# Quantum-sound property tests for linear and affine linear functions

David Cui, Jerry Zhang

March 16, 2025

**Abstract**

Given three players with some shared function over $\mathbb{F}_2$, the BLR test certifies that their shared function is linear in constant time. More specifically, if the test succeeds with probability $1-\epsilon$, then the players' functions differ from a linear function in at most $O(\epsilon)$ inputs.

It has been shown that this three-player version of the BLR test is *quantum-sound*: it similarly certifies the presence of a linear function over $\mathbb{F}_2$ within their strategies even when the players are allowed to share nontrivial correlations through entanglement. The existence of quantum-sound protocols allows us to quantize existing classical interactive protocols and prove containment between quantum multi-prover interactive proof systems, acting as the basis of foundational results in quantum complexity theory, such as MIP $\subseteq$ MIP* and MIP* = RE.

In this paper, we generalize this property testing result and show that a variation of the linearity test over $\mathbb{F}_p$ is also quantum-sound. Additionally, we show that even without the consistency test, the presence of linear functions can be certified.

## 1 Introduction

The BLR linearity test [BLR93] gives an efficient procedure to test the linearity of an arbitrary boolean function. The linearity test works as follows: given a boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, uniformly sample two points $x, y \in \mathbb{F}_2^n$ at random and check the linearity condition $f(x)+f(y) = f(x+y)$. An analysis of this test shows that

$$\Pr_{x,y\in\mathbb{F}_2^n}[f(x)+f(y)=f(x+y)] \geq 1-\epsilon$$

if and only if $f$ is $\epsilon$-close to a linear function, in Hamming distance. One can also consider this test in the distributed setting. Let Alice, Bob, and Charlie (who cannot communicate during testing) be three adversaries who claim to have some shared linear function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ in mind. We can test if this is true by randomly choosing $x, y \in \mathbb{F}_2^n$ and sending $x$ to Alice, $y$ to Bob, and $x+y$ to Charlie and demanding them to reply with $f(x)$, $f(y)$, and $f(x+y)$ for which we test if $f(x)+f(y) = f(x+y)$. Again, an analysis of this test shows that if Alice, Bob, and Charlie pass this test with high probability, then their strategy must depend on a shared close-to-linear function. These tests naturally arise due to one of the most celebrated results in the field of computational complexity theory, the PCP theorem. A formulation of this theorem is that the class of problems decidable by one-round, two-prover MIP proof systems with $O(\log n)$-length questions and $O(1)$-length answers is equal to the complexity class NP. This general context of a multi-prover one-round interactive protocol is called a *nonlocal game* and is studied in both classical and quantum complexity theory.

In quantum theories, the provers can share a quantum resource called *entanglement*, which allows them to use a broader class of strategies to interact with the verifier. The class of problems

decidable by such one-round interactive protocols is MIP*. Despite the provers having more power, it is actually not immediately obvious that MIP should be included in MIP*. This is because although the entangled provers could certainly convince the verifier of anything that the classical provers could, it is important that they don't convince the verifier of anything more. Ito and Vidick [IV12] showed that one can design protocols which constrain the entangled provers and thus showed that MIP is contained in MIP*. Furthermore, in 2020, Ji, Natarajan, Vidick, Wright, and Yuen [JNV+21] completely characterized the power of these multi-prover interactive protocols sharing entanglement, showing that MIP* = RE building off of a long line of work [NV18, FJVY19, NW19, JNV+20, JNV+22]. The results of Ito and Vidick and Ji et al. both rely on showing that certain classical property tests still certify the presence of certain shared functions between the provers, even against quantum provers. We say that a classical property test is *quantum-sound* if it has this property.

One of the main results of [IV12] was to show that the BLR linearity test is quantum-sound. This analysis was heavily inspired by the Fourier analytic proof [BCH+96] of the classical BLR result. In this paper, we extend the soundness of the BLR linearity test to $\mathbb{F}_p$. We also prove a soundness result for a variant of the BLR linearity test which tests for *affine* linear functions.

### 1.1 Results

Our main result is extending the quantum-soundness analysis of Ito and Vidick from $\mathbb{F}_2$ to $\mathbb{F}_p$. We give an informal statement of the result below.

**Theorem 1.1** (Informal)**.** *Suppose three entangled provers succeed in the linearity test with probability $1-\epsilon$ using a symmetric strategy $(\sigma, \{A_x^a\})$. Then there exists a measurement $\{M_u\}$ independent of $x$, indexed by $u \in \mathbb{F}_p^n$, such that if we let*

$$B_x^a := \sum_{u : u \cdot x = a} M_u$$

*then the correlations produced by $\{A_x^a\}$ and $\{B_x^a\}$ are $O_p(\epsilon^{1/4})$-close.*

The precise statement is given in Theorem 3.6. We additionally show quantum soundness for an affine linearity test in $\mathbb{F}_2$.

**Theorem 1.2** (Informal)**.** *Suppose three entangled provers succeed in the affine linearity test over $\mathbb{F}_2$ with probability $1-\epsilon$ using a symmetric strategy $(\sigma, \{A_x^a\})$. Then there exists a measurement $\{M_{u,b,b'}\}$ independent of $x$, indexed by $(u, b, b') \in \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2$, such that if we let*

$$B_x^a := \sum_{u \,:\, u \cdot x - b + b' = a} M_{u,b,b'}$$

*then the correlations produced by $\{A_x^a\}$ and $\{B_x^a\}$ are $O(\epsilon^{1/4})$-close.*

The precise statement is given in Theorem 4.5.

### 1.2 Future Directions

In the classical analysis of the linearity tests, succeeding with probability $1-\epsilon$ means that the strategy is $O(\epsilon^{1/2})$ close to a linear function. The most natural question is whether our bound of $O(\epsilon^{1/4})$ is a limitation of our proof technique or whether this is an artifact of quantum correlations.

Furthermore, there is a more combinatorial proof of the BLR linearity test [Mos]. It is natural to ask whether we can "quantize" this combinatorial proof of the BLR test, just as we

did for the Fourier-analytic proof of Bellare et al. [BCH+96]. This is motivated by the fact that the proofs of the quantum soundness of the low individual degree test and tensor code test [JNV+20, JNV+22] are combinatorial in nature.

# 2 Preliminaries

## 2.1 Fourier Analysis over Finite Fields

Let $G$ be a finite abelian group $G$ of order $n$, written additively. We define the following:

**Definition 2.1** (Characters)**.** A *character* of $G$ is a homomorphism $\chi : G \to \mathbb{C}^\times$ such that for $a, b \in G$

$$\chi(a+b) = \chi(a)\chi(b).$$

In particular, $\chi(-a) = \chi(a)^{-1} = \overline{\chi(a)}$ and each $\chi(a)$ is an $n^{\text{th}}$ root of unity. Let $\widehat{G}$ be the set of all characters.

Since we will be working in $\mathbb{F}_p$ we define the characters as powers of some arbitrary $p^{th}$ root of unity $\omega$.

**Definition 2.2** (Inner product of functions)**.** Let $\mathbb{C}^G$ denote the space of functions $f : G \to \mathbb{C}$ equipped with the inner product $\langle \cdot, \cdot \rangle$ defined as:

$$\langle f, g \rangle = \mathop{\mathbb{E}}_{a \in G}[\overline{f(a)} g(a)] \qquad f, g \in \mathbb{C}^G$$

where $\mathbb{E}_{x \in S}[f(x)]$ denotes the expected value of $f(x)$ where $x$ is chosen uniformly from $S$.

**Theorem 2.3** (Lemma 3, [Kop])**.** *Any function $f \in \mathbb{C}^G$ can be written as a linear combination of characters*

$$f = \sum_{\chi \in \widehat{G}} \hat{f}(\chi)\chi$$

*where the set of $\hat{f}(\chi)$ is called the Fourier coefficients and are given by $\langle \chi, f \rangle$.*

**Theorem 2.4** (Lemma 5, [Kop])**.** *For any functions $f, g \in \mathbb{C}^G$,*

$$\langle f, g \rangle = \mathop{\mathbb{E}}_{a \in G}[\overline{f(a)} g(a)] = \sum_{\chi \in \hat{G}} \overline{\hat{f}(\chi)} \hat{g}(\chi).$$

*This is called* Plancherel's theorem. *The case where $f = g$ is called* Parseval's theorem.

