a,b} D(a,b,x,y) Q_b^y w w^* Q_a^x (P - w\,w^*)\big) \Big| \\
&\leq \sqrt{\tau((P - ww^*)^2)} \cdot \sqrt{\mathop{\mathbb{E}}_{(x,y)\sim\mu} \tau\big(\big|\sum_{a,b} D(a,b,x,y) Q_a^x w w^* Q_b^y \big|^2\big)} \\
&\leq \sqrt{\varepsilon} \sqrt{\mathop{\mathbb{E}}_{(x,y)\sim\mu} \tau\big(\sum_{a,b} D(a,b,x,y) Q_b^y w w^* Q_a^x w w^* Q_b^y\big)} \\
&\leq \sqrt{\varepsilon} \sqrt{\mathop{\mathbb{E}}_{(x,y)\sim\mu} \sum_{a,b} \tau\big(Q_b^y w w^* Q_a^x w w^* Q_b^y\big)} \\
&= \sqrt{\varepsilon} \sqrt{\mathop{\mathbb{E}}_{(x,y)\sim\mu} \sum_{b} \tau\big(Q_b^y w w^*\big)} \\
&\leq \sqrt{\varepsilon}\,.
\end{aligned}
$$

The third line is due to Cauchy-Schwarz and Jensen's inequality, where $|A|^2 = A^*A$. The fourth line uses that $P - ww^*$ is a positive operator with operator norm at most 1 for the first term, and that for fixed x, y, the measurements $\{Q_a^x\}_a$ and $\{Q_b^y\}_b$ are projective. The fifth line is due to $D(x, y, a, b) \in \{0, 1\}$. The sixth line is due to $\sum_a Q_a^x = I_{\mathcal{N}}$. The seventh line is due to $\sum_a Q_b^y = I_{\mathcal{N}}$.

For $x \in \mathcal{X}$ such that $\mu(x) \neq 0$, denote by μ_x the (symmetrized) conditional distribution $\mu_x(y) = \frac{1}{2}(\mu(x, y) + \mu(y, x))/\mu(x)$. Then using the above

$$
\begin{aligned}
\big|\omega(G;\mathscr{S}) - \omega(G;\mathscr{S}')\big| &\leq 2\sqrt{\varepsilon} + \Big| \mathop{\mathbb{E}}_{(x,y)\sim\mu} \sum_{a,b} D(a,b,x,y)\big(\tau\big(P_a^x\, P_b^y\big) - \tau\big(w^* Q_a^x w\, w^* Q_b^y w\big)\big) \Big| \\
&\leq 2\sqrt{\varepsilon} + \Big| \mathop{\mathbb{E}}_{x\sim\mu} \sum_a \tau\Big(\big(P_a^x - w^* Q_a^x w\big) \Big(\mathop{\mathbb{E}}_{y\sim\mu_x} \sum_b D(a,b,x,y) P_b^y \Big)\Big) \Big| \\
&\qquad + \Big| \mathop{\mathbb{E}}_{y\sim\mu} \sum_b \tau\Big(\Big(\mathop{\mathbb{E}}_{x\sim\mu_y} \sum_a D(a,b,x,y) w^* Q_a^x w \Big) \big(P_b^y - w^* Q_b^y w\big) \Big) \Big| \\
&\leq 2\sqrt{\varepsilon} + 2 \mathop{\mathbb{E}}_{x\sim\mu} \sum_a \tau\big(\big|P_a^x - w^* Q_a^x w\big| \big) \\
&\leq 2\sqrt{\varepsilon} + 2(\varepsilon + 2\sqrt{\varepsilon}) \leq 8\sqrt{\varepsilon}\,,
\end{aligned}
$$

where the third line uses $\tau(AB) \leq \tau(|A|)\|B\|$ and the last line is by (1). □

Our final lemma is an application of *orthonormalization*, which transforms a nearly-orthogonal measurement to a nearby orthogonal measurement. See e.g. [KV11, JNV+20b] or [dlS21, Theorem 1.2] for the version that we use here.

Lemma 4.6. *Let $(\mathcal{M}, \tau^{\mathcal{M}})$ be a tracial von Neumann algebra, $P \in \mathcal{M}_\infty$ a projection of finite trace, $\mathcal{N} = P\mathcal{M}_\infty P$ and $\tau^{\mathcal{N}} = \tau_\infty/\tau_\infty(P)$, and $w \in P\mathcal{M}_\infty I_{\mathcal{M}}$ a partial isometry. Let*

$$
\varepsilon = \max\left\{\tau^{\mathcal{M}}\big(I_{\mathcal{M}} - w^*w\big)\,,\ \tau^{\mathcal{N}}\big(P - ww^*\big)\right\}\,.
$$

Then for any projective measurement $\{P_a\}_{a\in\mathcal{A}}$ on $\mathcal{N}$, there is a projective measurement $\{Q_a\}_{a\in\mathcal{A}}$ on $\mathcal{M}$ such that

$$\sum_{a\in\mathcal{A}} \big\|Q_a - w^* P_a w\big\|_2^2 \;\le\; 56\varepsilon \;. \tag{3}$$

Proof. If $\varepsilon \ge \frac{1}{2}$ the conclusion is trivial (for a suitably large implicit constant in the $O(\cdot)$ notation in (3)), so assume $\varepsilon < \frac{1}{2}$. Define

$$\tilde{Q}_a = w^* P_a w + \frac{1}{|\mathcal{A}|}\big(I_{\mathcal{M}} - w^* w\big) \in \mathcal{M} \;.$$

Then $\{\tilde{Q}_a\}$ is a POVM on $\mathcal{M}$. Moreover,

$$\begin{aligned}
\sum_a \tau^{\mathcal{M}}\big(\tilde{Q}_a^2\big) &\ge \sum_a \tau^{\mathcal{M}}\big((w^* P_a w)^2\big) \\
&= \sum_a \tau^{\mathcal{M}}\big(w^* P_a w w^* P_a w\big) \\
&= \sum_a \tau^{\mathcal{M}}\big(w^* P_a P P_a w\big) - \sum_a \tau^{\mathcal{M}}\big(w^* P_a (P - ww^*) P_a w\big) \\
&\ge 1 - \varepsilon - \sum_a \tau_\infty\big(w^* P_a (P - ww^*) P_a w\big)
\end{aligned}$$

(Henry: I don't get this next line... how did τ_∞ show up?) **(Thomas:** By definition, $\mathcal{M}$ is seen as a sub-algebra of $\mathcal{M}_\infty$, and τ_∞ restricted to that sub-algebra is $\tau^{\mathcal{M}}$. So, whenever $M \in \mathcal{M}$, $\tau^{\mathcal{M}}(M) = \tau_\infty(\mathcal{M})$ is a legal "shortcut" in the writing. It's this sentence about the "corner" in the prelims...should we add something more explicit? Or explain this line here more, since it's the first time we make the manipulation?) **(Henry:** I think it would be good to add at least one line of explanation...) **(Thomas:** added (extra line above and justification below))

$$\begin{aligned}
&\ge 1 - \varepsilon - \tau_\infty\Big(\big(P - ww^*\big)\Big(\sum_a P_a w w^* P_a\Big)\Big) \\
&\ge 1 - \varepsilon - \tau_\infty\big(P - ww^*\big)\;,
\end{aligned}$$

where the third line uses that $P_a P P_a = P_a$, $\sum_a P_a = I_{\mathcal{N}}$ and the definition of ε for the first term, and for the second the fact that for $A \in \mathcal{M}$, $\tau^{\mathcal{M}}(A) = \tau_\infty(A)$ by definition of τ_∞ and the identification of $\mathcal{M}$ with a "corner" in $\mathcal{M}_\infty$, the fourth line uses cyclicity of the trace for the second, and the last uses $\|ww^*\|, \|\sum_a P_a\|_\infty \le 1$. By assumption,

$$\tau_\infty\big(P - ww^*\big) \;\le\; \varepsilon\, \tau_\infty(P) \;\le\; \frac{\varepsilon}{1-\varepsilon}\;.$$

where the last inequality is because by definition, $\tau^N(P) = 1$, thus

$$1 - \varepsilon \;\le\; \tau^{\mathcal{N}}(ww^*) \;=\; \frac{\tau_\infty(ww^*)}{\tau_\infty(P)} \;=\; \frac{\tau_\infty(w^* w)}{\tau_\infty(P)} \;\le\; \frac{1}{\tau_\infty(P)}$$

since $\tau_\infty(w^* w) = \tau^{\mathcal{M}}(w^* w)$ and $w^* w \le I_{\mathcal{M}}$. Overall,

$$\sum_a \tau^{\mathcal{M}}\big(\tilde{Q}_a^2\big) \;\ge\; 1 - \varepsilon - \frac{\varepsilon}{1-\varepsilon} \;\ge\; 1 - 3\varepsilon\;.$$

