Robust self-testing via approximate representations

May 7, 2020

Let G be a non-local game with input spaces X, Y and ouput spaces A, B.

Consider a quantum (tensor product) strategy p given by a unit vector $\psi \in \mathscr{H}_A \otimes \mathscr{H}_B$, where $\mathscr{H}_A$ and $\mathscr{H}_B$ are Hermitian spaces (i.e. finite-dimensional complex Hilbert spaces), and by families of PVMs $(\Pi^x_{A,a})_{a\in A}$ on $\mathscr{H}_A$, for $x \in X$, and $(\Pi^y_{B,b})_{b\in B}$ on $\mathscr{H}_B$, for $y \in Y$. If the players (Alice and Bob) receive the inputs x and y, the probability that they will answer a and b is

$$\mathbb{P}(a, b \mid x, y) = \langle(\Pi^x_{A,a} \otimes \Pi^y_{B,b})\psi, \psi\rangle.$$

We will only consider strategies of that form.

Definition (See Section 3.1 of [Col20].)

We say that the correlation $\mathbb{P}(a, b \mid x, y)$ self-tests the strategy $p = (((\Pi^x_{A,a})_{a\in A})_{x\in X}, ((\Pi^y_{B,b})_{b\in B})_{y\in Y}, \psi)$ if, for any strategy $p' = (((\Pi'^x_{A,a})_{a\in A})_{x\in X}, ((\Pi'^y_{B,b})_{b\in B})_{y\in Y}, \psi')$ such that $\mathbb{P}(a, b \mid x, y) = \langle(\Pi'^x_{A,a} \otimes \Pi'^y_{B,b})\psi', \psi'\rangle$, there exists isometries $V_A : \mathscr{H}'_A \to \mathscr{H}_A \otimes \mathscr{H}''_A$, $V_B : \mathscr{H}'_B \to \mathscr{H}_B \otimes \mathscr{H}''_B$ and a unitary vector $\psi'' \in \mathscr{H}''_A \otimes \mathscr{H}''_B$ such that:

- $(V_A \otimes V_B)\psi' = \psi \otimes \psi''$;
- $(V_A \otimes V_B)(\Pi'^x_{A,a} \otimes \Pi'^y_{B,b})(\psi') = (\Pi^x_{A,a} \otimes \Pi^y_{B,b})(\psi) \otimes \psi''$.

Definition (See Section 3.1 of [Col20].)

Let G be a non-local game, and let $\delta : [0,1] \to \mathbb{R}_{\geq 0}$ be a function such that $\lim_{\varepsilon \to 0} \delta(\varepsilon) = 0$.
We say that the correlation $\mathbb{P}(a, b \mid x, y)$ self-tests the strategy $p = (((\Pi^x_{A,a})_{a \in A})_{x \in X}, ((\Pi^y_{B,b})_{b \in B})_{y \in Y}, \psi)$ with robustness δ if, for every $\varepsilon \geq 0$, for any strategy $p' = (((\Pi'^x_{A,a})_{a \in A})_{x \in X}, ((\Pi'^y_{B,b})_{b \in B})_{y \in Y}, \psi')$ inducing a correlation $\mathbb{P}'(a, b \mid x, y)$ such that $|\mathbb{P}'(a, b \mid x, y) - \mathbb{P}(a, b \mid x, y)| \leq \varepsilon$ for all x, y, a, b, there exists isometries $V_A : \mathscr{H}'_A \to \mathscr{H}_A \otimes \mathscr{H}''_A$, $V_B : \mathscr{H}'_B \to \mathscr{H}_B \otimes \mathscr{H}''_B$ and a unitary vector $\psi'' \in \mathscr{H}''_A \otimes \mathscr{H}''_B$ such that:

- $\|(V_A \otimes V_B)(\psi') - \psi \otimes \psi''\| \leq \delta(\varepsilon)$;
- $\|(V_A \otimes V_B)(\Pi'^x_{A,a} \otimes \Pi'^y_{B,b})(\psi') - (\Pi^x_{A,a} \otimes \Pi^y_{B,b})(\psi) \otimes \psi''\| \leq \delta(\varepsilon)$.

Here, we will only be interested in robustly testing perfect strategies, so we always use the correlation corresponding to such a strategy.

The Weyl-Heisenberg group

The n-qubit Weyl-Heisenberg group (or n-qubit Pauli group modulo complex conjugation) is the group

$$H^{(n)} = \left\{ \begin{pmatrix} 1 & * & \dots & * \\ & 1 & 0 & \vdots \\ & & 1 & * \\ 0 & & & 1 \end{pmatrix} \in GL_{n+2}(\mathbb{F}_2) \right\}.$$

It has 2^{2n+1} elements. If $a = (a_1, \dots, a_n) \in \mathbb{F}_2^n$, we write $g_X(a)$ for the element of $H^{(n)}$ that has first row equal to $(1, a_1, \dots, a_n, 0)$ and last column equal to $(0, \dots, 0, 1)$, and $g_Z(a)$ for the symmetric of $g_X(a)$ with respect to the antidiagonal. We also write J for the element of $H^{(n)}$ that has $(1, n+2)$ entry equal to 1 and all its other non-diagonal entries equal to 0. Then J is in the center of $H^{(n)}$, and we have

$$g_X(a)g_X(b) = g_X(a+b), \quad g_Z(a)g_Z(b) = g_Z(a+b), \quad g_X(a)g_Z(b) = J^{a \cdot b} g_Z(b)g_X(a).$$

If $n = 1$, we just write $g_X = g_X(1)$, $g_Z = g_Z(1)$.

