Exact self-testing for binary linear system games

Based (mostly) on arXiv:1606.02278 and arXiv:1709.09267

GdT Connes-Tsirelson – April 30 2020

Reminder on non-local games

Non-local game: G with input spaces X, Y and output spaces A, B, defined by its input probability distribution $\pi : X \times Y \to [0,1]$ and its winning condition $V : A \times B \times X \times Y \to \{0,1\}$.
Strategy of the players: Conditional probability distribution $p : A \times B \times X \times Y \to [0,1]$.
$\longrightarrow$ When receiving the pair of inputs $(x,y) \in X \times Y$, the players answer the pair of outputs $(a,b) \in A \times B$ with probability $p(a,b|x,y)$.

Winning probability of the players when playing game G with strategy p:

$$\omega(G,p) := \sum_{x \in X, y \in Y} \pi(x,y) \sum_{a \in A, b \in B} p(a,b|x,y) V(a,b,x,y) .$$

Reminder on non-local games

Non-local game: G with input spaces X, Y and output spaces A, B, defined by its input probability distribution $\pi : X \times Y \to [0,1]$ and its winning condition $V : A \times B \times X \times Y \to \{0,1\}$.
Strategy of the players: Conditional probability distribution $p : A \times B \times X \times Y \to [0,1]$.
$\longrightarrow$ When receiving the pair of inputs $(x,y) \in X \times Y$, the players answer the pair of outputs $(a,b) \in A \times B$ with probability $p(a,b|x,y)$.

Winning probability of the players when playing game G with strategy p:

$$\omega(G,p) := \sum_{x \in X, y \in Y} \pi(x,y) \sum_{a \in A, b \in B} p(a,b|x,y) V(a,b,x,y) \,.$$

Quantum (tensor product) strategy: p defined by a state $|\varphi\rangle \in \mathbf{C}^d \otimes \mathbf{C}^d$ and projection-valued measures (PVMs) $\{A_x^a\}_{a \in A}$, $x \in X$, $\{B_y^b\}_{b \in B}$, $y \in Y$, on $\mathbf{C}^d$ s.t.

$$p(a,b|x,y) = \langle \varphi | A_x^a \otimes B_y^b | \varphi \rangle \,.$$

Reminder on non-local games

Non-local game: G with input spaces X, Y and output spaces A, B, defined by its input probability distribution $\pi : X \times Y \to [0,1]$ and its winning condition $V : A \times B \times X \times Y \to \{0,1\}$.
Strategy of the players: Conditional probability distribution $p : A \times B \times X \times Y \to [0,1]$.
$\longrightarrow$ When receiving the pair of inputs $(x,y) \in X \times Y$, the players answer the pair of outputs $(a,b) \in A \times B$ with probability $p(a,b|x,y)$.

Winning probability of the players when playing game G with strategy p:

$$\omega(G,p) := \sum_{x\in X, y\in Y} \pi(x,y) \sum_{a\in A, b\in B} p(a,b|x,y)V(a,b,x,y) .$$

Quantum (tensor product) strategy: p defined by a state $|\varphi\rangle \in \mathbf{C}^d \otimes \mathbf{C}^d$ and projection-valued measures (PVMs) $\{A_x^a\}_{a\in A}$, $x \in X$, $\{B_y^b\}_{b\in B}$, $y \in Y$, on $\mathbf{C}^d$ s.t.

$$p(a,b|x,y) = \langle\varphi|A_x^a \otimes B_y^b|\varphi\rangle .$$

Quantum (tensor product) value of G:

$$\omega_q(G) := \sup\{\omega(G,p) : p \text{ quantum strategy}\} .$$

Self-testing

Definition [Self-testing (Mayers/Yao)]

A non-local game G self-tests a quantum strategy $p \equiv \left(\{\{A_x^a\}_a\}_x, \{\{B_y^b\}_b\}_y, |\varphi\rangle\right)$ on $\mathbf{C}^d \otimes \mathbf{C}^d$ if any quantum strategy $p' \equiv \left(\{\{A_x^{a\prime}\}_a\}_x, \{\{B_y^{b\prime}\}_b\}_y, |\varphi'\rangle\right)$ on $\mathbf{C}^{d'} \otimes \mathbf{C}^{d'}$ achieving $\omega_q(G)$ is equivalent to p up to local isometries.

That is, there exist $s \in \mathbf{N}$ and isometries $U, V : \mathbf{C}^{d'} \to \mathbf{C}^d \otimes \mathbf{C}^s$ s.t.