To conclude we apply [dlS21, Theorem 1.2] to obtain a projective measurement $\{Q_a\}$ on $\mathcal{M}$ such that

$$\sum_a \|Q_a - \tilde{Q}_a\|_2^2 \,=\, 27\varepsilon \,.$$

Finally,

$$\begin{aligned}\sum_a \|Q_a - w^* P_a w\|_2^2 &= \sum_a \Big\|Q_a - \tilde{Q}_a + \frac{1}{|\mathcal{A}|}(I_{\mathcal{M}} - w^* w)\Big\|_2^2 \\ &\le \sum_a 2\|Q_a - \tilde{Q}_a\|_2^2 + 2\frac{1}{|\mathcal{A}|}\|I_{\mathcal{M}} - w^* w\|_2^2 \\ &\le 54\varepsilon + 2\tau^{\mathcal{M}}((I_{\mathcal{M}} - w^* w)^2) \\ &\le 54\varepsilon + 2\tau^{\mathcal{M}}(I_{\mathcal{M}} - w^* w) \\ &\le 56\varepsilon \,,\end{aligned}$$

where the second line is by the triangle inequality, the fourth line is due to the fact that $I_{\mathcal{M}} - w^* w$ is positive and has operator norm at most 1, and the last line is by $\tau^{\mathcal{M}}(I_{\mathcal{M}} - w^* w) \le \varepsilon$. □

4.3 Proof of Proposition 4.3

We prove the proposition.

Proof of Proposition 4.3. We start with the first assertion. Suppose that $G_{\mathcal{C},M}$ is δ'-robust, for some function δ'. Let $(\mathcal{M}, A)$ be be an ε-local presentation of $(\mathcal{C}, M)$, and for each $S \subseteq \{1, \dots, n\}$ such that $|S| \le r$, $\{B^{S,i}\}_{i \in S}$ the commuting family of projective measurements promised by the definition. Then for every S there is a projection $P^S \in \mathcal{M}_\infty$ and an isometry $w^S \in P^S \mathcal{M}_\infty I_{\mathcal{M}}$ such that

$$\mathop{\mathbb{E}}_{S \sim \nu} \mathop{\mathbb{E}}_{i \in S} \sum_{a \in \mathbb{F}_q} \big\|A_a^i - (w^S)^* B_a^{S,i} w^S\big\|_2^2 \,\le\, \varepsilon \,.$$

(Thomas: adding this to break up the proof a little:) The key step consists in proving the following claim.

Claim 4.7. *Let D be the decision predicate associated with the game $G_{\mathcal{C},M}$. There is a family $\{P_a^S\}_{a \in \mathbb{F}_q^S}$ of projective measurements on $\mathcal{M}$, for every $S \subseteq \{1, \dots, n\}$ such that $|S| \le r$, such that*

$$\sum_{S,i} \mu(S,i) \sum_{a \in \mathbb{F}_q^S} \sum_{b \in \mathbb{F}_q} D(S,i,a,b)\tau\big(P_a^S A_b^i\big) \,\ge\, 1 - O(\sqrt{\varepsilon}) \,. \tag{4}$$

Proof. For any $a \in \mathbb{F}_q^S$ let $\tilde{P}_a^S = \prod_{i \in S} B_{a_i}^{S,i}$ (since the measurements $\{B^{S,i}\}_i$ are pairwise commuting, the order of the product does not matter). Then $\{\tilde{P}_a^S\}_{a \in \mathbb{F}_q^S}$ is a projective measurement such that for any $i \in S$ and $b \in \mathbb{F}_q$,

$$\sum_{a \,:\, a_i = b} \tilde{P}_a^S \,=\, B_b^{S,i} \,.$$

Using this identity,

$$\begin{aligned}\mathop{\mathbb{E}}_{S\sim\nu}\mathop{\mathbb{E}}_{i\in S}\sum_{a\in\mathbb{F}_q^S}\tau\big((w^S)^*\tilde{P}_a^S w^S\,A^i_{a_i}\big) &= \mathop{\mathbb{E}}_{S\sim\nu}\mathop{\mathbb{E}}_{i\in S}\sum_{b\in\mathbb{F}_q}\tau\big((w^S)^*B_b^{S,i}w^S\,A^i_b\big)\\ &= \mathop{\mathbb{E}}_{S\sim\nu}\mathop{\mathbb{E}}_{i\in S}\frac{1}{2}\Big(\tau\big((w^S)^*w^S\big)+\tau(1)-\sum_{b\in\mathbb{F}_q}\big\|(w^S)^*B_b^{S,i}w^S-A^i_b\big\|_2^2\Big)\\ &\geq \frac{1}{2}(1-\varepsilon+1-\varepsilon)\;. \end{aligned}\tag{5}$$

Starting from the $\{\tilde{P}_a^S\}$, let $\{P_a^S\}$ be the family of projective measurements on $\mathcal{M}$ that is promised by Lemma 4.6. By a simple averaging argument,

$$\mathop{\mathbb{E}}_{S\sim\nu}\sum_{a\in\mathbb{F}_q^S}\big\|P_a^S-(w^S)^*\tilde{P}_a^S(w^S)\big\|_2^2 \;=\; O(\varepsilon)\;.\tag{6}$$

We can write

$$\begin{aligned}&\Big|\mathop{\mathbb{E}}_{S\sim\nu}\mathop{\mathbb{E}}_{i\in S}\sum_{a\in\mathbb{F}_q^S}\tau\big(P_a^S A^i_{a_i}\big)-\mathop{\mathbb{E}}_{S\sim\nu}\mathop{\mathbb{E}}_{i\in S}\sum_{a\in\mathbb{F}_q^S}\tau\big((w^S)^*\tilde{P}_a^S(w^S)A^i_{a_i}\big)\Big|\\ &\qquad= \Big|\mathop{\mathbb{E}}_{S\sim\nu}\mathop{\mathbb{E}}_{i\in S}\sum_{a\in\mathbb{F}_q^S}\tau\big(\big(P_a^S-(w^S)^*\tilde{P}_a^S(w^S)\big)A^i_{a_i}\big)\Big|\\ &\qquad\leq \mathop{\mathbb{E}}_{S\sim\nu}\mathop{\mathbb{E}}_{i\in S}\sum_{a\in\mathbb{F}_q^S}\tau\big(\big|(w^S)^*\tilde{P}_a^S(w^S)-P_a^S\big|\big)\\ &\qquad= O(\sqrt{\varepsilon})\;,\end{aligned}\tag{7}$$

where the inequality uses Hölder's inequality with $\|A^i_a\|\leq 1$ and the last line is by Lemma 4.4 and (6). Using the definition of $G_{\mathcal{C},M}$, we have shown that

$$\begin{aligned}\sum_{S,i}\mu(S,i)\sum_{a\in\mathbb{F}_q^S}\sum_{b\in\mathbb{F}_q}D(S,i,a,b)\tau\big(P_a^S A^i_b\big) &= \mathop{\mathbb{E}}_{S\sim\nu}\mathop{\mathbb{E}}_{i\in S}\sum_{a\in\mathbb{F}_q^S}\tau\big(P_a^S A^i_{a_i}\big)\\ &\geq O\big(\sqrt{\varepsilon}\big)-\mathop{\mathbb{E}}_{S\sim\nu}\mathop{\mathbb{E}}_{i\in S}\sum_{a\in\mathbb{F}_q^S}\tau\big((w^S)^*\tilde{P}_a^S(w^S)A^i_{a_i}\big)\\ &= 1-O\big(\sqrt{\varepsilon}\big)\;,\end{aligned}$$

where the first line uses the definition of $\mu(\cdot,\cdot)$, the second line uses (7) and the last uses (5). □