Let $\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$. If $a = (a_1, \dots, a_n) \in \mathbb{F}_2^n$, we write $\sigma_X(a), \sigma_Z(a) \in \mathrm{End}((\mathbb{C}^2)^{\otimes n})$ for the tensor product $\sigma_X^{a_1} \otimes \dots \otimes \sigma_X^{a_n}$ and $\sigma_Z^{a_1} \otimes \dots \otimes \sigma_Z^{a_n}$.

Then the assignment $J^c g_X(a) g_Z(b) \mapsto (-1)^c \sigma_X(a) \sigma_Z(b)$ is the unique irreducible 2^n-dimensional representation of the group $H^{(n)}$, and it is faithful (so we can identify $H^{(n)}$ with its image in $U((\mathbb{C}^2)^{\otimes n})$).

All the other irreducible representations of this group have dimension 1 and send J to 1.

Schmidt decomposition

Let $\mathscr{H}_A$ and $\mathscr{H}_B$ be Hermitian spaces, and let $\psi \in \mathscr{H}_A \otimes \mathscr{H}_B$.

Lemma

There exist orthonormal bases $(u_1, \ldots, u_n)$ *and* $(v_1, \ldots, v_m)$ *of* $\mathscr{H}_A$ *and* $\mathscr{H}_B$*, and nonincreasing nonnegative real numbers* $\lambda_1, \ldots, \lambda_r$*, with* $r = \min(n, m)$*, such that*

$$\psi = \sum_{i=1}^{r} \sqrt{\lambda_i} u_i \otimes v_i.$$

Moreover, the numbers $\lambda_1, \ldots, \lambda_r$ *are uniquely determined by* ψ*.*

This is called the *Schmidt decomposition* of ψ, the u_i and v_j are called the *Schmidt vectors*, the $\sqrt{\lambda_i}$ are called the *Schmidt coefficients*, and the number of nonzero Schmidt coefficients is called the *Schmidt rank* (it is a measure of entanglement).

We have $\|\psi\|^2 = \lambda_1 + \ldots + \lambda_r$, so, if ψ is a unit vector (a “state”), then $\lambda_1 + \ldots + \lambda_r = 1$.

Proof.

Write $\psi = \sum_{i=1}^{n} \sum_{j=1}^{m} \psi_{ij} e_i \otimes f_j$, where (e_i) and (f_j) are orthonormal bases of $\mathscr{H}_A$ and $\mathscr{H}_B$, let $K = (\psi_{i,j})$, take the singular value decomposition of K. □

Reduced density

Definition

The *reduced density* (on the first system) of ψ is

$$\sigma_\psi = KK^*.$$

Remark

We can see $\psi \in \mathscr{H}_A \otimes \mathscr{H}_B$ as the linear map $K_\psi : \overline{\mathscr{H}_B} \to \mathscr{H}_A$, $w \mapsto \langle \psi, w \rangle_{\mathscr{H}_B}$. Then $K_\psi^* : \overline{\mathscr{H}_A} \to \mathscr{H}_B$ is the map $v \mapsto \langle \psi, v \rangle_{\mathscr{H}_A}$, and

$$\sigma_\psi = K_\psi \circ K_\psi^* = \sum_{i=1}^{r} \lambda_i u_i u_i^*,$$

where $(u_1^*, \dots, u_n^*)$ is the dual basis.
Also, if $A \in \mathrm{End}(\mathscr{H}_A)$ and $B \in \mathrm{End}(\mathscr{H}_B)$, then

$$K_{(A \otimes B)\psi} = A \circ K_\psi \circ B^*.$$

In the bases (e_i) and (f_j), the matrix of K_ψ is K and the matrix of $K_{(A \otimes B)\psi}$ is AK^tB.
In particular, we have

$$\|(A \otimes \mathrm{id}_{\mathscr{H}_B})\psi\|^2 = \mathrm{Tr}(A^* A K_\psi K_\psi^*).$$

Maximally entangled state

Let $\psi \in \mathscr{H}_A \otimes \mathscr{H}_B$ be a unit vector. Let $\psi = \sum_{i=1}^{r} \sqrt{\lambda_i} u_i \otimes v_i$ be its Schmidt decomposition. We say that ψ is *maximally entangled* if the entropy of $(\lambda_1, \ldots, \lambda_r)$ is maximal, i.e. if $\lambda_1 = \ldots = \lambda_r$.

So, up to isometry, the unique maximal entangled state is

$$\psi = \frac{1}{\sqrt{\min(n,m)}} \sum_{i=1}^{\min(n,m)} e_i \otimes f_i.$$

Goal

Find a non-local game that robustly tests the (perfect) strategy where the first player's strategy is given by the observables $\sigma_X(a)$ and $\sigma_Z(a)$, the second player's strategy is given by the same observables, and the vector on which we apply them is a maximally entangled state of $(\mathbb{C}^2)^{\otimes n} \otimes (\mathbb{C}^2)^{\otimes n}$.

Also, the robustness bound should not depend on n, and we also want a robust bound on the Schmidt rank of the state used by the strategy.

We will present a game due to Natarajan and Vidick (see [NV16] and [Vid17]), but there are other games that work, see for example [CS19].

Binear linear system (BLS) games

We consider a linear system $Mv = \mu$ over $\mathbb{F}_2$ with p equations in n variables, so $M \in M_{pn}(\mathbb{F}_2)$ and $\mu \in \mathbb{F}_2^p$. (Where $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.)