## 2.2 Classical linearity testing

We introduce the following variant of the BLR linearity test:

**Definition 2.5** (Linearity test)**.** Suppose we have 3 provers $P_1, P_2, P_3$ with outputs $P_i(x) \in \mathbb{F}_p$ for each $i$. Perform either of the following with probabiltiy 1/2 each:

1. (*Consistency*) Select $x \in \mathbb{F}_p^n, \alpha \in \mathbb{F}_p \setminus \{0\}$ uniformly and at random. Query $x$ to $P_1$ and $P_2$. Accept if and only if $P_1(\alpha x) = \alpha P_2(x)$, $P_2(\alpha x) = \alpha P_3(x)$, and $P_3(\alpha x) = \alpha P_1(x)$.
2. (*Linearity*) Select $x, y \in \mathbb{F}_p^n, \alpha \in \mathbb{F}_p \setminus \{0\}$ uniformly and at random. Let $z = x - y$. Query $x$ to $P_1$, $y$ to $P_2$, and $z$ to $P_3$. Accept if and only if $P_3(\alpha z) = \alpha(P_1(x) - P_2(y))$, or equivalently $P_3(\alpha z) + \alpha P_2(y) = \alpha P_1(x)$

We now define a classical strategy:

**Definition 2.6** (Classical strategies)**.** A *classical strategy in the linearity test* $S$ is a family of probability distributions $\{p_{x,y,z}\}_{x,y,z\in\mathbb{F}_p^n}$ such that $p_{x,y,z}(a,b,c)$ is the probability that $(P_1(x),P_2(y),P_3(z)) = (a,b,c)$. Denote the probability of success of a strategy $\omega(S)$. More explicitly, we have

$$\omega(S) = \frac{1}{2}\mathop{\mathbb{E}}_x\left[\sum_a p_{x,x,x}(a,a,a)\right] + \frac{1}{2}\mathop{\mathbb{E}}_x\left[\sum_a p_{x,y,x+y}(a,b,a+b)\right].$$

We now focus on a few relevant classical strategies: Call a classical strategy *deterministic* if each $p_{x,y,z}$ is a point distribution, or that there exist functions $f, g$, and $h$ such that

$$p_{x,y,z}(a,b,c) = \delta_{f(x)=a}\delta_{g(y)=a}\delta_{h(z)=a}$$

where $\delta_{x=y}$ is equal to 1 if $x = y$ and 0 otherwise.

Furthermore, a *classical probabilistic strategy* is a classical strategy such that there exist families of probability distributions $\{q_x\}$, $\{r_y\}$, $\{s_z\}$ such that

$$p_{x,y,z}(a,b,c) = q_x(a)r_y(b)s_z(c).$$

Finally, a *classical strategy with shared randomness* is a family of probability distributions $\{p_{x,y,z}\}_{x,y,z\in\mathbb{F}_p^n}$ such that

$$p_{x,y,z}(a,b,c) = \sum_i \lambda_i \cdot p^i_{x,y,z}(a,b,c)$$

where $\{p^i_{x,y,z}\}$ is a classical probabilistic strategies. More explicitly, $p^i_{x,y,z}(a,b,c) = q^i_x(a)r^i_y(b)s^i_z(c)$ for probability distributions $\{q^i_x\},\{r^i_y\},\{s^i_z\}$ and $\lambda_i \geq 0$ for each $i$, with $\sum_i \lambda_i = 1$.

## 2.3 Nonlocal Games and Correlations

In this paper, there will be two relevant types of measurements. Let $\mathcal{H}$ be a Hilbert space. We then have the following:

**Definition 2.7** (PVM measurement)**.** A *Projective-Valued Measure* or PVM is a collection of Hermitian operators $\{\Pi_a\}_{a\in A}$ on $\mathcal{H}$ such that $\Pi_i\Pi_j = \delta_{i=j}\Pi_i$ and $\sum_a \Pi_a = I$. Each $\Pi_i$ is called a *projector*.

**Definition 2.8** (POVM measurement)**.** A *Positive Operator-Valued Measure* or POVM is a collection of positive semi-definite ($A$ is positive semi-definite if there exists some $B$ such that $A = B^*B$) operators $\{P_a\}_{a\in A}$ on $\mathcal{H}$ such that $\sum_a P_a = I$.

We now introduce the idea of an entangled strategy.

**Definition 2.9** (Entangled strategies)**.** An *entangled strategy in the $r$-prover linearity test* $(\rho, \{(A_i)^a_x\}_{i\in[r]})$ is given by the following:

- Finite dimensional Hilbert spaces $\mathcal{P}_1,\ldots,\mathcal{P}_r$
- density operator $\rho \in \mathcal{L}(\mathcal{P}_1\otimes\cdots\otimes\mathcal{P}_r)$
- measurements $\{(A_i)^a_x\}_{a\in\mathbb{F}}$ on $\mathcal{P}_i$ for each $x\in\mathbb{F}^n$ and $i\in[r]$

An entangled strategy induces a family of probability distributions $\{p_{x_1,\ldots,x_r}\}_{x_1,\ldots,x_r\in\mathbb{F}^n}$

$$p_{x_1,\ldots,x_r}(a_1,\ldots,a_r) = \mathrm{Tr}\left(\left(\bigotimes_i (A_i)^{a_i}_{x_i}\right)\rho\right).$$

We say a strategy is *symmetric* if $\mathcal{P}_1 \simeq \cdots \simeq \mathcal{P}_r$ and $(A_1)^a_x = \cdots = (A_r)^a_x$ for each $x$ and $a$, and $\rho$ is invariant with respect to arbitrary permutation of the registers $\mathcal{P}_1,\ldots,\mathcal{P}_r$. Furthermore, we call a strategy *projective* if each measurement is a PVM (i.e. each operator $(A_i)^a_x$ is a projector).

We will be working with the case in which $r = 3$ and $\mathbb{F} \cong \mathbb{F}_p$ for some prime $p$ in the following sections. We extend the ideas of discrete Fourier analysis. Let $\{A_x^a\}_{a \in \mathbb{F}_p}$ be a PVM. Define

$$A_x \coloneqq \sum_{i=0}^{p-1} A_x^i \omega^i$$

where $\omega$ is some $p$th root of unity. Note that $A_x$ is unitary (i.e. $(A_x)^* = (A_x)^{-1}$), and that $(A_x)^k = \sum_i A_x^i \omega^{ki}$. For $u \in \mathbb{F}_p^n$,

$$\hat{A}_u^k \coloneqq \mathop{\mathbb{E}}_x[\overline{\omega^{ku \cdot x}}(A_x)^k] = \mathop{\mathbb{E}}_x[\omega^{-ku \cdot x}(A_x)^k]$$

Notice that a variant of Parseval still holds:

$$\sum_{u \in \mathbb{F}_p^n} (\hat{A}_u^k)^* (\hat{A}_u^k) = \sum_{u \in \mathbb{F}_p^n} (\hat{A}_u^k)(\hat{A}_u^k)^* = \sum_{u \in \mathbb{F}_p^n} \mathop{\mathbb{E}}_{x,y} \left[\omega^{-ku \cdot (x-y)} (A_x)^k (A_y)^{-k}\right] = \mathop{\mathbb{E}}_x[(A_x)^k (A_x)^{-k}] = I$$

as $x, y$ are sampled independently over the same distribution. A few notes about notation: For any density operator $\sigma \in \mathcal{L}(\mathcal{P}_1 \otimes \cdots \otimes \mathcal{P}_r)$, we let $\rho$ be the reduced density operator on the first register. We also let

$$\|A\|_\sigma^2 \coloneqq \mathrm{Tr}\,(AA^*\sigma)$$

This semi-norm satisfies the Cauchy-Schwarz inequality: for any sequences of matrices $M_i, N_i$,

$$\sum_i \mathrm{Tr}\,(M_i N_i^* \sigma) \leq \sqrt{\sum_i \|M_i\|_\sigma} \sqrt{\sum_i \|N_i\|_\sigma}.$$

## 2.4 Distance Measures

We consider two notions of distance between strategies:

**Definition 2.10** (Total variational distance)**.** The *total variational distance* between two strategies $p = \{p_{x,y,z}\}_{x,y,z \in \mathbb{F}_p^n}$ and $q = \{q_{x,y,z}\}_{x,y,z \in \mathbb{F}_p^n}$ is defined as

$$\|p - q\|_{\mathrm{TV}} = \frac{1}{2} \mathop{\mathbb{E}}_{x,y,z \sim \mathbb{F}_p^n} \left[\sum_{a,b,c} |p_{x,y,z}(a,b,c) - q_{x,y,z}(a,b,c)|\right].$$

**Lemma 2.11.** *Given two strategies $p = \{p_{x,y,z}\}_{x,y,z \in \mathbb{F}_p^n}$ and $q = \{q_{x,y,z}\}_{x,y,z \in \mathbb{F}_p^n}$,*

$$\|p - q\|_{TV} = \mathop{\mathbb{E}}_{x,y,z} \left[\max_{S \subseteq \mathbb{F}_p^3} \left\{\left|\sum_{(a,b,c) \in S} p_{x,y,z}(a,b,c) - q_{x,y,z}(a,b,c)\right|\right\}\right].$$

**Definition 2.12** ($\delta$-closeness)**.** Given entangled strategies $(\sigma, \{A_x^a\})$ and $(\sigma, \{\tilde{A}_x^a\})$, we say that they are *$\delta$-close* if

$$d_\sigma(A, \tilde{A}) \coloneqq \left(\mathop{\mathbb{E}}_x \left[\sum_a \mathrm{Tr}\left((A_x^a - \tilde{A}_x^a)^2 \sigma\right)\right]\right)^{1/2} \leq \delta$$

with appropriate padding of the registers.