Claim 4.7 shows that $\omega(G_{\mathcal{C},M};\mathscr{S})\geq 1-\varepsilon'$ for $\mathscr{S}$ the strategy with measurements $\{A^i_b\}$ and $\{P_a^S\}$ and some $\varepsilon'=O(\sqrt{\varepsilon})$. Using the definition of robustness we deduce that $\mathscr{S}$ is $(\delta'(\varepsilon'),\nu)$-close to a perfect strategy $\mathscr{S}'$ for $G_{\mathcal{C},M}$. Since ν is uniform on $\{1,\ldots,n\}$ we specialize to the A measurements; using the definition of closeness there exists a projection $P\in\mathcal{M}_\infty$ such that $\{C^i\}_a\subseteq P\mathcal{M}_\infty P$ and $\mathbb{E}_i\sum_a\|A^i_a-w^*C^i_a w\|_2^2\leq 2\delta'$, and moreover $\{C^i_a\}$ satisfy that for any S in the support of μ, $\{C^i_a\}$ pairwise commute for $i\in S$. Using the assumption that $(\mathcal{C},M)$ is Abelian, all the $\{C^i_a\}$ commute and form a representation of $\mathcal{C}$.

Now we show the second assertion. Suppose that M has quantum soundness δ. Let $\mathscr{S}=(\mathcal{M},A,P)$ be a strategy for $G_{\mathcal{C},M}$ on $(\mathcal{M},\tau)$ that succeeds with probability at least $1-\varepsilon$. This can be reformulated as

$$\sum_{(S,i)}\mu(S,i)\sum_{a\in\mathbb{F}_q^s}\sum_{b\in\mathbb{F}_q}D(S,i,a,b)\tau\big(P_a^S A^i_b\big)\;\geq\;1-\varepsilon\;.\tag{8}$$

For each S and $i \in S$, let $B_b^{S,i} = \sum_{a:a_i=b} P_a^S$. Then using the definition of μ and D, rewriting (8) immediately gives

$$\mathop{\mathbb{E}}_{S\sim\nu}\mathop{\mathbb{E}}_{i\in S}\sum_{b\in\mathbb{F}_q}\left\|A_b^i - B_b^{S,i}\right\|_2^2 \leq 2\varepsilon\ . \tag{9}$$

Thus $(\mathcal{M}, A)$ is an ε'-local presentation of code, for $\varepsilon' = 2\varepsilon$. Using quantum soundness, there is a representation $(\mathcal{N}, C)$ of $\mathcal{C}$ that is δ'-close to $(\mathcal{M}, A)$, for $\delta' = \delta(\varepsilon')$.

For every S, let $Q_a^S = \prod_{i\in S} C_{a_i}^i$, which is a projective measurement on $\mathcal{N}$. It is easy to verify that $(\mathcal{N}, C, Q)$ is a perfect strategy in $G_{\mathcal{C},M}$. Using the definition of ν, it follows that $(\mathcal{N}, B, Q)$ is $O(\delta')$-close to $(\mathcal{M}, A, P)$.

□

5 Main result

In this section we focus on binary codes only, see Section 6 for the case of fields over $\mathbb{F}_q$ for q a power of 2.

We start by defining a notion of "qubit test," and state an interesting consequence of the definition in terms of dimension tests. In Section **??** we describe a test, the *braiding test*, that can be constructed from any linear code and in Section 5 we state and prove our main result, which is that whenever the braiding test is based on a quantum sound code then it is a qubit test.

5.1 Qubit tests

Let $\mathcal{C}$ be an $[n,k,d]$ linear code and M an r-local tester for $\mathcal{C}$. Recall that for a projective measurement $P = \{P_a\}_{a\in\mathbb{F}_2^k}$, we use $\widehat{P}(b)$ to denote the corresponding observable (see

??). For binary outcome measurements $P = \{P_0, P_1\}$, we write $\widehat{P}$ to denote $P_0 - P_1$.

Definition 5.1. Let $k \in \mathbb{N}$ and $\delta : [0,1] \to \mathbb{R}_+$. A $(k, \delta(\varepsilon))$*-qubit test* is a synchronous game $G = (\mathcal{X}, \mu, \mathcal{A}, D)$ such there are two sets $S_X, S_Z \subseteq \mathbb{F}_2^k$ that span $\mathbb{F}_2^k$ and an injection $\phi : (\{X\} \times S_X) \cup (\{Z\} \times S_Z) \to \mathcal{X}$ such that $\mathcal{A}(\phi(X,a)) = \mathcal{A}(\phi(Z,b)) = \mathbb{F}_2$ for all $a \in S_X$, $b \in S_Z$ and such that the following holds:

- (Completeness:) There is a synchronous strategy $(\mathcal{M}, P)$ for G on $\mathcal{M} = M_{2^k}(\mathbb{C})$ that succeeds with probability 1 in G and is such that $\widehat{P}^{\phi(W,a)} = \sigma^W(a)$ for every $W \in \{X, Z\}$ and $a \in S_W$.
- (Soundness:) **(Thomas:** added:) Let μ' denote the (renormalized) restriction of (the marginal of) μ to the image of ϕ in $\mathcal{X}$. Any synchronous strategy in $(\mathcal{M}, \tau)$ for G that succeeds with probability $1-\varepsilon$ for some $\varepsilon \geq 0$ is $(\delta(\varepsilon), \tilde{\mu})$-close to a strategy on some algebra $(M_{2^k}(\mathbb{C}) \otimes \mathcal{N}, \mathrm{tr} \otimes \tau')$ where $(\mathcal{N}, \tau')$ is a tracial sub-algebra of $\mathcal{M}_\infty$ and such that
$$\widehat{P}^{\phi(W,a)} = \sigma^W(a) \otimes I_{\mathcal{N}}\ .$$

(Thomas: commented out remark about special case where $S_X, S_Z = \emptyset$)

The next proposition states a simple consequence of a qubit test, which is that strategies with a high enough success probability must have a large dimension. This consequence is used in [JNV+20a].

Proposition 5.2. *Let* $G = (\mathcal{X}, \mu, \mathcal{A}, D)$ *denote a* $(k, \delta(\varepsilon))$*-qubit test Then all synchronous strategies* $\mathscr{S}$ *in* $(\mathcal{M}, \tau)$ *for* G *that succeed with probability* $1-\varepsilon$ *must satisfy*

$$\dim(\mathcal{M}) \geq \left(1 + O(\sqrt{\delta(\varepsilon)}) + \frac{\delta(\varepsilon)}{1-\delta(\varepsilon)}\right)^{-1} 2^k\ .$$

Proof. If $\mathcal{M}$ is infinite-dimensional, then we are done. Suppose instead it were finite-dimensional. Then $\mathcal{M}$ must be (isomorphic to) a direct sum of finite-dimensional matrix algebras. Without loss of generality we assume that $\mathcal{M} = M_d(\mathbb{C})$ with the dimension-normalized trace $\tau = \frac{1}{d}\mathrm{Tr}$.

By the soundness property of qubit tests, the strategy $\mathscr{S}$ is $(\delta(\varepsilon), \tilde{\mu})$-close to a strategy $\mathscr{S}'$ on an algebra $(M_{2^k}(\mathbb{C}) \otimes \mathcal{N}, \mathrm{tr}_{2^k} \otimes \tau')$ for some tracial algebra $(\mathcal{N}, \tau')$ where $\mathrm{tr}_{2^k} = 2^{-k}\mathrm{Tr}$. For notational brevity we write $\mathcal{R} = M_{2^k}(\mathbb{C}) \otimes \mathcal{N}$ and $\tau^{\mathcal{R}} = \mathrm{tr}_{2^k} \otimes \tau'$. By definition there exists a projection $P \in \mathcal{M}_\infty$ of finite trace and a partial isometry $w \in P\mathcal{M}_\infty 1_{\mathcal{M}}$ satisfying

1. $\mathcal{R} = P\mathcal{M}_\infty P$.
2. $\max\left\{\tau(1_{\mathcal{M}} - w^*w), \tau^{\mathcal{R}}(P - ww^*)\right\} \le \delta(\varepsilon)$.
3. $\tau^{\mathcal{R}} = \tau_\infty/\tau_\infty(P)$.