Definition (Associated BLS game)

Alice receives as input $x \in \{1, \ldots, p\}$, Bob receives as input $y \in \{1, \ldots, n\}$ such that $M_{xy} = 1$ (i.e. the variable v_y appears in equation x).
Alice has to output an assignment to the variables v_z appearing in equation x (i.e. such that $M_{xz} = 1$), Bob has to output an assignment to the variable v_y.
They win if Alice's assignments satisfies equation x and if their assignments for v_y coincide.

Definition (Solution group of a BLS)

This is the group Γ generated by $g_1, \ldots, g_n$ and f, satisfying the following relations:

- $g_i^2 = e$ for every i and $f^2 = e$ (where e is the unit);
- $g_i f = f g_i$ for every i;
- if there exists $k \in \{1, \ldots, p\}$ such that $M_{k,i} = M_{k,j}$, then $g_i g_j = g_j g_i$ (local compatibility);
- for every $k \in \{1, \ldots, p\}$, we have

$$g_1^{M_{k,1}} \ldots g_n^{M_{k,n}} = f^{\mu_k}$$

  (constraint satisfaction).

Example (Magic square game)

The magic square game corresponds to

$$M = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \mu = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

The solution group is $H^{(2)}$, with $g_X(1,0) = g_7$, $g_X(0,1) = g_9$, $g_Z(1,0) = g_2$, $g_Z(0,1) = g_1$, and $J = f$.

Perfect strategies and representations

We saw last time that perfect strategies in a BLS game correspond to representations $\rho : \Gamma \to U_d(\mathbb{C})$ such that $\rho(f) = -I_d$. Let's review the construction. (Cf. Theorem 1 in [CM13], Theorem 5 in [CLS16].)

A strategy is given by a unit vector $\psi \in \mathscr{H}_A \otimes \mathscr{H}_B$ (where $\mathscr{H}_A$ and $\mathscr{H}_B$ are Hermitian spaces), and by families of PVMs $(\Pi^x_{A,a})_{a \in \mathbb{F}_2^{\{z \in \{1,\dots,n\} \mid M_{xz}=1\}}}$ on $\mathscr{H}_A$, for $1 \leq x \leq p$, and $(\Pi^y_{B,b})_{b \in \mathbb{F}_2}$ on $\mathscr{H}_B$, for $1 \leq y \leq n$, such that, if Alice and Bob receive the inputs x and y, the probability that they will answer a and b is

$$\mathbb{P}(a, b \mid x, y) = \langle (\Pi^x_{A,a} \otimes \Pi^y_{B,b})\psi, \psi\rangle.$$

Remember that an *observable* is a hermitian matrix whose square is the identity (equivalently, a hermitian and unitary matrix). Define observables by

$$A^y_x = \sum_{a \in \mathbb{F}_2^{\{z \in \{1,\dots,n\} \mid M_{xz}=1\}}} (-1)^{a_y} \Pi^x_{A,a}$$

for $1 \leq x \leq p$ and y such that $M_{xy} = 1$, and

$$B_y = \sum_{b \in \mathbb{F}_2} (-1)^b \Pi^y_{B,b},$$

for $1 \leq y \leq n$. These uniquely determine the PVMs. Also, it is easy to check that A^y_x and A^z_x commute. We have

$$\langle (A^y_x \otimes B_y)\psi, \psi\rangle = \sum_{a \in \mathbb{F}_2^{\{z \in \{1,\dots,n\} \mid M_{xz}=1\}}} \sum_{b \in \mathbb{F}_2} (-1)^{a_y + b} \mathbb{P}(a, b \mid x, y).$$

Let $\psi = \sum_{i=1}^{r} \sqrt{\lambda_i} u_i \otimes v_i$ be a Schmidt decomposition. We may assume that $\mathscr{H}_A = \mathrm{Span}(u_1, \dots, u_r)$ and $\mathscr{H}_B = \mathrm{Span}(v_1, \dots, v_r)$.

Since the strategy is perfect, we have, for $x, x' \in \{1, \dots, p\}$ and $y \in \{1, \dots, n\}$ such that $M_{xy} = M_{x'y} = 1$:

$$\langle (A_x^y \otimes B_y)\psi, \psi \rangle = \langle (A_{x'}^y \otimes B_y)\psi, \psi \rangle = 1.$$

This implies that $\langle (A_x^y \otimes \mathrm{id}_{\mathscr{H}_B})\psi = (\mathrm{id}_{\mathscr{H}_A} \otimes B_y^{-1})(\psi) = (A_{x'}^y \otimes \mathrm{id}_{\mathscr{H}_B})\psi$, then that $A_x^y = A_{x'}^y$ ("Alice's observables are non-contextual").

We define $\rho : \Gamma \to U(\mathscr{H}_A)$ by $\rho(g_y) = A_x^y$ for any x such that $M_{xy} = 1$, and by $\rho(f) = -\mathrm{id}_{\mathscr{H}_A}$.

We need to check the constraints, i.e. that, for every x,

$$\prod_{z \text{ st } M_{xz}=1} A_x^z = (-1)^{\mu_z} \mathrm{id}_{\mathscr{H}_A}. \qquad (*)$$

As

$$\prod_{z \text{ st } M_{xz}=1} A_x^z = \sum_{a \in \mathbb{F}_2^{\{z \in \{1,\dots,n\} \mid M_{xz}=1\}}} (-1)^{\sum a_z} \Pi_{A,a}^x$$

by definition of the A_x^z, we get

$$\langle (\prod_{z \text{ st } M_{xz}=1} A_x^z \otimes \mathrm{id}_{\mathscr{H}_B})\psi, \psi \rangle = (-1)^{\mu_x}$$

(the last equality uses the fact that the strategy is perfect), which implies (*).