We may relate the two measures of distance with the following lemma:

**Lemma 2.13.** *Given a projective, symmetric entangled strategy $(\sigma, \{A_x^a\})$ and a symmetric entangled strategy $(\sigma, \{B_x^a\})$ where each $B_x^a$ is a POVM, with corresponding probability distributions $\{p_{x,y,z}\}_{x,y,z\in\mathbb{F}_p^n}$ and $\{\ell_{x,y,z}\}_{x,y,z\in\mathbb{F}_p^n}$ respectively,*

$$\|p-\ell\|_{\mathrm{TV}} \leq 3d_\rho(A,B).$$

*Proof.* By definition and Lemma 2.11,

$$\begin{aligned}\|p-\ell\|_{\mathrm{TV}} &= \frac{1}{2}\mathop{\mathbb{E}}_{x,y,z}\left[\sum_{a,b,c}\left|\mathrm{Tr}\left((A_x^a\otimes A_y^b\otimes A_z^c)\sigma\right)-\mathrm{Tr}\left((B_x^a\otimes B_y^b\otimes B_z^c)\sigma\right)\right|\right]\\ &= \mathop{\mathbb{E}}_{x,y,z}\left[\max_S\left\{\left|\sum_{(a,b,c)\in S}\mathrm{Tr}\left((A_x^a\otimes A_y^b\otimes A_z^c)\sigma\right)-\mathrm{Tr}\left((B_x^a\otimes B_y^b\otimes B_z^c)\sigma\right)\right|\right\}\right].\end{aligned}$$

Notice that we may decompose our differences of traces on each register, yielding

$$\begin{aligned}&\mathrm{Tr}\left((A_x^a\otimes A_y^b\otimes A_z^c)\sigma\right)-\mathrm{Tr}\left((B_x^a\otimes B_y^b\otimes B_z^c)\sigma\right)\\ &\quad=\mathrm{Tr}\left(\left[((A_x^a-B_x^a)\otimes A_y^b\otimes A_z^c)+(B_x^a\otimes(A_y^b-B_y^b)\otimes A_z^c)+(B_x^a\otimes B_y^b\otimes(A_z^c-B_z^c))\right]\sigma\right).\end{aligned}$$

Thus by triangle inequality, we have

$$\begin{aligned}\|p-\ell\|_{\mathrm{TV}} \leq \mathop{\mathbb{E}}_{x,y,z}\max_S&\left|\sum_{(a,b,c)\in S}\mathrm{Tr}\left(((A_x^a-B_x^a)\otimes A_y^b\otimes A_z^c)\sigma\right)\right|+\left|\sum_{(a,b,c)\in S}\mathrm{Tr}\left((B_x^a\otimes(A_y^b-B_y^b)\otimes A_z^c)\sigma\right)\right|\\ &+\left|\sum_{(a,b,c)\in S}\mathrm{Tr}\left((B_x^a\otimes B_y^b\otimes(A_z^c-B_z^c))\sigma\right)\right|.\end{aligned}$$

Since the strategy is symmetric, we may permute the registers such that the difference is in the first register and apply Cauchy Schwarz to get

$$\begin{aligned}\|p-\ell\|_{\mathrm{TV}} &\leq \mathop{\mathbb{E}}_{x,y,z}\left[\max_S\sqrt{\sum_{(a,b,c)\in S}\mathrm{Tr}\left((A_x^a-B_x^a)^2\rho\right)}\sqrt{\sum_{(a,b,c)\in S}\mathrm{Tr}\left((I\otimes A_y^b\otimes A_z^c)\sigma\right)}\right.\\ &\quad+\sqrt{\sum_{(a,b,c)\in S}\mathrm{Tr}\left((A_x^a-B_x^a)^2\rho\right)}\sqrt{\sum_{(a,b,c)\in S}\mathrm{Tr}\left((I\otimes(B_y^b)^2\otimes A_z^c)\sigma\right)}\\ &\quad\left.+\sqrt{\sum_{(a,b,c)\in S}\mathrm{Tr}\left((A_x^a-B_x^a)^2\rho\right)}\sqrt{\sum_{(a,b,c)\in S}\mathrm{Tr}\left((I\otimes(B_y^b)^2\otimes(B_z^c)^2)\sigma\right)}\right]\\ &\leq 3\mathop{\mathbb{E}}_{x,y,z}\left[\sqrt{\sum_a\mathrm{Tr}\left((A_x^a-B_x^a)^2\rho\right)}\right].\end{aligned}$$

The secpnd inequality comes from the fact that $\sum_a A_x^a = I$ and that each $B_y^b$ is positive semidefinite, which implies that

$$\sum_b (B_y^b)^2 \leq \sum_{b,b'} B_y^b B_y^{b'} = \left(\sum_b B_y^b\right)^2 = I.$$

We finish with Cauchy Schwarz to get

$$\|p - \ell\|_{\mathrm{TV}} \leq 3\sqrt{\mathop{\mathbb{E}}_{x}\left[\sum_{a} \mathrm{Tr}\left((A_x^a - B_x^a)^2\rho\right)\right]} \tag{2.1}$$

$$= 3d_\rho(A, B), \tag{2.2}$$

as desired. □

## 3 Linearity testing over $\mathbb{F}_p$

In [IV12], Ito and Vidick prove that for symmetric strategies between the three provers, if the provers pass the linearity test with high probability, then they must be using a strategy which is close to a classical mixture of true linear functions, or a classical strategy with shared randomness. More precisely,

**Theorem 3.1** ([Vid], Theorem 4)**.** *Suppose three entangled provers succeed in the linearity test with probability $1 - \epsilon$ using a symmetric strategy $(\sigma, \{A_x^a\})$. Then there exists a measurement $\{M_u^k\}$ independent of $x$, where $M_u^k$ corresponds to outcome $u \in \mathbb{F}_2^n$, such that if we let*

$$B_x^a := \sum_{u : u \cdot x = a} M_u^k$$

*then*

$$(d_\rho(A, B))^2 = \mathop{\mathbb{E}}_{x}\left[\sum_{a \in \{0,1\}} \mathrm{Tr}\left((A_x^a - B_x^a)^2\rho\right)\right] \leq 12\sqrt{\epsilon}.$$

For them, it suffices to consider symmetric strategies as a result of the following reduction.

**Lemma 3.2** ([IV12], Lemma 7)**.** *Given a nonlocal game and an $r$-player strategy $(\rho, \{A_x^a\}_r)$ that succeeds in it with probability $p$, there exists a symmetric strategy $(\rho', \{A_x'^a\}_r)$ with success probability at least $p$.*

This is a reduction we shall use in this section as well. The results of this section generalizes the above by considering the linearity test in $\mathbb{F}_p^n$, using a Fourier analytic technique similar to the one used in Vidick's proof.

We begin by first showing that succeeding at the linearity test implies a lower bound on some function of the Fourier transform of the operators.