For $u \in \mathbb{F}_2^k$ let σ_u^Z denote the projection

$$\sigma_u^Z = 2^{-k} \sum_{a \in \mathbb{F}_2^k} (-1)^{a \cdot u} \sigma^Z(a) \ .$$

It is easy to verify that $\{\sigma_u^Z \otimes I_{\mathcal{N}}\}_{u \in \mathbb{F}_2^k}$ is a projective measurement in $\mathcal{R}$ and furthermore $\tau^{\mathcal{R}}(\sigma_u^Z \otimes I_{\mathcal{N}}) = 2^{-k}$. Applying

?? we get that there exist projective measurement $\{Q_u\}_{u \in \mathbb{F}_2^k}$ on $\mathcal{M}$ such that

$$\sum_u \|Q_u - w^*(\sigma_u^Z \otimes I_{\mathcal{N}})w\|_2^2 \le 56\,\delta(\varepsilon) \ .$$

Applying

?? we get

$$\sum_u \tau\Big(\Big|Q_u - w^*(\sigma_u^Z \otimes I_{\mathcal{N}})w\Big|\Big) \le O(\sqrt{\delta(\varepsilon)}) \ .$$

Then we have

$$\begin{aligned}
\sum_u \Big|\tau(Q_u) - 2^{-k}\Big| &\le \sum_u \Big|\tau(w^*(\sigma_u^Z \otimes I_{\mathcal{N}})w) - 2^{-k}\Big| + \tau\Big(\Big|Q_u - w^*(\sigma_u^Z \otimes I_{\mathcal{N}})w\Big|\Big) \\
&= O(\sqrt{\delta(\varepsilon)}) + \sum_u \Big|\tau_\infty(ww^*(\sigma_u^Z \otimes I_{\mathcal{N}})) - 2^{-k}\Big| \\
&= O(\sqrt{\delta(\varepsilon)}) + \sum_u \Big|\tau_\infty(P(\sigma_u^Z \otimes I_{\mathcal{N}})) - 2^{-k}\Big| + \Big|\tau_\infty((P - ww^*)(\sigma_u^Z \otimes I_{\mathcal{N}}))\Big|
\end{aligned}$$

Notice that $\tau_\infty(P(\sigma_u^Z \otimes I_{\mathcal{N}})) = \tau_\infty(\sigma_u^Z \otimes I_{\mathcal{N}}) = 2^{-k}$, and that $ww^* \le P$ and thus $\tau_\infty((P - ww^*)(\sigma_u^Z \otimes I_{\mathcal{N}}))$ is a nonnegative real number. Therefore the sum in the last line simplifies to

$$\sum_u \tau_\infty((P - ww^*)(\sigma_u^Z \otimes I_{\mathcal{N}})) = \tau_\infty((P - ww^*)P) = \tau_\infty(P - ww^*) \le \tau_\infty(P) \cdot \delta(\varepsilon) \ .$$

On the other hand the proof of

?? shows that $\tau_\infty(P) \le \frac{1}{1-\delta(\varepsilon)}$, and thus

$$\sum_u \Big|\tau(Q_u) - 2^{-k}\Big| \le O(\sqrt{\delta(\varepsilon)}) + \frac{\delta(\varepsilon)}{1 - \delta(\varepsilon)} \ .$$

By averaging, there exists a $u \in \mathbb{F}_2^k$ such that

$$\tau(Q_u) = \frac{1}{d}\mathrm{Tr}(Q_u) \le \Big(1 + O(\sqrt{\delta(\varepsilon)}) + \frac{\delta(\varepsilon)}{1-\delta(\varepsilon)}\Big)2^{-k} \,.$$

Rearranging, this implies that d, the dimension of $\mathcal{M}$, satisfies

$$d \ge \Big(1 + O(\sqrt{\delta(\varepsilon)}) + \frac{\delta(\varepsilon)}{1-\delta(\varepsilon)}\Big)^{-1} 2^k$$

as desired. □

5.2 The braiding test

We introduce our main test, the *braiding test*, which can be based on any linear code $\mathcal{C}$ and tester M for it. Before we state the test, we recall the classic *commutation* and *anticommutation* games.

Commutation game. We call *commutation game* the game defined in [dlS22, Section 3.1]. For convenience we change the notation slightly and denote $x_{\mathrm{X},0}, x_{\mathrm{Z},0} \in \mathcal{X}_{com}$ the two special questions, $x_{com,1}$ and $x_{com,2}$ respectively.

Anti-commutation game. We call *anti-commutation game* the game defined in [dlS22, Section 3.2]. For convenience we change the notation slightly and denote $x_{\mathrm{X},1}, x_{\mathrm{Z},1} \in \mathcal{X}_{anticom}$ the two special questions, $x_{anticom,1}$ and $x_{anticom,2}$ respectively.

The braiding test. Let $\mathcal{C}$ be an $[n,k,d]_2$ linear code and M an r-local tester for $\mathcal{C}$. The braiding test constructed from $\mathcal{C}$ and M is described in Figure 1. Informally, the test combines two independent copies of the code test from Section **??** with appropriate commutation and anti-commutation games that will force any successful strategy in the game to be close, in some sense, to a representation of the Pauli group generated by observables $\sigma^X(a)$ and $\sigma^Z(b)$, $a, b \in \mathbb{F}_2^k$.

5.3 A qubit test from any quantum-sound code

Our main theorem shows that the braiding test is a qubit test, whenever it is instantiated with a pair $(\mathcal{C}, M)$ that is quantum sound.

Theorem 5.3. *Let $\mathcal{C}$ be an $[n,k,d]$ linear code and M an r-local tester for $\mathcal{C}$ that is $\delta(\varepsilon)$-quantum sound and such that $(\mathcal{C}, M)$ is Abelian. Then the braiding test over $\mathcal{C}$ is a (k, δ')-qubit test with sets $S_{\mathrm{X}} = S_{\mathrm{Z}} = \{E_{\mathcal{C}} e_i : i \in \{1,\ldots,n\}\} \subseteq \mathbb{F}_2^k$, map $\phi(W, E_{\mathcal{C}} e_i) = (W, i)$ and error function $\delta' = O(\delta^{1/2}(6\varepsilon))$.*[4]

Before we give the proof of the theorem we introduce a game, which we denote G_{dlS}, that is a specific instantiation of a more general class of games analyzed in [dlS22, Section 3.4]. The proof of soundness of the qubit test will be a reductio to the results from [dlS22]. Using notation from [dlS22], the game G_{dlS} is obtained by making the following choices. The group is $H = \mathbb{F}_2^k$. Let

$$S_{\mathrm{X}} = S_{\mathrm{Z}} = \{G_{\mathcal{C}} e_i : i \in \{1,\ldots,n\}\} \subseteq \mathbb{F}_2^k \,,$$

[4] Assume $E_{\mathcal{C}}$ has no repeated columns.

Let M be an r-local tester with distribution ν for the $[n,k,d]$ code $\mathcal{C}$. Execute either of the following tests with probability $1/3$ each.

1. (**Code test**) Sample $W \in \{X,Z\}$ uniformly at random, a set $S \subseteq \{1,\ldots,n\}$ from the distribution ν, and an index $i \in S$ uniformly at random. Send (W,S) to A and (W,i) to B. Receive $a \in \mathbb{F}_2^S$ from A and $b \in \mathbb{F}_2$ from B. Accept if and only if $M(S,a) = 1$ and $a_i = b$.
2. (**Anti-commutation test**) Sample $(i_X, i_Z) \in \{1,\ldots,n\}^2$ uniformly at random. Let $\omega = (E_{\mathcal{C}} e_{i_X}, E_{\mathcal{C}} e_{i_Z})$ and $\gamma = (E_{\mathcal{C}} e_{i_X}) \cdot (E_{\mathcal{C}} e_{i_Z}) \in \mathbb{F}_2$.
   (a) If $\gamma = 0$ then sample a pair of questions (x_c, y_c) as in the commutation game. Send (x_c, ω) to A and (y_c, ω) to Bob. Accept if and only if their answers are accepted in the commutation game.
   (b) If $\gamma \neq 0$ then do the same but for the anti-commutation game.
3. (**Consistency test**) Sample $(i_X, i_Z) \in \{1,\ldots,n\}^2$ and $W \in \{X,Z\}$ uniformly at random. Let $\omega = (E_{\mathcal{C}} e_{i_X}, E_{\mathcal{C}} e_{i_Z})$ and $\gamma = (E_{\mathcal{C}} e_{i_X}) \cdot (E_{\mathcal{C}} e_{i_Z}) \in \mathbb{F}_2$. Send (W, i_W) to A and $(x_{W,\gamma}, \omega)$ to B, where $x_{W,\gamma}$ is a question from the anti-commutation game. Receive $a \in \mathbb{F}_2$ and $b \in \mathbb{F}_2$ respectively. Accept if and only if $a = b$.