Definition

Let Γ be a finite group, $\mathscr{H}$ be a Hermitian space and $\rho : \Gamma \to U(\mathscr{H})$ be a function. If $\sigma \in \mathrm{End}(\mathscr{H})$ is semi-definite positive and $\varepsilon > 0$, we say that ρ is an (ε, σ)-*representation* if

$$\mathbb{E}_{x,y\in\Gamma} \operatorname{Re}\langle \rho(x)^*\rho(y), \rho(x^{-1}y)\rangle_\sigma \geq 1 - \varepsilon,$$

where we use the uniform measure on Γ and where, if $T, T' \in \mathrm{End}(\mathscr{H})$, then $\langle T, T'\rangle_\sigma = \mathrm{Tr}(TT'^*\sigma)$.

Note that this is also equivalent to

$$\mathbb{E}_{x,y\in\Gamma}\|\rho(x)^*\rho(y) - \rho(x^{-1}y)\|_\sigma^2 \leq 2\varepsilon,$$

where $\|T\|_\sigma^2 = \langle T, T\rangle_\sigma$.

A plan:

1. Find a game whose ε-close to perfect strategies correspond to $(O(\varepsilon), \sigma_\psi)$-representations of $H^{(n)}$, where ψ is the state used by the strategy.
2. Show that approximate representations are close to representations.

We will explain step 2 in the next slides.

Step 1 is not totally straightfoward: It is true that approximate representations of the solution group give close-to-perfect strategies (Slofstra uses this in [Slo19], with a weaker definition of “approximate representation” that works for infinite solution groups, to construct a BLS game G such that G has finite-dimensional strategy that succeed with probability $1 - \varepsilon$ for every $\varepsilon > 0$, but no perfect finite-dimensional strategy). However, the converse does not seem to be so easy. It was proved under some conditions on Γ in [CS19], but the proof looks complicated.

Instead, we will construct by hand, using the magic square game as a building block, a game whose close-to-perfect strategies produce approximate representations of $H^{(n)}$.

Approximate representations are close to true representations

Theorem (Gowers-Hatami, [GH16])

Let Γ be a finite group, $\mathscr{H}$ be a Hermitian space, $\sigma \in \mathrm{End}(\mathscr{H})$ be semi-definite positive and $\varepsilon \geq 0$.
If $\rho : \Gamma \to U(\mathscr{H})$ is a (ε, σ)-representation, then there exist an isometry $V : \mathscr{H} \to \mathscr{H}'$ and a representation $\rho' : \Gamma \to U(\mathscr{H}')$ such that

$$\mathbb{E}_{x\in\Gamma} \|\rho(x) - V^* \rho'(x) V\|_\sigma^2 \leq 2\varepsilon.$$

Proof.

Let $\mathscr{H}' = L(\Gamma, \mathscr{H})$ be the space of functions $f : \Gamma \to \mathscr{H}$, with the Hermitian inner form $\langle f_1, f_2\rangle = \mathbb{E}_{x\in\Gamma}\langle f_1(x), f_2(x)\rangle_{\mathscr{H}}$.
Consider the map $V : \mathscr{H} \to L(\Gamma, \mathscr{H})$ sending $u \in \mathscr{H}$ to the function $V(u) : x \mapsto \rho(x)(u)$. Then $V^* : L(\Gamma, \mathscr{H}) \to \mathscr{H}$ sends $f : \Gamma \to \mathscr{H}$ to $\mathbb{E}_{x\in\Gamma}(\rho(x)^*(f(x)))$, so, for every $u \in \mathscr{H}$, $V^*V(u) = \mathbb{E}_{x\in\Gamma}(\rho(x)^*(\rho(x)(u))) = u$.
Let ρ' be the right regular representation of Γ on $L(\Gamma, \mathscr{H})$: if $x \in \Gamma$ and $f \in L(\Gamma, \mathscr{H})$, then $(\rho'(x)f)(y) = f(yx)$.
Then, for $x \in \Gamma$ and $u \in \mathscr{H}$,

$$(V^*\rho'(x)V)(u) = \mathbb{E}_{y\in\Gamma}(\rho(y)^*(\rho'(x)(\rho(y))(u))) = \mathbb{E}_{y\in\Gamma}(\rho(y)^*(\rho(yx)(u))),$$

so

$$\mathbb{E}_{x\in\Gamma}\,\mathrm{Re}\langle\rho(x), V^*\rho'(x)V\rangle_\sigma = \mathbb{E}_{x,y\in\Gamma}\,\mathrm{Re}\langle\rho(x), \rho(y)^*\rho(yx)\rangle_\sigma \geq 1 - \varepsilon.$$

□

Constructing approximate representations of $H^{(n)}$

Proposition (Vidick, [Vid17])

Let $n \geq 1$, $\mathscr{H}$ be a Hermitian space, $\psi \in \mathscr{H} \otimes \mathscr{H}$ be a unit vector, $\varepsilon \geq 0$. Consider a map $f : \{X, Z\} \times \mathbb{F}_2^n \to U(\mathscr{H})$, write $X(a) = f(X, a)$ and $Z(b) = f(Z, b)$, and assume that:

1. *$X(a), Z(b)$ are observables for all $a, b \in \mathbb{F}_2^n$;*
2. *$\mathbb{E}_a \langle (X(a) \otimes X(a))(\psi), \psi \rangle \geq 1 - \varepsilon$, $\mathbb{E}_b \langle (Z(b) \otimes Z(b))(\psi), \psi \rangle \geq 1 - \varepsilon$ (consistency);*
3. *$\mathbb{E}_{a,a'} \|X(a)X(a') - X(a + a')\|_{\sigma_\psi}^2 \leq \varepsilon$, $\mathbb{E}_{b,b'} \|Z(b)Z(b') - Z(b + b')\|_{\sigma_\psi}^2 \leq \varepsilon$ (linearity);*
4. *$\mathbb{E}_{a,b} \|X(a)Z(b) - (-1)^{a \cdot b} Z(b)X(a)\|_{\sigma_\psi}^2 \leq \varepsilon$ (anticommutation).*
   Then the assignment $g_X(a) \mapsto X(a)$, $g_Z(b) \mapsto Z(b)$ extends to a $(O(\varepsilon), \sigma_\psi)$-representation ρ of Γ sending $J^c g_X(a) g_Z(b)$ to $(-1)^c X(a)Z(b)$ (for $a, b \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$), where the implicit constant does not depend on n or $\dim \mathscr{H}$.

Corollary

Under the assumptions of the proposition, there exist an isometry $V : \mathscr{H} \to \mathscr{H}'$ and a representation $\rho' : \Gamma \to U(\mathscr{H}')$ such that:

1. *$\mathbb{E}_{a,b} \|X(a)Z(b) - V^* \rho'(g_X(a) g_Z(b)) V\|_\sigma^2 = O(\varepsilon)$;*
2. *If we write $\mathscr{H}' = \mathscr{H}'_+ \oplus^\perp \mathscr{H}'_-$, where $\mathscr{H}'_\pm$ is the subrepresentation of $\mathscr{H}'$ on which J acts by $\pm\mathrm{id}$, and if we decompose $(V \otimes V)\psi$ as $\psi'_+ + \psi'_-$, then $\|\psi'_+\|^2 = O(\varepsilon)$.*

Proof of the corollary.

By the proposition and the Gowers-Hatami theorem, we get an isometry $V : \mathscr{H} \to \mathscr{H}'$ and a representation $\rho' : \Gamma \to U(\mathscr{H}')$ such that

$$\mathbb{E}_{a,b} \|(-1)^c X(a)Z(b) - V^* \rho'(J^c g_X(a) g_Z(b)) V\|_\sigma^2 = O(\varepsilon).$$

In particular, taking $a = b = 0$ and $c = 1$, we get $(*) \quad \|\mathrm{id}_{\mathscr{H}} + V^* \rho'(J) V\|_\sigma^2 = O(\varepsilon)$. As $\rho'(J)$ is an observable, we have an orthogonal decomposition $\mathscr{H}' = \mathscr{H}'_+ \oplus \mathscr{H}'_-$, where $\rho'(J)$ acts by $\pm\mathrm{id}$ on $\mathscr{H}'_\pm$. If we write $(V \otimes V)\psi = \psi'_+ + \psi'_-$ with $\psi'_\pm \in \mathscr{H}_\pm$, then (*) becomes $\|\psi'_+\|^2 = O(\varepsilon)$.

□

Proof of the proposition.

We must prove that the formula for ρ does define a $(O(\varepsilon), \sigma_\psi)$-representation. Let $a, a', b, b' \in \mathbb{F}_2^n$. We are trying to bound $\|X(a)Z(b)X(a')Z(b') - (-1)^{a'\cdot b}X(a+a')Z(b+b')\|_{\sigma_\psi}^2$.We would like to use the fact that

$$\begin{aligned} X(a)Z(b)X(a')Z(b') - (-1)^{a'\cdot b}X(a+a')Z(b+b') = \\ X(a)\left(Z(b)X(a') - (-1)^{a'\cdot b}X(a')Z(b)\right)Z(b') \\ + (-1)^{a'\cdot b}X(a)X(a')\left(Z(b)Z(b') - Z(b+b')\right) \\ + (-1)^{a'\cdot b}\left(X(a)X(a') - X(a+a')\right)Z(b+b') \end{aligned}$$

because we know that the expressions in red have small $\|.\|_{\sigma_\psi}$-norm. Unfortunately, this does not work, because $\|.\|_{\sigma_\psi}$ is invariant by right multiplication by unitary matrices, but not by left multiplication. (Remember that $\langle A, B\rangle_{\sigma_\psi} = \mathrm{Tr}(AB^*\sigma_\psi)$.) On the other hand, using the definition of σ_ψ, we see that, if $A \in \mathrm{End}(\mathscr{H})$ is Hermitian, then $\|(A \otimes \mathrm{id}_{\mathscr{H}})\psi\|^2 = \|A\|_{\sigma_\psi}^2$, hence, if A is Hermitian and $U, V \in U(\mathscr{H})$, then

$$\|(UA \otimes V)\psi\|^2 = \|A\|_{\sigma_\psi}^2.$$

Also, if A is an observable and $\langle (A \otimes A)\psi, \psi\rangle \geq 1 - \varepsilon$, then $\langle (A \otimes \mathrm{id}_{\mathscr{H}})\psi, (\mathrm{id}_{\mathscr{H}} \otimes A)\psi\rangle \geq 1 - \varepsilon$, so $\|(A \otimes \mathrm{id}_{\mathscr{H}})\psi - (\mathrm{id}_{\mathscr{H}} \otimes A)\psi\|^2 \leq 2\varepsilon$. □

Proof.