**Lemma 3.3.** *If the three entangled provers succeed in the lineraity test with probability $1 - \epsilon$ using a symmetric strategy $(\sigma, \{A_x^a\})$, then*

$$\mathop{\mathbb{E}}_{\alpha \in \mathbb{F}_p}\left[\sum_{k=1}^{p-1} \sum_{u \in \mathbb{F}_p^n} \mathrm{Tr}\left((\hat{A}_u^{k\alpha})^* \otimes \hat{A}_u^k \otimes I)\sigma\right)\right] \geq p(1 - 2\epsilon) - 1,$$

*and*

$$\mathop{\mathbb{E}}_{\alpha \in \mathbb{F}_p}\left[\sum_{k=1}^{p-1} \sum_{u \in \mathbb{F}_p^n} \mathrm{Tr}\left((\hat{A}_u^{k\alpha})^* \otimes \hat{A}_u^{k\alpha} \otimes \hat{A}_u^k)\sigma\right)\right] \geq p(1 - 2\epsilon) - 1.$$

*Proof.* The probability that the provers succeed in the consistency and linearity parts of the test must each be at least $1 - 2\epsilon$. Then,

$$\Pr[\text{consistent}] = \mathop{\mathbb{E}}_{x\in\mathbb{F}_p^n,\alpha\in\mathbb{F}_p}\left[\sum_{a\in\mathbb{F}_p}\operatorname{Tr}\left((A_x^a\otimes A_{\alpha x}^{\alpha a}\otimes I)\sigma\right)\right]\geq 1-2\epsilon$$

$$\Pr[\text{linear}] = \mathop{\mathbb{E}}_{x,y\in\mathbb{F}_p^n,\alpha\in\mathbb{F}_p}\left[\sum_{a,b\in\mathbb{F}_p}\operatorname{Tr}\left((A_x^a\otimes A_y^b\otimes A_{\alpha(x-y)}^{\alpha(a-b)})\sigma\right)\right]\geq 1-2\epsilon$$

Furthermore, we must have that

$$\begin{aligned}
&\sum_{k=1}^{p-1}\operatorname{Tr}\left(((A_x)^{-\alpha k}\otimes(A_{\alpha x})^k\otimes I)\sigma\right)\\
&=(p-1)\sum_{\alpha a=b}\operatorname{Tr}\left((A_x^a\otimes A_{\alpha x}^b\otimes I)\sigma\right)+\sum_{k=1}^{p-1}\sum_{a\neq b}\omega^{k(\alpha a-b)}\operatorname{Tr}\left((A_x^a\otimes A_{\alpha x}^b\otimes I)\sigma\right)\\
&=(p-1)\sum_{\alpha a=b}\operatorname{Tr}\left((A_x^a\otimes A_{\alpha x}^b\otimes I)\sigma\right)-\sum_{\alpha a\neq b}\operatorname{Tr}\left((A_x^a\otimes A_{\alpha x}^b\otimes I)\sigma\right).
\end{aligned}$$

as $\sum_{k=1}^{p-1}\omega^{ki}=-1$ for $i\neq 0$. Note that since $\sum_{a,b}A_x^a\otimes A_y^b=\sum_a A_x^a\otimes\sum_b A_y^b=I$, adding 1 to both sides gives

$$p\sum_{a\in\mathbb{F}_p}\operatorname{Tr}\left((A_x^a\otimes A_{\alpha x}^{\alpha a}\otimes I)\sigma\right)=1+\sum_{k=1}^{p-1}\operatorname{Tr}\left(((A_x)^{-\alpha k}\otimes(A_{\alpha x})^k\otimes I)\sigma\right).$$

Similarly,

$$\begin{aligned}
&\sum_{k=1}^{p-1}\operatorname{Tr}\left(((A_x)^{-\alpha k}\otimes(A_y)^{\alpha k}\otimes(A_{\alpha(x-y)})^k)\sigma\right)\\
&=(p-1)\sum_{a,b\in\mathbb{F}_p}\operatorname{Tr}\left((A_x^a\otimes A_y^b\otimes A_{\alpha(x-y)}^{\alpha(a-b)})\sigma\right)+\sum_{k=1}^{p-1}\sum_{\alpha(a-b)\neq c}\omega^{k(-\alpha a+\alpha b+c)}\operatorname{Tr}\left((A_x^a\otimes A_y^b\otimes A_{\alpha(x-y)}^c)\sigma\right)\\
&=(p-1)\sum_{a,b\in\mathbb{F}_p}\operatorname{Tr}\left((A_x^a\otimes A_y^b\otimes A_{\alpha(x-y)}^{\alpha(a-b)})\sigma\right)-\sum_{c\neq\alpha a-\alpha b}\operatorname{Tr}\left((A_x^a\otimes A_y^b\otimes A_{\alpha(x-y)}^c)\sigma\right)\\
&\implies p\sum_{a,b\in\mathbb{F}_p}\operatorname{Tr}\left((A_x^a\otimes A_y^b\otimes A_{\alpha(x-y)}^{\alpha(a-b)})\sigma\right)=1+\sum_{k=1}^{p-1}\operatorname{Tr}\left(((A_x)^{-\alpha k}\otimes(A_y)^{\alpha k}\otimes(A_{\alpha(x-y)})^k)\sigma\right).
\end{aligned}$$

Thus,

$$\mathop{\mathbb{E}}_{\alpha}\left[\sum_{k=1}^{p-1}\mathop{\mathbb{E}}_{x}\left[\operatorname{Tr}\left(((A_x)^{-\alpha k}\otimes(A_{\alpha x})^k\otimes I)\sigma\right)\right]\right]\geq p(1-2\epsilon)-1$$

$$\mathop{\mathbb{E}}_{\alpha}\left[\sum_{k=1}^{p-1}\mathop{\mathbb{E}}_{x,y}\left[\operatorname{Tr}\left(((A_x)^{-\alpha k}\otimes(A_y)^{\alpha k}\otimes(A_{\alpha(x-y)})^k)\sigma\right)\right]\right]\geq p(1-2\epsilon)-1.$$

Now, by definition, we have

$$\sum_u\operatorname{Tr}\left(((\hat{A}_u^{\alpha k})^*\otimes\hat{A}_u^k\otimes I)\sigma\right)=\mathop{\mathbb{E}}_{x,y}\left[\sum_u\omega^{ku\cdot(-\alpha x+y)}\operatorname{Tr}\left(((A_x)^{-\alpha k}\otimes(A_y)^k\otimes I)\sigma\right)\right].$$

For $-\alpha x + y \neq 0$, notice that $u \cdot (-\alpha x + y)$ reaches each residue mod $p$ the same number of times summing across $u$. Thus,

$$\mathop{\mathbb{E}}_{x,y}\left[\sum_u \omega^{ku\cdot(-\alpha x+y)}\mathrm{Tr}\left(((A_x)^{-\alpha k}\otimes(A_y)^k\otimes I)\sigma\right)\right] = \mathop{\mathbb{E}}_{x,y}\left[p^n\delta_{\alpha x=y}\mathrm{Tr}\left(((A_x)^{-\alpha k}\otimes(A_y)^k\otimes I)\sigma\right)\right]$$
$$= \mathop{\mathbb{E}}_{x}\left[\mathrm{Tr}\left(((A_x)^{-\alpha k}\otimes(A_{\alpha x})^k\otimes I)\sigma\right)\right].$$

Similarly, we have

$$\sum_u \mathrm{Tr}\left(((\hat{A}_u^{\alpha k})^*\otimes\hat{A}_u^{\alpha k}\otimes\hat{A}_u^k)\sigma\right) = \mathop{\mathbb{E}}_{x,y,z}\left[\sum_u \omega^{ku\cdot(-\alpha x+\alpha y+z)}\mathrm{Tr}\left(((A_x)^{-\alpha k}\otimes(A_y)^{-\alpha k}\otimes(A_z)^k)\sigma\right)\right]$$
$$= \mathop{\mathbb{E}}_{x,y,z}\left[p^n\delta_{z=\alpha(x-y)}\mathrm{Tr}\left(((A_x)^{-\alpha k}\otimes(A_y)^{-\alpha k}\otimes(A_z)^k)\sigma\right)\right]$$
$$= \mathop{\mathbb{E}}_{x,y}\left[\mathrm{Tr}\left(((A_x)^{-\alpha k}\otimes(A_y)^{\alpha k}\otimes(A_{\alpha(x-y)})^k)\sigma\right)\right].$$

Substituting in to our bounds above give

$$\mathop{\mathbb{E}}_{\alpha}\left[\sum_{k=1}^{p-1}\sum_{u\in\mathbb{F}_p^n}\mathrm{Tr}\left(((\hat{A}_u^{\alpha k})^*\otimes\hat{A}_u^k\otimes I)\sigma\right)\right] \geq p(1-2\epsilon)-1$$
$$\mathop{\mathbb{E}}_{\alpha}\left[\sum_{k=1}^{p-1}\sum_{u\in\mathbb{F}_p^n}\mathrm{Tr}\left(((\hat{A}_u^{\alpha k})^*\otimes\hat{A}_u^{\alpha k}\otimes\hat{A}_u^k)\sigma\right)\right] \geq p(1-2\epsilon)-1,$$

as desired. □

**Lemma 3.4.** *If*

$$\mathop{\mathbb{E}}_{\alpha}\left[\sum_{k=1}^{p-1}\sum_{u\in\mathbb{F}_p^n}\mathrm{Tr}\left(((\hat{A}_u^{\alpha k})^*\otimes\hat{A}_u^k\otimes I)\sigma\right)\right] \geq \beta,$$

*then*

$$\mathop{\mathbb{E}}_{\alpha}\left[\sum_{k=1}^{p-1}\sum_{u\in\mathbb{F}_p^n}\|\hat{A}_u^{\alpha k}\otimes I\otimes I - I\otimes\hat{A}_u^k\otimes I\|_\sigma^2\right] \leq 2(p-1)-2\beta$$