Figure 1: The braiding test over $\mathcal{C}$ verifies that the players respond consistently with a uniformly random codeword from $\mathcal{C}$.

and let μ_{dlS} be the uniform distribution over $S_X \times S_Z$. Let Ω be the support of μ_{dlS} and α, β the coordinate projections. Then $G_{\mathrm{dlS}} = (\mathcal{X}, \mu_{\mathrm{dlS}}, \mathcal{A}, D)$ has question set $\mathcal{X} = \{PX, PZ\} \cup (\mathcal{X}_{com} \times \Omega_+) \cup (\mathcal{X}_{anticom} \times \Omega_-)$ and is as described in [dlS22, Section 3.4]. For clarity we recall the game, using our notation, in Figure 2.

Let $S_X, S_Z \subseteq \mathbb{F}_2^k$. Sample $\omega = (\omega_X, \omega_Z) \in S_X \times S_Z$ uniformly at random. Let $\gamma = \omega_X \cdot \omega_Z \in \mathbb{F}_2$. Execute either of the following tests with probability $1/3$ each.

1. (**Anti-commutation test**)

   (a) If $\gamma = 0$ then sample a pair of questions (x_c, y_c) as in the commutation game. Send (x_c, ω) to A and (y_c, ω) to Bob. Accept if and only if their answers are accepted in the commutation game.

   (b) If $\gamma \neq 0$ then do the same but for the anti-commutation game.

2. (Z-**Consistency test**) Send Z to A and $(x_{Z,\gamma}, \omega)$ to B. Receive $a \in \mathbb{F}_2^k$ and $b \in \mathbb{F}_2$ respectively. Accept if and only if $a \cdot \omega_Z = b$.

3. (X-**Consistency test**) Send X to A and $(x_{X,\gamma}, \omega)$ to B. Receive $a \in \mathbb{F}_2^k$ and $b \in \mathbb{F}_2$ respectively. Accept if and only if $a \cdot \omega_X = b$.

Figure 2: The game G_{dlS} checks (anti)commutation relations between two collections of observables.

We will also make use of the following simple fact.

Lemma 5.4 (Data-processing). *Let $\{P_a\}$ and $\{Q_a\}$ be two POVMs on $(\mathcal{M}, \tau)$ with the same outcome set $\mathcal{A}$. Then for any function $f : \mathcal{A} \to \mathcal{B}$ for some finite set $\mathcal{B}$,*

$$\sum_{b \in \mathcal{B}} \Big\| \sum_{a \in f^{-1}(b)} (P_a - Q_a) \Big\|_2^2 \leq \sum_{a \in \mathcal{A}} \|P_a - Q_a\|_2^2 \,. \tag{10}$$

Proof. This follows by expending the left-hand side and using $\tau(P_a Q_{a'}) \geq 0$ for all $a \neq a'$. □

Proof of Theorem 5.3. Completeness: We first verify completeness. For $W \in \{X, Z\}$, $i \in \{1, \ldots, n\}$ and $b \in \mathbb{F}_2$ let $P_b^{(W,i)} = \frac{1}{2}(I + (-1)^b \sigma^W(E_{\mathcal{C}} e_i))$, and for $a \in \mathbb{F}_2^S$ let $P_a^{(W,S)} = \prod_{i \in S} P_{a_i}^{(W,i)}$. Writing (f_0, f_1) for the canonical basis of $\mathbb{C}^2$, $P_a^{(W,S)}$ is the projection on the span of all $\otimes_{i=1}^k f_{u_i}$ where $u = (u_1, \ldots, u_k)$ is such that $u^T E_{\mathcal{C}} = a$.

For $(i_X, i_Z) \in \{1, \ldots, n\}^2$ let $\omega = (E_{\mathcal{C}} e_{i_X}, E_{\mathcal{C}} e_{i_Z})$ and $\gamma = (E_{\mathcal{C}} e_{i_X}) \cdot (E_{\mathcal{C}} e_{i_Z})$ we let $P^{x_{W,\gamma},\omega} = P^{(W,i_W)}$.

These choices already ensure that the strategy succeeds with probability 1 in the consistency test. We verify that it succeeds in the code test. Let $S \subseteq \{1, \ldots, n\}$. As observed above, for any $a \in \mathbb{F}_2^S$ such that $P_a^{W,S} \neq 0$ there is an $u \in \mathbb{F}_2^k$ such that $u^T E_{\mathcal{C}} = a$, which means that $a \in \mathcal{C}$. Using the completeness property of M it follows that M must accept any a such that $P_a^{W,S} \neq 0$, which shows that the strategy succeeds in the code test with probability 1.

It remains to verify that the anti-commutation test is passed with probability 1. For this we observe that the binary observables

$$U = \widehat{P}^{x_{X,\gamma},\omega} \quad \text{and} \quad V = \widehat{P}^{x_{Z,\gamma},\omega}$$

commute in case $\gamma = 0$ and anti-commute in case $\gamma = 1$. This is because by construction $U = \sigma^X(E_{\mathcal{C}} i_X)$ and $V = \sigma^W(E_{\mathcal{C}} i_W)$, and because of the definition of γ. Hence the pair (U, V) can be completed to a perfect strategy for the commutation game (if $\gamma = 0$) or anti-commutation game (if $\gamma = 1$). This defines the measurements $P^{(x,\omega)}$ for $x \notin \{x_{W,\gamma}, W \in \{X, Z\}, \gamma \in \{0, 1\}\}$.

Soundness: Next we show soundness. Let $\mathscr{S}$ be a synchronous strategy for the braiding test in $(\mathcal{M}, \tau)$ that succeeds with probability at least $1 - \varepsilon$. For $W \in \{X, Z\}$ let $\mathscr{S}^W$ be the strategy in $G_{\mathcal{C},M}$ that is obtained by restricting $\mathscr{S}$ to the relevant measurements **(Henry:** added:) corresponding to the "Code test" part of the braiding test, i.e. the $P^{W,S}$ and $P^{W,i}$. Then $\mathscr{S}^W$ succeeds with probability at least $1 - 3\varepsilon$ in $G_{\mathcal{C},M}$. Using the assumption that M is $\delta(\cdot)$-quantum sound and the second item from Proposition 4.3 it follows that there is a $\delta_1 = O(\delta(6\varepsilon))$ such that for each $W \in \{X, Z\}$, $\mathscr{S}^W$ is (δ_1, ν) close to a perfect strategy $\tilde{\mathscr{S}}^W$ on $(\mathcal{N}^W, \tau^W)$ for $G_{\mathcal{C},M}$, where ν is uniform on $\{1, \ldots, n\}$. This strategy has measurement operators $\{\tilde{P}_a^{W,S}\}$ and $\{\tilde{P}_b^{W,i}\}$ associated with questions of the form S and i in $G_{\mathcal{C},M}$. Using the definition of ν, these satisfy that

$$\mathop{\mathbb{E}}_{i\in\{1,\ldots,n\}} \sum_{b\in\mathbb{F}_2} \big\|P_b^{W,i} - (w^W)^* \tilde{P}_b^{W,i} w^W\big\|_2^2 = O(\delta_1)\,. \tag{11}$$

Furthermore, since $(\mathcal{C}, M)$ is Abelian, there is a POVM $\{\tilde{P}_u^W\}_{u\in\mathbb{F}_2^n}$ such that $\sum_{u\in\mathcal{C}} \tilde{P}_u^W = I$ and for each $i \in \{1, \ldots, n\}$, $\tilde{P}_b^{W,i} = \sum_{u: u_i = b} \tilde{P}_u^W$.