Now note that

$$
\begin{aligned}
(X(a)Z(b)X(a')Z(b') - (-1)^{a'\cdot b}X(a+a')Z(b+b')) \otimes \mathrm{id}_{\mathscr{H}} = \\
&(X(a)Z(b)X(a') \otimes \mathrm{id}_{\mathscr{H}})(Z(b') \otimes \mathrm{id}_{\mathscr{H}} - \mathrm{id}_{\mathscr{H}} \otimes Z(b')) \\
&+ X(a)(Z(b)X(a') - (-1)^{a'\cdot b}X(a')Z(b)) \otimes Z(b') \\
&+ (-1)^{a'\cdot b}(X(a)X(a') \otimes Z(b'))(Z(b) \otimes \mathrm{id}_{\mathscr{H}} - \mathrm{id}_{\mathscr{H}} \otimes Z(b)) \\
&+ (-1)^{a'\cdot b}X(a)X(a') \otimes (Z(b')Z(b) - Z(b+b')) \\
&+ (-1)^{a'\cdot b}(X(a)X(a') - X(a+a')) \otimes Z(b+b') \\
&+ (-1)^{a'\cdot b}(X(a+a') \otimes \mathrm{id}_{\mathscr{H}})(\mathrm{id}_{\mathscr{H}} \otimes Z(b+b') - Z(b+b') \otimes \mathrm{id}_{\mathscr{H}})
\end{aligned}
$$

Applying this operator to ψ and using the calculations of the previous slide and the assumptions, we get that

$$
\mathbb{E}_{a,b}\|X(a)X(a')Z(b)Z(b') - (-1)^{a'\cdot b}X(a+a')Z(b+b')\|^2_{\sigma_\psi} \leq 9\varepsilon.
$$

□

Now we need to find games that test the hypotheses of the proposition.

Testing linearity and consistency

Definition

Consider the following game G_{CL}, based on the Blum-Luby-Rubinfeld linearity test:

(a) The referee selects $W \in \{X, Z\}$ and $a, a' \in \mathbb{F}_2^n$ uniformly at random. He sends (W, a, a') to Alice and (W, a), (W, a') or $(W, a + a')$ to Bob.

(b) Alice answers with two bits and Bob with one bit. The referee accepts if and only if the players' answers are consistent (that is, if Bob got (W, a) resp. (W, a'), his bit must equal the first resp. second bit of Alice, and if Bob got $(W, a + a')$, his bit must equal the sum of Alice's two bits).

Lemma

Suppose that we have a strategy that wins G_{CL} with probability $1 - \varepsilon$, that the state used in that strategy is $\psi \in \mathscr{H}_A \otimes \mathscr{H}_B$, and that Bob's strategy is described by observables $X(a)$ and $Z(a)$, for $a \in \mathbb{F}_2^n$.
Then these observables satisfy linearity, with a bound $O(\varepsilon)$. (Where the implicit constant does not depend on n.)

Suppose that that Bob's strategy is defined by a family of PVMs $(\Pi^a_{B,W,u})_{u \in \mathbb{F}_2}$, for $W \in \{X, Z\}$ and $a \in \mathbb{F}_2^n$. Then the observables $X(a)$ and $Z(a)$ are given by:

$$X(a) = \sum_{u \in \mathbb{F}_2} (-1)^u \Pi^a_{B,X,u} \quad \text{and} \quad Z(a) = \sum_{u \in \mathbb{F}_2} (-1)^u \Pi^a_{B,Z,u}.$$

Proof.

Suppose that Alice's strategy is defined by a family of PVMs $(\Pi^{a,a'}_{A,W,u_0,u_1})_{u_0,u_1\in\mathbb{F}_2}$, for $W \in \{X, Z\}$ and $a, a' \in \mathbb{F}_2^n$.
Define observables for Alice by

$$W_i(a,a') = \sum_{u_0,u_1\in\mathbb{F}_2} (-1)^{u_i}\Pi^{a,a'}_{A,W,u_0,u_1},$$

for $W \in \{X, Z\}$, $i \in \{0, 1\}$ and $a, a' \in \mathbb{F}_2^n$. Then we have

$$\mathbb{E}_{a,a'}\langle (X_0(a,a')\otimes X(a))\psi,\psi\rangle \geq 1-2\varepsilon, \quad \mathbb{E}_{a,a'}\langle (X_1(a,a')\otimes X(a'))\psi,\psi\rangle \geq 1-2\varepsilon,$$

$$\mathbb{E}_{a,a'}\langle (X_0(a,a')X_1(a,a')\otimes X(a+a'))\psi,\psi\rangle \geq 1-2\varepsilon$$

(and similarly for Z). For example, to prove the third statement, note that $\langle (X_0(a,a')X_1(a,a')\otimes X(a+a'))\psi,\psi\rangle$ is equal to

$$\sum_{u_0,u_1,v\in\mathbb{F}_2} (-1)^{u_0+u_1+v}\mathbb{P}(u_0,u_1;v \mid X,a,a';a+a').$$

As the strategy wins with probability $1-\varepsilon$, the expectation of this is bounded below by $(1-\varepsilon)-\varepsilon = 2\varepsilon$.