*Proof.* Expanding the product gives

$$\mathop{\mathbb{E}}_{\alpha}\left[\sum_{k=1}^{p-1}\sum_{u\in\mathbb{F}_p^n}\|\hat{A}_u^k\otimes I\otimes I - I\otimes\hat{A}_u^k\otimes I\|_\sigma^2\right] = \mathop{\mathbb{E}}_{\alpha}\left[\sum_{k=1}^{p-1}\sum_{u\in\mathbb{F}_p^n}\|\hat{A}_u^{\alpha k}\|_\rho^2 + \|\hat{A}_u^k\|_\rho^2 - 2\mathrm{Tr}\left(((\hat{A}_u^{\alpha k})^*\otimes\hat{A}_u^k\otimes I)\sigma\right)\right]$$

as $\mathbb{E}_\alpha\left[\sum_k\sum_u \mathrm{Tr}\left(((\hat{A}_u^{\alpha k})^*\otimes\hat{A}_u^k\otimes I)\sigma\right)\right] = \mathbb{E}_\alpha\left[\sum_k\sum_u \mathrm{Tr}\left((\hat{A}_u^{\alpha k}\otimes(\hat{A}_u^k)^*\otimes I)\sigma\right)\right]$ since our trace is real. By Parseval's, $\sum_u\|\hat{A}_u^{\alpha k}\|_\rho^2 = 1$ for $\alpha\neq 0$, giving us

$$\mathop{\mathbb{E}}_{\alpha}\left[\sum_{k=1}^{p-1}\sum_{u\in\mathbb{F}_p^n} 2 - 2\mathrm{Tr}\left(((\hat{A}_u^{\alpha k})^*\otimes\hat{A}_u^k\otimes I)\sigma\right)\right] \leq 2(p-1)-2\beta,$$

as desired. □

**Lemma 3.5.** *Given that*

$$\mathop{\mathbb{E}}_{\alpha}\left[\sum_{k=1}^{p-1}\sum_{u\in\mathbb{F}_p^n}\|\hat{A}_u^{\alpha k}\otimes I\otimes I - I\otimes\hat{A}_u^k\otimes I\|_\sigma^2\right]\leq\beta_1$$

*and*

$$\mathop{\mathbb{E}}_{\alpha}\left[\sum_{k=1}^{p-1}\sum_{u\in\mathbb{F}_p^n}\operatorname{Tr}\left(((\hat{A}_u^{\alpha k})^*\otimes\hat{A}_u^{\alpha k}\otimes\hat{A}_u^k)\sigma\right)\right]\geq\beta_2,$$

*we have*

$$\mathop{\mathbb{E}}_{\alpha}\left[\sum_{k=1}^{p-1}\sum_{u\in\mathbb{F}_p^n}\operatorname{Tr}\left((\hat{A}_u^{\alpha k})^*\hat{A}_u^{\alpha k}\hat{A}_u^k\rho\right)\right]\geq\beta_2-2\sqrt{(p-1)\beta_1}.$$

*Proof.* We consider the following difference of traces:

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\operatorname{Tr}\left(\left((\hat{A}_u^{\alpha k})^*\hat{A}_u^{\alpha k}\hat{A}_u^k\otimes I\otimes I-(\hat{A}_u^{\alpha k})^*\otimes\hat{A}_u^{\alpha k}\otimes\hat{A}_u^k\right)\sigma\right)\right]\\
&=\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\operatorname{Tr}\left(\left((\hat{A}_u^{\alpha k})^*\hat{A}_u^{\alpha k}\otimes I\otimes I\right)\left(\hat{A}_u^k\otimes I\otimes I-I\otimes\hat{A}_u^{\alpha k}\otimes I\right)\sigma\right)\right]\\
&\quad+\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\operatorname{Tr}\left(\left((\hat{A}_u^{\alpha k})^*\otimes\hat{A}_u^{\alpha k}\otimes I\right)\left(\hat{A}_u^{\alpha k}\otimes I\otimes I-I\otimes I\otimes\hat{A}_u^k\right)\sigma\right)\right].
\end{aligned}$$

Separating the product using Cauchy-Schwarz gives

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\operatorname{Tr}\left(\left((\hat{A}_u^{\alpha k})^*\hat{A}_u^{\alpha k}\hat{A}_u^k\otimes I\otimes I-(\hat{A}_u^{\alpha k})^*\otimes\hat{A}_u^{\alpha k}\otimes\hat{A}_u^k\right)\sigma\right)\right]\\
&\leq\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\left\|(\hat{A}_u^{\alpha k})^*\hat{A}_u^{\alpha k}\otimes I\otimes I\right\|_\sigma^2\right]^{1/2}\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\left\|\hat{A}_u^k\otimes I\otimes I-I\otimes\hat{A}_u^{\alpha k}\otimes I\right\|_\sigma^2\right]^{1/2}\\
&\quad+\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\left\|(\hat{A}_u^{\alpha k})^*\otimes\hat{A}_u^{\alpha k}\otimes I\right\|_\sigma^2\right]^{1/2}\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\left\|\hat{A}_u^{\alpha k}\otimes I\otimes I-I\otimes I\otimes\hat{A}_u^k\right\|_\sigma^2\right]^{1/2}.
\end{aligned}$$

Since our strategy is symmetric, $\hat{A}_u^{\alpha k}\otimes I\otimes I-I\otimes I\otimes\hat{A}_u^k=I\otimes\hat{A}_u^{\alpha k}\otimes I-\hat{A}_u^k\otimes I\otimes I$, giving us by our bounds

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\left\|(\hat{A}_u^{\alpha k})^*\hat{A}_u^{\alpha k}\otimes I\otimes I\right\|_\sigma^2\right]^{1/2}\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\left\|\hat{A}_u^k\otimes I\otimes I-I\otimes\hat{A}_u^{\alpha k}\otimes I\right\|_\sigma^2\right]^{1/2}\\
&\quad+\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\left\|(\hat{A}_u^{\alpha k})^*\otimes\hat{A}_u^{\alpha k}\otimes I\right\|_\sigma^2\right]^{1/2}\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\left\|\hat{A}_u^{\alpha k}\otimes I\otimes I-I\otimes I\otimes\hat{A}_u^k\right\|_\sigma^2\right]^{1/2}\\
&\leq\sqrt{\beta_1}\left(\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\operatorname{Tr}\left(((\hat{A}_u^{\alpha k})^*\hat{A}_u^{\alpha k})^2\rho\right)\right]^{1/2}+\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\operatorname{Tr}\left(\left((\hat{A}_u^{\alpha k})^*\hat{A}_u^{\alpha k}\otimes\hat{A}_u^{\alpha k}(\hat{A}_u^{\alpha k})^*\otimes I\right)\sigma\right)\right]^{1/2}\right).
\end{aligned}$$

Since $\operatorname{Tr}(MN)\leq\operatorname{Tr}(M)\|N\|_{op}$ (where $\|\cdot\|_{op}$ denotes the operator norm) for positive semi-definite $M$, we have

$$\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\operatorname{Tr}\left(((\hat{A}_u^{\alpha k})^*\hat{A}_u^{\alpha k})^2\rho\right)\right]^{1/2}+\mathop{\mathbb{E}}_{\alpha}\left[\sum_k\sum_u\operatorname{Tr}\left(\left((\hat{A}_u^{\alpha k})^*\hat{A}_u^{\alpha k}\otimes\hat{A}_u^{\alpha k}(\hat{A}_u^{\alpha k})^*\otimes I\right)\sigma\right)\right]^{1/2}$$

$$\leq \mathop{\mathbb{E}}_{\alpha}\left[\sum_k \sum_u \mathrm{Tr}\left((\hat{A}_u^{\alpha k})^* \hat{A}_u^{\alpha k}\rho\right) \|(\hat{A}_u^{\alpha k})^* \hat{A}_u^{\alpha k}\|_{op}\right]^{1/2} + \mathop{\mathbb{E}}_{\alpha}\left[\sum_k \sum_u \mathrm{Tr}\left(\hat{A}_u^{\alpha k}(\hat{A}_u^{\alpha k})^*\rho\right) \|(\hat{A}_u^{\alpha k})^* \hat{A}_u^{\alpha k}\|_{op}\right]^{1/2}$$
$$\leq 2\sqrt{(p-1)},$$

where the final inequality results because $\|(\hat{A}_u^{\alpha k})^* \hat{A}_u^{\alpha k}\|_{op} \leq 1$ and Parseval's. To conclude, notice our bound holds regardless of a sign in front of the first expression. Hence,

$$\sum_{k=1}^{p-1} \sum_{u \in \mathbb{F}_p^n} \mathrm{Tr}\left((\hat{A}_u^{\alpha k})^* \hat{A}_u^{\alpha k} \hat{A}_u^k \rho\right) \geq \sum_k \sum_u \mathrm{Tr}\left(\left(\hat{A}_u^{\alpha k}\right)^* \otimes \hat{A}_u^{\alpha k} \otimes \hat{A}_u^k\right)\sigma\right) - 2\sqrt{(p-1)\beta_1}$$
$$\geq \beta_2 - 2\sqrt{(p-1)\beta_1},$$

as desired. □

We now prove our main result.