Applying Lemma 4.6, we obtain projective measurements $\{Q_u^W\}$ on $\mathcal{M}$ such that

$$\sum_u \big\|Q_u^W - (w^W)^* \tilde{P}_u^W w^W\big\|_2^2 = O(\delta_1)\,. \tag{12}$$

For any $i \in \{1, \ldots, n\}$ let $Q_b^{W,i} = \sum_{a:\, a_i = b} Q_a^W$. Then by Lemma 5.4,

$$\begin{aligned}\mathop{\mathbb{E}}_i \sum_b \tau\big(Q_b^{W,i}(w^W)^* \tilde{P}_b^{W,i}(w^W)\big) &\geq \mathop{\mathbb{E}}_i \sum_a \tau\big(Q_a^W(w^W)^* \tilde{P}_a^W(w^W)\big)\\ &\geq 1 - O(\delta_1)\,.\end{aligned}$$

For $W \in \{X, Z\}$ and $b \in \mathbb{F}_2^k$ let $R_b^W = Q_{G_{\mathcal{C}}^T b}^W$, where by definition $G_{\mathcal{C}}^T b \in \mathcal{C}$.

We now define a strategy $\mathscr{S}'$ for the game G_{dlS}. On question $W \in \{X, Z\}$ the projective measurement is $\{R_b^W\}$. On question of the form (x_c, ω) for x_c a question in the commutation game, the projective measurement is $\{P^{x_c,\omega}\}$, i.e. the same projective measurement as used in $\mathscr{S}$. Similarly, on a question of the form (x_{ac}, ω) for x_{ac} a question in the anti-commutation game, the projective measurement is $\{P^{x_{ac},\omega}\}$.

To conclude we show that this strategy succeeds in the game G_{dlS} with probability $1 - O(\sqrt{\delta_1})$. Assuming that this has been shown, by [dlS22, Corollary 3.9] the strategy $\mathscr{S}'$ is $O(\sqrt{\delta_1})$-close to a strategy $\mathscr{S}''$ on an algebra of the form $(M_{2^k}(\mathbb{C}) \otimes \mathcal{N}, \mathrm{tr} \otimes \tau')$ such that $P_b^W = \sigma_b^W \otimes I_{\mathcal{N}}$. By definition of R,

$$Q_b^{W,i} = \sum_{a\in\mathbb{F}_2^n:\, a_i = b} Q_a^W = \sum_{c\in\mathbb{F}_2^k: (G_{\mathcal{C}}^T c)_i = b} R_c^W\,, \tag{13}$$

hence

$$\widehat{Q}^{W,i} = \sum_c (-1)^{c\cdot(G_{\mathcal{C}} e_i)} R_c^W = \widehat{R}^W(G_{\mathcal{C}} e_i)\,.$$

Using the definition of the game distribution, closeness of $\mathscr{S}'$ and $\mathscr{S}''$ thus implies that

$$\mathop{\mathbb{E}}_{i\in\{1,\ldots,n\}} \big\|\widehat{Q^{W,i}} - (w'')^* \sigma^W(G_{\mathcal{C}} e_i)(w'')\big\|_2^2 = O(\sqrt{\delta_1})\,.$$

Combining with (11) and (12), this shows the theorem.

It remains to verify that $\mathscr{S}'$ succeeds in the game G_{dlS} with probability $1 - O(\sqrt{\delta_1})$. By definition $\mathscr{S}'$ succeeds in the (anti)-commutation test with probability $1 - O(\varepsilon)$. It remains to check the W-consistency test, for $W \in \{X, Z\}$. Because $\mathscr{S}$ succeeds with probability $1 - O(\varepsilon)$ in the consistency test,

$$\mathop{\mathbb{E}}_{i_X,i_Z\in\{1,\dots,n\}} \sum_b \tau\big(P_b^{W,i} P_b^{x_{W,\gamma,\omega}}\big) \,\geq\, 1 - O(\varepsilon)\,,$$

where ω and γ are defined as in Figure 1. Using (11), (12) and Lemma 4.5 it follows that

$$\mathop{\mathbb{E}}_{i_X,i_Z\in\{1,\dots,n\}} \sum_b \tau\big(Q_b^{W,i} P_b^{x_{W,\gamma,\omega}}\big) \,\geq\, 1 - O(\sqrt{\delta_1})\,,$$

Using (13), this can be rewritten as

$$\mathop{\mathbb{E}}_{i_X,i_Z\in\{1,\dots,n\}} \sum_{b,c:(G_{\mathcal{C}}^T c)_i = b} \tau\big(R_c^{W} P_b^{x_{W,\gamma,\omega}}\big) \,\geq\, 1 - O(\sqrt{\delta_1})\,. \tag{14}$$

Since $\omega_W = G_{\mathcal{C}} e_i$, $(G_{\mathcal{C}}^T c)_i = c \cdot \omega_W$. Thus (14) shows that $\mathscr{S}'$ succeeds with probability $1 - O(\sqrt{\delta_1})$ in the W-consistency test, as desired. □

6 Application: the Pauli braiding test

In this section we apply the general construction from Section 5 to a specific quantum-sound code with particularly good parameters, the Reed-Muller code. This was shown sound in [JNV+22] as part of a slightly more general class of "tensor codes" shown quantum sound. The resulting qubit test is an important ingredient in the work [JNV+20a].

6.1 Code composition

Theorem 5.3 requires a quantum-sound code defined over the binary field. The Reed-Muller code is defined over $\mathbb{F}_q$, for q a large prime power. We can transform any q-ary code, for $q = 2^t$, into a binary code using the idea of *code composition* which we now describe.

For $q = 2^t$ and $a \in \mathbb{F}_2$ we let $\kappa(a) \in \mathbb{F}_2^t$ denote the binary representation of a, taken in a fixed but usually left implicit self-dual basis of $\mathbb{F}_2^t$ over $\mathbb{F}_2$. We extend κ to vectors over $\mathbb{F}_2$ coordinate-wise. We let $\mathrm{tr}(\cdot) : \mathbb{F}_q \to \mathbb{F}_2$ denote the trace over $\mathbb{F}_2$. Because we chose a self-dual basis for the binary representation, the trace satisfies $\mathrm{tr}(ab) = \kappa(a) \cdot \kappa(b)$.

Let $q = 2^t$ and $\mathcal{C}$ an $[n, k, d]_q$ linear code. Let $\mathcal{C}_{\mathrm{HAD}}$ be the Hadamard code over $\mathbb{F}_2^t$ (see Section 3.3). Let $T = 2^t$. Let $\mathcal{C}'$ be the $[Tn, tk, d']$ linear code over $\mathbb{F}_2$ defined as follows. Given $a \in (\mathbb{F}_2^t)^k$, first map $a \mapsto a' = \kappa^{-1}(a) \in \mathbb{F}_q^k$. Then encode a' to $b' = \mathcal{C}_{\mathrm{RM}}(a') \in \mathbb{F}_q^n$. Finally, return $b = \mathcal{C}_{\mathrm{HAD}}(\kappa(b')) \in (\mathbb{F}_2^T)^n$, where $\mathcal{C}_{\mathrm{HAD}}$ is applied component-wise. Using that $\mathcal{C}_{\mathrm{HAD}}$ has relative distance $\frac{1}{2}$, it is easy to verify that this code has distance $d' \geq dT/2$.

Given an r-local δ-tester M for $\mathcal{C}$, there is a natural rq-local tester M' for $\mathcal{C}'$ which can be described as follows. Index coordinates of $\mathcal{C}'$ by pairs $(i, \alpha) \in [n] \times \mathbb{F}_2^t$, fixing a bijection between $[Tn]$ and $[n] \times \mathbb{F}_2^t$. Then ν' is the uniform mixtures of two distributions, ν_1' and ν_2'. To sample from ν_1', sample $S \sim \nu$ and return the set $S \times \mathbb{F}_2^t$. To sample from ν_2', sample $i \sim [n]$ uniformly at random and $x, y \in \mathbb{F}_2^t$ uniformly at random, and return $\{i\} \times \{x, y, x + y\}$. The decision predicate M' executes M for all sets of the form $S \times \mathbb{F}_2^t$, and the tester for the Hadamard code (Section 3.3) for sets of the form $\{i\} \times \{x, y, x + y\}$.