□

So we get:

$$\mathbb{E}_{a,a'} \|(X_0(a,a') \otimes X(a))\psi - \psi\|^2 \leq 4\varepsilon,$$

hence $\mathbb{E}_{a,a'} \|(X_0(a,a')X_1(a,a') \otimes X(a)X(a'))\psi - (X_1(a,a') \otimes X(a')\psi\|^2 \leq 4\varepsilon;$

$$\mathbb{E}_{a,a'} \|(X_1(a,a') \otimes X(a'))\psi - \psi\|^2 \leq 4\varepsilon;$$

$$\mathbb{E}_{a,a'} \|(X_0(a,a')X_1(a,a') \otimes X(a+a'))\psi - \psi\|^2 \leq 4\varepsilon.$$

This shows that

$$\mathbb{E}_{a,a'} \|(\mathrm{id}_{\mathscr{H}_A} \otimes X(a)X(a'))\psi - (X_0(a,a')X_1(a,a') \otimes \mathrm{id}_{\mathscr{H}_B})\psi\|^2 \leq 8\varepsilon$$

$$\mathbb{E}_{a,a'} \|(\mathrm{id}_{\mathscr{H}_A} \otimes X(a+a'))\psi - (X_0(a,a')X_1(a,a') \otimes \mathrm{id}_{\mathscr{H}_B})\psi\|^2 \leq 4\varepsilon,$$

and finally that

$$\mathbb{E}_{a,a'} \|(\mathrm{id}_{\mathscr{H}_A} \otimes X(a)X(a'))\psi - (\mathrm{id}_{\mathscr{H}_A} \otimes X(a+a'))\psi\|^2 \leq 12\varepsilon.$$

□

What about consistency ?

The consistency condition is only testable if the players apply the same strategy, but the game G_{LC} is not symmetric. Two possible fixes:

- In the proposition building approximate representations, replace $X(a), Z(a)$ by families of observables $X_1(a), Z_1(a)$ acting on $\mathscr{H}_1$ and $X_2(a), Z_2(a)$ acting on $\mathscr{H}_2$, take $\psi \in \mathscr{H}_1 \otimes \mathscr{H}_2$, assume that the X_i and Z_i satisfy linearity and anticommutation, and replace consistency with ($W \in \{X, Z\}$):

$$\mathbb{E}_a \langle (W_1(a) \otimes W_2(a))\psi, \psi \rangle \geq 1 - \varepsilon.$$

  The proof goes through. Then use the observables associated to $\Pi^{a,b}_{A,W,u_0} := \sum_{u_1 \in \mathbb{F}_2} \Pi^{a,b}_{A,W,u_0,u_1}$.
- Make the game symmetric in the two players (this is a good idea anyway). Then it is easy to see that if there exists a strategy succeeding with probability $\geq 1 - \varepsilon$, there exists a symmetric strategy succeeding with probability $\geq 1 - \varepsilon$. Restrict attention to symmetric strategies.

The symmetric linearity game

Here is the symmetric version of the linearity game:

1. Choose one player at random and label it Alice; label the other player Bob.
2. Choose $W \in \{X, Z\}$ uniformly at random, choose $a, b \in \mathbb{F}_2^n$ uniformuly at random, send (W, a, b) to Alice.
3. Choose c be a, b or $a + b$ with equal probablity, choose $c' \in \mathbb{F}_2^n$ uniformly at random, send (W, c, c') to Bob.
4. Alice responds with $(\alpha, \beta) \in \mathbb{F}_2^2$, Bob responds with $(\gamma, \gamma') \in \mathbb{F}_2^2$,
5. The referee performs one of the following tests:
   - If c was a (resp. b), accept if only if $\gamma = \alpha$ (resp. $\gamma = \beta$);
   - If c was $a + b$, accept if and only if $\gamma = \alpha + \beta$.

Testing anticommutation

Lemma ([WBMS16], [CN16])

Consider a strategy for the magic square game that succeeds with probability $\geq 1 - \varepsilon$, using a state $\psi \in \mathscr{H}_A \otimes \mathscr{H}_B$. Let X and Z be the observables corresponding to questions 7 and 3 for Bob. Then

$$\langle (\mathrm{id}_{\mathscr{H}_A} \otimes (XZ + ZX))\psi, \psi \rangle \geq 1 - O(\sqrt{\varepsilon}).$$

The anticommutation test is the following game:

1. The referee selects $a, b \in \mathbb{F}_2^n$ uniformly at random under the condition that $a \cdot b = 1$. He plays the magic square game with the players, with the following modification: if the question that he sends Bob should have been question 7 (resp. 3), then he sends (X, a) (resp. (Z, b)) instead; otherwise, he sends the question label and (a, b).
2. The players provide answers as in the magic square game, and the referee accepts the answers if and only if they would have been accepted in the magic square game.

Lemma

If a strategy succeeds with probability $1 - \varepsilon$, using a state $\psi \in \mathscr{H}_A \otimes \mathscr{H}_B$, and if Bob's observables corresponding to the questions (X, a) and (Z, b) are $X(a)$ and $Z(b)$ respectively, then

$$\mathbb{E}_{a,b|a\cdot b=1} \langle (\mathrm{id}_{\mathscr{H}_A} \otimes (X(a)Z(b) - (-1)^{a\cdot b} Z(b)X(a)))\psi, \psi \rangle \geq 1 - O(\sqrt{\varepsilon}).$$

The Pauli braiding test

We consider the following game, called the ***n*-qubit Pauli braiding test**: With probability $1/2$ each, execute the linearity test or the anticommutation test.

(This is an informal description, as we actually want to make the game symmetric in the two players.)

Theorem

Suppose that we have a symmetric strategy for this game that succeeds with probability $\geq 1 - \varepsilon$, using a state $\psi \in \mathscr{H} \otimes \mathscr{H}$. Then the Schmidt rank of ψ is $(1 - O(\sqrt{\varepsilon}))2^n$.

Proof outline.