**Theorem 3.6.** *Suppose three entangled provers succeed in the linearity test with probability 1-$\epsilon$ using a symmetric strategy $(\sigma, \{A_x^a\})$. Then there exists a measurement $\{M_u\}$ for $u \in \mathbb{F}_p^n$ such that if we let*

$$B_x^a \coloneqq \sum_{u : u \cdot x = a} M_u$$

*then*

$$(d_\rho(A,B))^2 \leq 4\left(1 + 2\sqrt{\frac{p-1}{p}}\right)\sqrt{\epsilon}.$$

*Proof.* Define a measurement $\{M_u\} \coloneqq \left\{\mathbb{E}_\alpha\left[(\hat{A}_u^\alpha)^* \hat{A}_u^\alpha\right]\right\}$ This is a POVM measurement: $M_u$ is positive semi-definite and Hermitian, and Parseval's identity shows that $\sum_u M_u = I$. Let $C_x^k = (A_x)^k - \sum_u \omega^{ku\cdot x} M_u$. Taking the Fourier transform gives

$$\begin{aligned}\hat{C}_u^k &= \hat{A}_u^k - \mathop{\mathbb{E}}_x\left[\omega^{-ku\cdot x}\sum_v \omega^{kv\cdot x} M_v\right] \\ &= \hat{A}_u^k - \mathop{\mathbb{E}}_x\left[\sum_v \omega^{k(v-u)\cdot x} M_v\right] \\ &= \hat{A}_u^k - M_u.\end{aligned}$$

Summing over $\|C_x^k\|_\rho^2$ gives

$$\begin{aligned}\mathop{\mathbb{E}}_x\left[\sum_{k=1}^{p-1}\left\|(A_x)^k - \sum_u \omega^{ku\cdot x} M_u\right\|_\rho^2\right] &= \mathop{\mathbb{E}}_x\left[\sum_{k=1}^{p-1}\|C_x^k\|_\rho^2\right] = \sum_{k=1}^{p-1}\sum_u \|\hat{C}_u^k\|_\rho^2 \\ &= \sum_{k=1}^{p-1}\sum_u \|\hat{A}_u^k - M_u\|_\rho^2 \\ &= \sum_{k=1}^{p-1}\sum_u \mathrm{Tr}\left(((\hat{A}_u^k)^*\hat{A}_u^k - M_u\hat{A}_u^k - (\hat{A}_u^k)^* M_u + M_u^2)\rho\right).\end{aligned}$$

Extracting an $M_u$ using the operator norm and noting that $\|M_u\| \leq 1$ gives

$$\sum_{k=1}^{p-1}\sum_u \mathrm{Tr}\left(((\hat{A}_u^k)^*\hat{A}_u^k - M_u\hat{A}_u^k - (\hat{A}_u^k)^* M_u + M_u^2)\rho\right)$$

$$
\begin{aligned}
&\leq \sum_{k=1}^{p-1} 1 - 2\sum_u \mathrm{Tr}\left(M_u \hat{A}_u^k \rho\right) + \sum_u \|M_u\|_{op} \mathrm{Tr}\left(M_u \rho\right) \\
&\leq \sum_{k=1}^{p-1} 2 - 2\sum_u \mathrm{Tr}\left(\mathop{\mathbb{E}}_\alpha \left[(\hat{A}_u^\alpha)^* \hat{A}_u^\alpha\right] \hat{A}_u^k \rho\right) \\
&\leq 2(p-1) - 2\sum_{k=1}^{p-1}\sum_u \mathrm{Tr}\left(\mathop{\mathbb{E}}_\alpha \left[(\hat{A}_u^\alpha)^* \hat{A}_u^\alpha\right] \hat{A}_u^k \rho\right).
\end{aligned}
$$

Since $\alpha \mapsto \alpha k$ is a bijection in $\mathbb{F}_p \setminus \{0\}$, we may write $\mathbb{E}_\alpha \left[(\hat{A}_u^\alpha)^* \hat{A}_u^\alpha\right] = \mathbb{E}_\alpha \left[(\hat{A}_u^{\alpha k})^* \hat{A}_u^{\alpha k}\right]$ for arbitrary $k$, giving us

$$
\begin{aligned}
2(p-1) - 2\sum_{k=1}^{p-1}\sum_u \mathrm{Tr}\left(\mathop{\mathbb{E}}_\alpha \left[(\hat{A}_u^\alpha)^* \hat{A}_u^\alpha\right] \hat{A}_u^k \rho\right) &= 2(p-1) - 2\mathop{\mathbb{E}}_\alpha \left[\sum_{k=1}^{p-1}\sum_u \mathrm{Tr}\left((\hat{A}_u^{\alpha k})^* \hat{A}_u^{\alpha k} \hat{A}_u^k \rho\right)\right] \\
&\leq 4(p\epsilon + \sqrt{p-1}\sqrt{p\epsilon}) \\
&\leq 4\left(p + 2\sqrt{p(p-1)}\right)\sqrt{\epsilon}.
\end{aligned}
$$

by Lemma 3.5 where $\beta_1 = 4p\epsilon$ by Lemma 3.4 and $\beta_2 = (p-1) - 2p\epsilon$ by Lemma 3.3. Notice that when $k = 0$, we have that $(A_x)^k - \sum_u \omega^{ku\cdot x} M_u = I - I = 0$. By definition of $A_x$,

$$
\sum_{k=0}^{p-1} \left|(A_x)^k - \sum_u \omega^{ku\cdot x} M_u\right|^2 = \sum_{k=0}^{p-1} \left|\sum_i \omega^{ki} A_x^i - \sum_u \omega^{ku\cdot x} M_u\right|^2.
$$

Separating the sum over $M_u$ with respect to $i$ and expanding gives

$$
\begin{aligned}
&\sum_{k=0}^{p-1} \left|(A_x)^k - \sum_u \omega^{ku\cdot x} M_u\right|^2 \\
=&\sum_{k=0}^{p-1} \left|\sum_i \left(\omega^{ki} A_x^i - \sum_{u\cdot x = i} \omega^{ku\cdot x} M_u\right)\right|^2 \\
=&\sum_{k=0}^{p-1} \left(\sum_{i,j} \left(\omega^{ki} A_x^i - \sum_{u\cdot x = i} \omega^{ku\cdot x} M_u\right)\left(\omega^{-kj} A_x^j - \sum_{u\cdot x = j} \omega^{-ku\cdot x} M_u\right)\right).
\end{aligned}
$$

Factoring out each $\omega^{ku\cdot x}$ gives

$$
\begin{aligned}
&\sum_{k=0}^{p-1} \left(\sum_{i,j} \left(\omega^{ki} A_x^i - \sum_{u\cdot x = i} \omega^{ku\cdot x} M_u\right)\left(\omega^{-kj} A_x^j - \sum_{u\cdot x = j} \omega^{-ku\cdot x} M_u\right)\right) \\
=&\sum_{k=0}^{p-1} \left(\sum_{i,j} \omega^{k(i-j)} \left(A_x^i - \sum_{u\cdot x = i} M_u\right)\left(A_x^j - \sum_{u\cdot x = j} M_u\right)\right) \\
=&p\sum_i \left(A_x^i - \sum_{u\cdot x = i} M_u\right)^2.
\end{aligned}
$$

Dividing by $p$ implies the claim. □

**Corollary 3.7.** *Suppose three entangled provers succeed in the linearity test with probability 1-$\epsilon$ using a symmetric strategy $(\sigma, \{A_x^a\})$, and let its corresponding probability distributions be*

$\{p_{x,y,z}\}_{x,y,z\in\mathbb{F}_p^n}$. *Then there exists a measurement* $\{M_u\}$ *such that if we let* $B_x^a \coloneqq \sum_{u:u\cdot x=a} M_u$ *with corresponding probability distributions* $\{\ell_{x,y,z}\}_{x,y,z\in\mathbb{F}_p^n}$,

$$\|p-\ell\|_{\mathrm{TV}} \leq 6\epsilon^{1/4}\sqrt{1+2\left(1-\frac{1}{p}\right)^{1/2}}.$$

*Proof.* The result immediately follows from Lemma 2.13. □

# 4 The Affine Linearity Test

Classically, if one drops the consistency test in BLR, we can still make conclusions regarding the player's strategy (i.e. bound the total variational distance with respect to some deterministic strategy). A very natural question is whether this extends to the quantum case. We first introduce the affine linearty test:

**Definition 4.1** (Affine linearity test)**.** Suppose we have 3 provers $P_1, P_2, P_3$ with outputs $P_i(x) \in \mathbb{F}_2$ for each $i$. We perform the following test:

1. Select $x, y \in \mathbb{F}_2^n$ uniformly and at random. Let $z = x + y$. Query $x$ to $P_1$, $y$ to $P_2$, and $z$ to $P_3$. Accept if and only if $P_3(z) = P_1(x) + P_2(y)$.