Proposition 6.1. *Suppose that M is an r-local tester for $\mathcal{C}$ with quantum soundness δ. Then M' is an rq-local tester for $\mathcal{C}'$ with quantum soundness δ' such that $\delta'(\varepsilon) = \delta(O(\varepsilon))$.*

Proof. Let $\{A^{(i,\alpha)}\}$ and $\{B^{S,(i,\alpha)}\}$ be an ε-local presentation of $\mathcal{C}'$. By definition of the measure ν', there are $\{\varepsilon_i\}$ such that $\mathbb{E}_i\,\varepsilon_i \leq 2\varepsilon$ and for every i, the collections $\{A^{(i,\alpha)}\}$, for $\alpha \in \mathbb{F}_2^t$, and $\{B^{\{i\}\times\{x,y,x+y\},(i,x)}\}$, for $x, y \in \mathbb{F}_2^t$, form an ε_i-local presentation of $\mathcal{C}_{\mathrm{HAD}}$. By quantum soundness of $\mathcal{C}_{\mathrm{HAD}}$ (Theorem 3.9) $\{i\} \times \{x, y, x+y\}$), for each i there exists commuting $\{\hat{A}^{(i,\alpha)}\}$ that are $O(\varepsilon_i)$-close to the $\{A^{(i,\alpha)}\}$ and moreover are a representation of $\mathcal{C}_{\mathrm{HAD}}$. Let $w^{(i)}$ be the implied isometry. For every $a \in \mathbb{F}_2^t$, define $\hat{A}^i_a = \mathbb{E}_\alpha(-1)^{a\cdot\alpha}\hat{A}^{(i,\alpha)}$. Then by linearity this is a projective measurement:

$$\begin{aligned}
(\hat{A}^i_a)^2 &= \Big(\mathbb{E}_\alpha(-1)^{a\cdot\alpha}\hat{A}^{(i,\alpha)}\Big)^2\\
&= \mathbb{E}_{\alpha,\alpha'}(-1)^{a\cdot(\alpha+\alpha')}\hat{A}^{(i,\alpha)}\hat{A}^{(i,\alpha')}\\
&= \mathbb{E}_{\alpha,\alpha'}(-1)^{a\cdot(\alpha+\alpha')}\hat{A}^{(i,\alpha+\alpha')}\\
&= \hat{A}^i_a\,,
\end{aligned}$$

where the third line uses that $\{A^{(i,\alpha)}\}$ are a representation of $\mathcal{C}_{\mathrm{HAD}}$. Moreover, $\sum_a \hat{A}^i_a = \hat{A}^{(i,0)} = I$. Hence using Lemma 4.6, for every i we obtain a projective measurement $\{\tilde{A}^i_a\}$ on $\mathcal{M}$ such that

$$\sum_a \big\|\tilde{A}^i_a - (w^{(i)})^*\hat{A}^i_a(w^{(i)})\big\|_2^2 = O(\varepsilon_i)\,. \tag{15}$$

We then get

$$\begin{aligned}
\mathbb{E}_i\sum_a\Big\|\mathbb{E}_\alpha(-1)^{a\cdot\alpha}A^{(i,\alpha)} - \tilde{A}^i_a\Big\|_2^2 &\leq 2\,\mathbb{E}_i\sum_a\Big\|\mathbb{E}_\alpha(-1)^{a\cdot\alpha}A^{(i,\alpha)} - (w^{(i)})^*\hat{A}^i_a(w^{(i)})\Big\|_2^2 + O(\varepsilon)\\
&= 2\,\mathbb{E}_i\sum_a\Big\|\mathbb{E}_\alpha(-1)^{a\cdot\alpha}A^{(i,\alpha)} - \mathbb{E}_\alpha(-1)^{a\cdot\alpha}(w^{(i)})^*\hat{A}^{i,\alpha}(w^{(i)})\Big\|_2^2 + O(\varepsilon)\\
&= 2\,\mathbb{E}_i\,\mathbb{E}_\alpha\big\|A^{(i,\alpha)} - (w^{(i)})^*\hat{A}^{i,\alpha}(w^{(i)})\big\|_2^2 + O(\varepsilon)\\
&= O(\varepsilon)\,,
\end{aligned} \tag{16}$$

where the first line uses the triangle inequality and (15), the second line uses the definition of $\hat{A}^i_a$, the third line is Parseval's identity and the last is by closeness.

Now for $b \in \mathbb{F}_q$ define $\tilde{B}^{S,i}_b = \mathbb{E}_\alpha(-1)^{b\cdot\alpha}B^{S\times\mathbb{F}_2^t,(i,\alpha)}$, which for the same reasons as earlier is a projective measurement. To conclude we show that $\{\tilde{A}^i\}$ and $\{\tilde{B}^{S,i}\}$ form an $O(\varepsilon)$-presentation of $\mathcal{C}$. The fact that the $\{\tilde{B}^{S,i}\}$ satisfy the constraints imposed by M is clear, because $\{B^{S,(i,\alpha)}\}$ satisfy those of M'. For the closeness condition, we have

$$\begin{aligned}
\mathbb{E}_S\,\mathbb{E}_i\sum_b\big\|\tilde{A}^i_b - \tilde{B}^{S,i}_b\big\|_2^2 &\leq 2\,\mathbb{E}_S\,\mathbb{E}_i\sum_b\Big\|\mathbb{E}_\alpha(-1)^{b\cdot\alpha}A^{(i,\alpha)} - \mathbb{E}_\alpha(-1)^{b\cdot\alpha}B^{S\times\mathbb{F}_2^t,(i,\alpha)}\Big\|_2^2 + O(\varepsilon)\\
&= 2\,\mathbb{E}_S\,\mathbb{E}_i\,\mathbb{E}_\alpha\big\|A^{(i,\alpha)} - B^{S\times\mathbb{F}_2^t,(i,\alpha)}\big\|_2^2 + O(\varepsilon)\\
&\leq 4\varepsilon + O(\varepsilon)\,,
\end{aligned}$$

where the first inequality is by (16) and the triangle inequality, the second line by Parseval's formula and the last is by assumption. Thus quantum soundness of $\mathcal{C}'$ follows from quantum soundness of $\mathcal{C}$. □

6.2 The Reed-Muller code over $\mathbb{F}_q$

Fix integers $m, t \in \mathbb{N}$ and let $q = 2^t$ and $M = 2^m$. Let $\mathcal{P}(q, m, d)$ be the vector space over $\mathbb{F}_q$ that consists of all m-variate polynomials f over $\mathbb{F}_q$ of individual degree at most d, that is all functions of the form

$$f(x_1, \dots, x_m) = \sum_{\alpha \in \{0,1,\dots,d\}^m} c_\alpha \, x_1^{\alpha_1} \cdots x_m^{\alpha_m} \,,$$

where $\{c_\alpha\}$ is a collection of coefficients in $\mathbb{F}_q$. It is easy to verify that $\mathcal{P}(q, m, d)$ has dimension $D = (d+1)^m$ over $\mathbb{F}_q$. It follows that the map $\mathcal{C}_{\mathrm{RM}} : (c_\alpha) \mapsto f$ defines a $[q^m, (d+1)^m, D]_q$ linear code over $\mathbb{F}_q$, where $D \geq (1 - md/q)q^m$ follows from the Schwartz-Zippel lemma:

Lemma 6.2 (Schwartz-Zippel lemma [Sch80, Zip79])**.** *Let $f, g : \mathbb{F}_q^m \to \mathbb{F}_q$ be two unequal polynomials with total degree at most d. Then*

$$\Pr_{x \sim \mathbb{F}_q^m} \big(f(x) = g(x) \big) \leq \frac{d}{q} \,.$$

We define a tester M_{RM} for the code $\mathcal{C}_{\mathrm{RM}}$ over $\mathbb{F}_q$, see Figure 3. The second test applied by the tester, the subcube commutation test, may seem superfluous, because it always accepts. However, the test is important to show that the code is robust. Note that including the test imposes a non-trivial constraint of pairwise approximate commutation on representations of $\mathcal{C}_{\mathrm{RM}}$, and hence also on ε-local presentations. In particular, due to the presence of this test the pair $(\mathcal{C}_{\mathrm{RM}}, M_{\mathrm{RM}})$ is trivially Abelian.