Consider observables $X(a), Z(b)$ defined as before. Then they satisfy the conditions of the approximate-representation-building proposition, with a bound $O(\sqrt{\varepsilon})$. Using the corollary of that proposition, we get an isometry $V : \mathscr{H} \to \mathscr{H}'$ and a representation ρ of $H^{(n)}$ on $\mathscr{H}'$ such that

$$(*) \quad \mathbb{E}_{a,b}\|X(a)Z(b) - V^*\rho(g_X(a)g_Z(b))V\|_\sigma^2 = O(\sqrt{\varepsilon}).$$

Also, if $\mathscr{H}'_-$ is the subrepresentation of $\mathscr{H}$ on which J acts by $-\mathrm{id}$, and if ψ'_- is the orthogonal projection of $(V \otimes V)\psi$ on $\mathscr{H}'_- \otimes \mathscr{H}'_-$, then $\|\psi'_-\|^2 \geq 1 - O(\sqrt{\varepsilon})$. Equation (*) implies that $\mathbb{E}_{a,b}\|(\rho(g_X(a)g_Z(b)) \otimes \rho(g_X(a)g_Z(b)))\psi'_-\|^2 \geq 1 - O(\sqrt{\varepsilon})$.
This implies that there exists is a maximally entangled state φ in $\mathscr{H}'_- \otimes \mathscr{H}'_-$ such that $|\langle\varphi, \psi\rangle|^2 \geq 1 - O(\sqrt{\varepsilon})$ (see the first lemma).Let d (resp. d') be the Schmidt rank of ψ (resp. ψ'_-). Then $d \geq d'$ and $|\langle\varphi, \psi\rangle|^2 \leq d'2^{-n}$ (see the second lemma), so we get the result.

Lemma

Let $\mathscr{H}$ be the space of the unique 2^n-dimensional representation of $H^{(n)}$, and let $\psi \in \mathscr{H} \otimes \mathscr{H}$ be a nonzero vector such that

$$E_{a,b}\langle(\rho_X(a)\rho_Z(b) \otimes \rho_X(a)\rho_Z(b))\psi, \psi\rangle \geq 1 - \varepsilon.$$

Then there exists a maximally entangled state $\varphi \in \mathscr{H} \otimes \mathscr{H}$ such that $|\psi^*\varphi|^2 \geq \|\psi\|^2(1 - \varepsilon)$.

Proof.

The point is that there exists a maximally entangled state $\varphi \in \mathscr{H} \otimes \mathscr{H}$ such that the subspace of $\mathscr{H} \otimes \mathscr{H}$ generated by φ is exactly the subspace of fixed points of all the operators $\sigma_X(a)\sigma_Z(b) \otimes \sigma_X(a)\sigma_Z(b)$. The condition implies that ψ is very close to its orthogonal projection on the subspace.

□

The second lemma

Lemma

Let $\varphi \in \mathscr{H} \otimes \mathscr{H}$ be a maximally entangled state, and let $\psi \in \mathscr{H} \otimes \mathscr{H}$ be a vector. If r is the Schmidt rank of ψ, then $\|\psi^* \varphi\|^2 \leq \frac{r}{\dim \mathscr{H}} \|\psi\|^2$.

Proof.

Suppose first that $\psi = u \otimes v$, with $u, v \in \mathscr{H}$ unit vectors. Let $d = \dim(\mathscr{H})$, and write $\varphi = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} e_i \otimes f_i$, where (e_i) and (f_i) are orthonormal bases of $\mathscr{H}$. Then

$$|\psi^* \varphi|^2 = \frac{1}{d} \left| \sum_{i=1}^{d} \langle u, e_i \rangle \langle v, f_i \rangle \right| \leq \frac{1}{d} \left(\sum_{i=1}^{d} |\langle u, e_i \rangle|^2 \right) \left(\sum_{i=1}^{d} |\langle v, f_i \rangle|^2 \right) = \frac{1}{d}.$$

We now take ψ arbitrary. Let $\psi = \sum_{i=1}^{r} \sqrt{\lambda_i} u_i \otimes v_i$ be a Schmidt decomposition, where we only write the nonzero Schmidt coefficients. Then

$$|\psi^* \varphi| = |\sum_{i=1}^{r} \sqrt{\lambda_i} (u_i \otimes v_i)^* \varphi| \leq \frac{1}{\sqrt{d}} \sum_{i=1}^{d} \sqrt{\lambda_i},$$

hence

$$|\psi^* \varphi|^2 \leq \frac{1}{d} (\sum_{i=1}^{r} \sqrt{\lambda_i}) \leq \frac{r}{d} \sum_{i=1}^{r} \lambda_i = \frac{r}{d} \|\psi\|^2.$$

□

[CLS16] Richard Cleve, Li Liu, and William Slofstra, *Perfect commuting-operator strategies for linear system games*, 2016.

[CM13] Richard Cleve and Rajat Mittal, *Characterization of binary constraint system games*, 2013.

[CN16] Matthew Coudron and Anand Natarajan, *The parallel-repeated magic square game is rigid*, 2016.

[Col20] Andrea Coladangelo, *Quantum correlations, certifying quantum devices, and the quest forinfinite entanglement*, 2020.

[CS19] Andrea Coladangelo and Jalex Stark, *Robust self-testing for linear constraint system games*, 2019.

[GH16] Timothy Gowers and Omid Hatami, *Inverse and stability theorems for approximaterepresentations of finite groups*, 2016.

[NV16] Anand Natarajan and Thomas Vidick, *Robust self-testing of many-qubit states*, 2016.

[Slo19] William Slofstra, *The set of quantum correlations is not closed*, Forum Math. Pi **7** (2019), e1, 41. MR 3898717

[Vid17] Thomas Vidick, *Note on the pauli braiding test*, 2017.

[WBMS16] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani, *Device-independent parallel self-testing of two singlets*, 2016.