Notice that because we are working in $\mathbb{F}_2$, $\alpha$ completely disappears. Furthermore, we have that $A_x$ is both Hermitian and unitary for all $x$, and $\hat{A}_u$ is Hermitian for all $u$ by definition. Setting $\alpha = 1$ using an argument similar to Lemma 3.3 and noticing that in $\mathbb{F}_2$ we must have $x - y = x + y$, we have that

$$\mathop{\mathbb{E}}_{x,y}\left[\mathrm{Tr}\left((A_x\otimes A_y\otimes A_{x+y})\sigma\right)\right] \geq 1-2\epsilon.$$

This implies some form of consistency, as there exists some fixed $z \in \mathbb{F}_2^n$ such that

$$\mathop{\mathbb{E}}_{x}\left[\mathrm{Tr}\left((A_x\otimes A_{x+z}\otimes A_z)\sigma\right)\right] \geq 1-2\epsilon.$$

We now show the following lemmas.

**Lemma 4.2.** *If the three entangled provers succeed in the affine lineraity test with probability* $1-\epsilon$ *using a symmetric strategy* $(\sigma, \{A_x^a\})$*, then*

$$\sum_u \mathrm{Tr}\left(\left(\hat{A}_u\otimes\hat{A}_u\otimes\hat{A}_u\right)\sigma\right) \geq 1-2\epsilon$$

*and*

$$\sum_u \mathrm{Tr}\left(\left(\hat{A}_u\otimes\hat{A}_u\otimes(-1)^{u\cdot z}A_z\right)\sigma\right) \geq 1-2\epsilon.$$

*Proof.* Using a similar argument with that in Lemma 3.3, notice that

$$\begin{aligned}\sum_u \mathrm{Tr}\left(\left(\hat{A}_u\otimes\hat{A}_u\otimes\hat{A}_u\right)\sigma\right) &= \mathop{\mathbb{E}}_{x,y,w}\left[\sum_u (-1)^{u\cdot(x+y+w)}\mathrm{Tr}\left((A_x\otimes A_y\otimes A_w)\sigma\right)\right]\\ &= \mathop{\mathbb{E}}_{x,y,w}\left[2^n\delta_{w=x+y}\mathrm{Tr}\left((A_x\otimes A_y\otimes A_w)\sigma\right)\right]\\ &= \mathop{\mathbb{E}}_{x,y}\left[\mathrm{Tr}\left((A_x\otimes A_y\otimes A_{x+y})\sigma\right)\right].\end{aligned}$$

Similarly, we have

$$\begin{aligned}\sum_u \mathrm{Tr}\left(\left(\hat{A}_u \otimes \hat{A}_u \otimes (-1)^{u\cdot z} A_z\right)\sigma\right) &= \mathop{\mathbb{E}}_{x,y}\left[\sum_u (-1)^{u\cdot(x+y+z)} \mathrm{Tr}\left((A_x \otimes A_y \otimes A_z)\sigma\right)\right] \\ &= \mathop{\mathbb{E}}_{x,y}\left[2^n \delta_{y=x+z} \mathrm{Tr}\left((A_x \otimes A_y \otimes A_z)\sigma\right)\right] \\ &= \mathop{\mathbb{E}}_{x}\left[\mathrm{Tr}\left((A_x \otimes A_{x+z} \otimes A_z)\sigma\right)\right].\end{aligned}$$

By the above, we have

$$\sum_u \mathrm{Tr}\left(\left(\hat{A}_u \otimes \hat{A}_u \otimes (-1)^{u\cdot z} A_z\right)\sigma\right) = \mathop{\mathbb{E}}_{x}\left[\mathrm{Tr}\left((A_x \otimes A_{x+z} \otimes A_z)\sigma\right)\right] \geq 1 - 2\epsilon$$

and

$$\sum_u \mathrm{Tr}\left(\left(\hat{A}_u \otimes \hat{A}_u \otimes \hat{A}_u\right)\sigma\right) = \mathop{\mathbb{E}}_{x,y}\left[\mathrm{Tr}\left((A_x \otimes A_y \otimes A_{x+y})\sigma\right)\right] \geq 1 - 2\epsilon,$$

as desired. □

**Lemma 4.3.** *If*

$$\sum_u \mathrm{Tr}\left(\left(\hat{A}_u \otimes \hat{A}_u \otimes (-1)^{u\cdot z} A_z\right)\sigma\right) \geq \beta$$

*then*

$$\sum_{u\in\mathbb{F}_2^n} \|\hat{A}_u \otimes (-1)^{u\cdot z} A_z \otimes I - I \otimes I \otimes \hat{A}_u\|_\sigma^2 \leq 2(1-\beta).$$

*Proof.* Expanding the product gives us

$$\begin{aligned}&\sum_{u\in\mathbb{F}_2^n} \|\hat{A}_u \otimes (-1)^{u\cdot z} A_z \otimes I - I \otimes I \otimes \hat{A}_u\|_\sigma^2 \\ &\quad = 2\sum_{u\in\mathbb{F}_2^n} \mathrm{Tr}\left((\hat{A}_u)^2\rho\right) - \mathrm{Tr}\left(\left(\hat{A}_u \otimes \hat{A}_u \otimes (-1)^{u\cdot z} A_z\right)\sigma\right),\end{aligned}$$

where the second line arises due to the strategy being symmetric. By Parseval's, $\sum_u (\hat{A}_u)^2 = I$, which implies by the given bounds that

$$2\sum_{u\in\mathbb{F}_2^n} \mathrm{Tr}\left((\hat{A}_u)^2\rho\right) - \mathrm{Tr}\left(\left(\hat{A}_u \otimes \hat{A}_u \otimes (-1)^{u\cdot z} A_z\right)\sigma\right) \leq 2(1-\beta),$$

as desired. □

**Lemma 4.4.** *Given that*

$$\sum_{u\in\mathbb{F}_2^n} \|\hat{A}_u \otimes (-1)^{u\cdot z} A_z \otimes I - I \otimes I \otimes \hat{A}_u\|_\sigma^2 \leq \beta_1$$

*and*

$$\sum_u \mathrm{Tr}\left(\left(\hat{A}_u \otimes \hat{A}_u \otimes \hat{A}_u\right)\sigma\right) \geq \beta_2,$$

*then*

$$\sum_{u\in\mathbb{F}_p^n} \mathrm{Tr}\left(\left((\hat{A}_u)^3 \otimes A_z \otimes A_z\right)\sigma\right) \geq \beta_2 - 2\sqrt{\beta_1}.$$

*Proof.* We expand the following difference of traces:

$$\begin{aligned}
&\sum_u \mathrm{Tr}\left(\left((\hat{A}_u)^3 \otimes A_z \otimes A_z - \hat{A}_u \otimes \hat{A}_u \otimes \hat{A}_u\right)\sigma\right) \\
&= \sum_u \mathrm{Tr}\left(\left((\hat{A}_u)^3 \otimes (-1)^{u\cdot z} A_z \otimes (-1)^{u\cdot z} A_z - \hat{A}_u \otimes \hat{A}_u \otimes \hat{A}_u\right)\sigma\right) \\
&= \sum_u \mathrm{Tr}\left(\left((\hat{A}_u)^2 \otimes (-1)^{u\cdot z} A_z \otimes I\right)\left(\hat{A}_u \otimes I \otimes (-1)^{u\cdot z} A_z - I \otimes \hat{A}_u \otimes I\right)\sigma\right) \\
&\quad + \sum_u \mathrm{Tr}\left(\left(\hat{A}_u \otimes (-1)^{u\cdot z} A_z \otimes I - I \otimes I \otimes \hat{A}_u\right)\left(\hat{A}_u \otimes \hat{A}_u \otimes I\right)\sigma\right).
\end{aligned}$$