Perform one of the following tests with probability $\frac{1}{2}$ each.

1. **Axis-parallel lines test:** Let $u \sim \mathbb{F}_q^m$ be a uniformly random point, $j \sim \{1, \dots, m\}$ chosen uniformly at random, and let $\ell = \{(u_1, \dots, u_{j-1}, s, u_{j+1}, \dots, u_m) \in \mathbb{F}_q^m : s \in \mathbb{F}_q\}$ be the axis-parallel line passing through u in the j-th direction. Read the entries indexed by ℓ and accept if and only if they match a degree-d polynomial.

2. **Subcube commutation test:** Sample $j \sim \{1, \dots, m\}$ uniformly at random, and sample $x_{m-j+2}, \dots, x_m \sim \mathbb{F}_q$ uniformly at random. Sample u, v independently and uniformly at random from $\mathbb{F}_q^m$, conditioned on the last $(j-1)$ coordinates of both points being $x_{m-j+2}, \dots, x_m$. Read the entries indexed by u and v and accept.

Figure 3: A local test for $\mathcal{C}_{\mathrm{RM}}$

Theorem 6.3. *M_{RM} has quantum soundness $\delta(\varepsilon) = \mathrm{poly}(m, d) \cdot \mathrm{poly}(\varepsilon, n^{-1})$.*

Proof. In [JNV⁺22] it is shown that the game $G_{\mathcal{C}_{\mathrm{RM}}, M_{\mathrm{RM}}}$ (played using $\mathbb{F}_q$ as the base field) is (δ, ν)-robust, where ν is the uniform distribution over $\mathbb{F}_q^m \subseteq \mathcal{X}$ and δ satisfies $\delta(\varepsilon) = \mathrm{poly}(m, d) \cdot \mathrm{poly}(\varepsilon, n^{-1})$. The theorem follows by the second item of Proposition 4.3. □

6.3 The Pauli braiding test

By applying Proposition 6.1 to the tester M_{RM}, which is quantum sound by Theorem 6.3, we deduce that M'_{RM}, defined from M_{RM} as in Section 6.1, is an $O(\delta)$-sound rq-local tester for the binary code $\mathcal{C}'_{\mathrm{RM}}$, where

δ is as in Theorem 6.3. This allows us to apply Theorem 5.3 to obtain a concrete instantiation of the braiding test.[5] We call it the Pauli braiding test. For completeness, we give a description of the test in its entirety in Figure 4. To formulate the test, we make explicit the sets S_X and S_Y. For the rows of the generating matrix $E_{\mathcal{C}_{\mathrm{RM}}}$ we take an arbitrary basis of all individual degree-d polynomials, e.g. for $\alpha \in \{0, \dots, d\}^m$,

$$\mathrm{ind}_\alpha(x) = \prod_i x_i^{\alpha_i}(1 - x_i)^{d-\alpha_i} .$$

Then the x-th column of $E_{\mathcal{C}_{\mathrm{RM}}}$, $E_{\mathcal{C}_{\mathrm{RM}}} e_x$ for $x \in \mathbb{F}_q^m$, has entries $\mathrm{ind}(x) = (\mathrm{ind}_\alpha(x))_{\alpha \in \{0,\dots,d\}^m}$.

Let $S_X, S_Z \subseteq \mathbb{F}_2^k$. Sample $u_X, u_Z \in \mathbb{F}_q^m$ and $r_X, r_Z \in \mathbb{F}_q$ uniformly at random. Let $\omega_X = \mathrm{ind}(u_X)$, $\omega_Z = \mathrm{ind}(u_Z)$, and $\omega = (\omega_X, \omega_Z, r_X, r_Z) \in (\mathbb{F}_q^{(d+1)^m})^2 \times (\mathbb{F}_q)^2$. Let $\gamma = \mathrm{tr}((r_X \omega_X) \cdot (r_Z \omega_Z)) \in \mathbb{F}_2$. Execute either of the following tests with probability $1/3$ each.

1. (**Code test**) Sample $W \in \{X, Z\}$ uniformly at random, and $(S, T) \subseteq \mathbb{F}_q^{(d+1)^m} \times \mathbb{F}_2^t$ from ν'_{RM}. Sample $(i, \alpha) \in (S, T)$ uniformly at random. Send $(W, (S, T))$ to A and $(W, (i, \alpha))$ to B. Receive $a \in \mathbb{F}_2^{S \times T}$ from A and $b \in \mathbb{F}_2$ from B. Accept if and only if $M'_{\mathrm{RM}}((S, T), a) = 1$ and $a_{(i,\alpha)} = b$.
2. (**Anti-commutation test**)
   (a) If $\gamma = 0$ then sample a pair of questions (x_c, y_c) as in the commutation game. Send (x_c, ω) to A and (y_c, ω) to Bob. Accept if and only if their answers are accepted in the commutation game.
   (b) If $\gamma \neq 0$ then do the same but for the anti-commutation game.
3. (**Consistency test**) sample $W \in \{X, Z\}$ uniformly at random. Send $(W, (\omega_W, r_W))$ to A and $(x_{W,\gamma}, \omega)$ to B. Receive $a \in \mathbb{F}_2$ and $b \in \mathbb{F}_2$ respectively. Accept if and only if $a = b$.

Figure 4: The Pauli braiding test.

Theorem 6.4. *The braiding test is a* $(t(d+1)^m, \delta')$*-qubit test, for some* $\delta'(\varepsilon) = \mathrm{poly}(m, d) \cdot \mathrm{poly}(\varepsilon, n^{-1})$.

Proof. Follows from Theorem 5.3 and Theorem 6.3. □

As a corollary we obtain quantum soundness for the variant of the Pauli braiding test which is described in [JNV+20a, Section 7.3]. This is because any (synchronous) strategy for the latter can be mapped into a strategy for the former. The only difference is that in the variant from [JNV+20a], some of the answers, specifically the ones from the "Code test" associated with $\mathcal{C}_{\mathrm{RM}}$, are specified over $\mathbb{F}_q$. Of course this is equivalent to returning the binary representation of all $\mathbb{F}_q$ elements, which is what is required in the "Code test" here, for the cases where the set $T = \mathbb{F}_q$. (**Thomas:** This part is loose; I didn't check things formally and I'm not sure we want to either)

[5] (**Thomas:** "History" of PBT could be described here)

References

[BLR90] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/correcting with applications to numerical problems. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, pages 73–83, 1990. 3.3

[dlS21] Mikael de la Salle. Orthogonalization of positive operator valued measures. *arXiv preprint arXiv:2103.14126*, 2021. 4.2, 4.2

[dlS22] Mikael de la Salle. Spectral gap and stability for groups and non-local games. *arXiv preprint arXiv:2204.07084*, 2022. (document), 5.2, 5.2, 5.3, 5.3

[Gol17] Oded Goldreich. *Locally Testable Codes and Proofs*, page 370–410. Cambridge University Press, 2017. 3.1

[JNV$^+$20a] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP*= RE. *arXiv preprint arXiv:2001.04383*, 2020. (document), 5.1, 6, 6.3

[JNV$^+$20b] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. Quantum soundness of the classical low individual degree test. *arXiv preprint arXiv:2009.12982*, 2020. 4.2

[JNV$^+$22] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. Quantum soundness of testing tensor codes. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 586–597. IEEE, 2022. (document), 6, 6.2

[KV11] Julia Kempe and Thomas Vidick. Parallel repetition of entangled games. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 353–362, 2011. 4.2

[NV16] Anand Natarajan and Thomas Vidick. Robust self-testing of many-qubit states. *arXiv preprint arXiv:1610.03574*, 2016. (document), 3.3, 3.9, 3

[PRSS22] Connor Paddock, Vincent Russo, Turner Silverthorne, and William Slofstra. Arkhipov's theorem, graph minors, and linear system nonlocal games. *arXiv preprint arXiv:2205.04645*, 2022. 3.8

[Sch80] Jacob Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980. 6.2

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and Algebraic Computation*, pages 216–226, 1979. 6.2

Notes

[1] Warning: notes on