By Cauchy-Schwarz, we have

$$\begin{aligned}
&\sum_u \mathrm{Tr}\left(\left((\hat{A}_u)^2 \otimes (-1)^{u\cdot z} A_z \otimes I\right)\left(\hat{A}_u \otimes I \otimes (-1)^{u\cdot z} A_z - I \otimes \hat{A}_u \otimes I\right)\sigma\right) \\
&\quad + \sum_u \mathrm{Tr}\left(\left(\hat{A}_u \otimes (-1)^{u\cdot z} A_z \otimes I - I \otimes I \otimes \hat{A}_u\right)\left(\hat{A}_u \otimes \hat{A}_u \otimes I\right)\sigma\right) \\
&\leq \sqrt{\beta_1}\left[\left(\sum_u \left\|\left(\hat{A}_u \otimes \hat{A}_u \otimes I\right)\right\|_\sigma^2\right)^{1/2} + \left(\sum_u \left\|\left((\hat{A}_u)^2 \otimes (-1)^{u\cdot z} A_z \otimes I\right)\right\|_\sigma^2\right)^{1/2}\right]
\end{aligned}$$

by our bounds above. We may expand the expression multiplied by the constant and use the operator norm bound (i.e. $\mathrm{Tr}\,(NM) \leq \|N\|_{op}\mathrm{Tr}\,(M)$ for positive semi-definite $M$) along with Parseval's to get

$$\begin{aligned}
&\left(\sum_u \left\|\left(\hat{A}_u \otimes \hat{A}_u \otimes I\right)\right\|_\sigma^2\right)^{1/2} + \left(\sum_u \left\|\left((\hat{A}_u)^2 \otimes (-1)^{u\cdot z} A_z \otimes I\right)\right\|_\sigma^2\right)^{1/2} \\
&\leq \sum_u \mathrm{Tr}\left((\hat{A}_u)^2\rho\right)\|(\hat{A}_u)^2\|_{op} + \sum_u \mathrm{Tr}\left(\hat{A}_u)^2\rho\right)\|(\hat{A}_u)^2\|_{op} \\
&\leq 2.
\end{aligned}$$

where the $(-1)^{u\cdot z}A_z$ vanishes as it is unitary. To conclude, notice our bound holds regardless of a sign in front of the first expression. Hence,

$$\sum_{u\in\mathbb{F}_p^n} \mathrm{Tr}\left(\left((\hat{A}_u)^3 \otimes A_z \otimes A_z\right)\sigma\right) \geq \sum_u \mathrm{Tr}\left(\left(\hat{A}_u \otimes \hat{A}_u \otimes \hat{A}_u\right)\sigma\right) - 2\sqrt{\beta_1} \geq \beta_2 - 2\sqrt{\beta_1},$$

obtaining the desired inequality. □

This leads us to the following theorem:

**Theorem 4.5.** *Suppose three entangled provers succeed in the affine linearity test (i.e. linearity test without consistency) with probability 1-$\epsilon$ using a symmetric strategy $(\sigma, \{A_x^a\})$. Then there exists a measurement $\{M^{u,b,b'}\}$ for $(u,b,b') \in \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2$ such that if we let*

$$B_x^a \coloneqq \sum_{u,b,b' : u\cdot x + b + b' = a} M^{u,b,b'}$$

*then*

$$(d_\sigma(A,B))^2 \leq 6\sqrt{\epsilon}.$$

*Proof.* Define a measurement $\{M_{u,b,b'}\} \coloneqq \left\{(\hat{A}_u)^2 \otimes A_z^b \otimes A_z^{b'}\right\}_{u,b,b'}$.

This is a POVM measurement, as $M_{u,b,b'}$ is positive semi-definite and Hermitian, and Parseval's identity shows that $\sum_{u,b,b'} M_{u,b,b'} = I$. Let $C_x = A_x - \sum_{u,b,b'}(-1)^{u\cdot x+b+b'} M_{u,b,b'}$. Notice that

$$\begin{aligned}\hat{C}_u &= \hat{A}_u - \mathop{\mathbb{E}}_x\left[\sum_{v,b,b'}(-1)^{(v-u)\cdot x+b+b'} M_{v,b,b'}\right] \\ &= \hat{A}_u - \mathop{\mathbb{E}}_x\left[\sum_{b,b'}(-1)^{-b+b'} M_{u,b,b'}\right].\end{aligned}$$

Separating $(-1)^{b+b'}$ across the two registers with the projectors gives

$$\begin{aligned}&\hat{A}_u - \mathop{\mathbb{E}}_x\left[\sum_{b,b'}(-1)^{-b+b'} M_{u,b,b'}\right] \\ &\hat{A}_u - \mathop{\mathbb{E}}_x\left[(\hat{A}_u)^2 \otimes \sum_b (-1)^b A_z^b \otimes \sum_{b'}(-1)^{b'} A_z^{b'}\right] \\ &= \hat{A}_u \otimes I \otimes I - (\hat{A}_u)^2 \otimes A_z \otimes A_z.\end{aligned}$$

Summing over $\|C_x\|_\sigma^2$ gives

$$\begin{aligned}\mathop{\mathbb{E}}_x\left[\left\|A_x - \sum_{u,b,b'}(-1)^{u\cdot x+b+b'} M_{u,b,b'}\right\|_\sigma^2\right] &= \sum_u \|\hat{C}_u\|_\sigma^2 \\ &\le \sum_u \operatorname{Tr}\left((\hat{A}_u)^2\rho\right) + \operatorname{Tr}\left((\hat{A}_u)^4\rho\right) - 2\operatorname{Tr}\left((\hat{A}_u)^3 \otimes A_z \otimes A_z\sigma\right).\end{aligned}$$

By Parseval's and the operator norm bound, we have

$$\begin{aligned}&\sum_u \operatorname{Tr}\left((\hat{A}_u)^2\rho\right) + \operatorname{Tr}\left((\hat{A}_u)^4\rho\right) - 2\operatorname{Tr}\left((\hat{A}_u)^3 \otimes A_z \otimes A_z\sigma\right) \\ &\quad\le 2 - 2\sum_u \operatorname{Tr}\left((\hat{A}_u)^3 \otimes A_z \otimes A_z\sigma\right) \\ &\quad\le 4\epsilon + 8\sqrt{\epsilon} \le 12\sqrt{\epsilon}\end{aligned}$$

by Lemma 4.4 with $\beta_1 = 4\epsilon$ by Lemma 4.3 and $\beta_2 = 1 - 2\epsilon$ by Lemma 4.2. To finish, note that

$$\begin{aligned}\left(A_x - \sum_{u,b,b'}(-1)^{u\cdot x+b+b'} M_{u,b,b'}\right)^2 &= \left((A_x^0 - B_x^0) - (A_x^1 - B_x^1)\right)^2 \\ &= \left((A_x^0 - B_x^0) - (A_x^1 - B_x^1)\right)^2 + \left((A_x^0 - B_x^0) + (A_x^1 - B_x^1)\right)^2 \\ &= 2\left(A_x^0 - B_x^0\right)^2 + 2\left(A_x^1 - B_x^1\right)^2,\end{aligned}$$

as $(A_x^0 - B_x^0) + (A_x^1 - B_x^1) = I - I = 0$. Dividing by 2 implies the claim. □

## Acknowledgements

This research was initiated as part of the MIT PRIMES-USA program. The authors would like to thank MIT PRIMES-USA for this wonderful opportunity.

## References


[BCH+96] M. Bellare, D. Coppersmith, J. Hastad, M. Kiwi, and M. Sudan. Linearity testing in characteristic two. *IEEE Transactions on Information Theory*, 42(6):1781–1795, 1996.

[BLR93] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/correcting with applications to numerical problems. *Journal of Computer and System Sciences*, 47(3):549–595, 1993.

[FJVY19] Joseph Fitzsimons, Zhengfeng Ji, Thomas Vidick, and Henry Yuen. Quantum proof systems for iterated exponential time, and beyond. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019, page 473–480, New York, NY, USA, 2019. Association for Computing Machinery.

[IV12] Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for nexp sound against entangled provers. *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 243–252, 2012.

[JNV+20] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. Quantum soundness of the classical low individual degree test, 2020.

[JNV+21] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. Mip* = re. *Commun. ACM*, 64(11):131–138, oct 2021.

[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, 2022.

[Kop] Swastik Kopparty. Fourier analysis. https://sites.math.rutgers.edu/~sk1233/courses/finitefields-F13/fourier.pdf.

[Mos] Dana Moshkovitz. Lecture 16: Linearity testing. https://ocw.mit.edu/courses/18-405j-advanced-complexity-theory-spring-2016/b090bc9af298990b8aeb48a468a60a9b_MIT18_405JS16_Linearity.pdf.

[NV18] Anand Natarajan and Thomas Vidick. Low-degree testing for quantum states, and a quantum entangled games pcp for qma. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 731–742, 2018.

[NW19] Anand Natarajan and John Wright. Neexp is contained in mip. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 510–518. IEEE, 2019.

[Vid] Thomas Vidick. Linearity testing with entangled provers. http://users.cms.caltech.edu/~vidick/notes/linearity_test.pdf.