- $UA_x^{a\prime}U^* = A_x^a \otimes I$ for all x, a, $VB_y^{b\prime}V^* = B_y^b \otimes I$ for all y, b,
- $U \otimes V|\varphi'\rangle = |\varphi\rangle \otimes |\theta\rangle$ for some state $|\theta\rangle \in \mathbf{C}^s \otimes \mathbf{C}^s$.

Self-testing

Definition [Self-testing (Mayers/Yao)]

A non-local game G self-tests a quantum strategy $p \equiv \left(\{\{A_x^a\}_a\}_x, \{\{B_y^b\}_b\}_y, |\varphi\rangle\right)$ on $\mathbf{C}^d \otimes \mathbf{C}^d$ if any quantum strategy $p' \equiv \left(\{\{A_x^{a\prime}\}_a\}_x, \{\{B_y^{b\prime}\}_b\}_y, |\varphi'\rangle\right)$ on $\mathbf{C}^{d'} \otimes \mathbf{C}^{d'}$ achieving $\omega_q(G)$ is equivalent to p up to local isometries.
That is, there exist $s \in \mathbf{N}$ and isometries $U, V : \mathbf{C}^{d'} \to \mathbf{C}^d \otimes \mathbf{C}^s$ s.t.

- $UA_x^{a\prime}U^* = A_x^a \otimes I$ for all x, a, $VB_y^{b\prime}V^* = B_y^b \otimes I$ for all y, b,
- $U \otimes V|\varphi'\rangle = |\varphi\rangle \otimes |\theta\rangle$ for some state $|\theta\rangle \in \mathbf{C}^s \otimes \mathbf{C}^s$.

This is a rigidity result: the optimal quantum strategy for G is essentially unique.

Self-testing

Definition [Self-testing (Mayers/Yao)]

A non-local game G self-tests a quantum strategy $p \equiv \left(\{\{A_x^a\}_a\}_x, \{\{B_y^b\}_b\}_y, |\varphi\rangle\right)$ on $\mathbf{C}^d \otimes \mathbf{C}^d$ if any quantum strategy $p' \equiv \left(\{\{A_x^{a'}\}_a\}_x, \{\{B_y^{b'}\}_b\}_y, |\varphi'\rangle\right)$ on $\mathbf{C}^{d'} \otimes \mathbf{C}^{d'}$ achieving $\omega_q(G)$ is equivalent to p up to local isometries.
That is, there exist $s \in \mathbf{N}$ and isometries $U, V : \mathbf{C}^{d'} \to \mathbf{C}^d \otimes \mathbf{C}^s$ s.t.

- $UA_x^{a'}U^* = A_x^a \otimes I$ for all x, a, $VB_y^{b'}V^* = B_y^b \otimes I$ for all y, b,
- $U \otimes V|\varphi'\rangle = |\varphi\rangle \otimes |\theta\rangle$ for some state $|\theta\rangle \in \mathbf{C}^s \otimes \mathbf{C}^s$.

This is a rigidity result: the optimal quantum strategy for G is essentially unique.

Interest: A classical verifier (the referee) can certify that quantum provers (the players) perform a specific procedure (specific measurements on a specific state).
$\longrightarrow$ Relevant to design certified device-independent protocols in quantum information theory (randomness generation, delegated computation etc.)
$\longrightarrow$ Can be used as an "entanglement dimension witness": If the provers achieve a given performance, then they must share an entangled state of a given local dimension.

Self-testing

Definition [Self-testing (Mayers/Yao)]

A non-local game G self-tests a quantum strategy $p \equiv \left(\{\{A_x^a\}_a\}_x, \{\{B_y^b\}_b\}_y, |\varphi\rangle\right)$ on $\mathbf{C}^d \otimes \mathbf{C}^d$ if any quantum strategy $p' \equiv \left(\{\{A_x^{a'}\}_a\}_x, \{\{B_y^{b'}\}_b\}_y, |\varphi'\rangle\right)$ on $\mathbf{C}^{d'} \otimes \mathbf{C}^{d'}$ achieving $\omega_q(G)$ is equivalent to p up to local isometries.
That is, there exist $s \in \mathbf{N}$ and isometries $U, V : \mathbf{C}^{d'} \to \mathbf{C}^d \otimes \mathbf{C}^s$ s.t.

- $UA_x^{a'}U^* = A_x^a \otimes I$ for all x, a, $VB_y^{b'}V^* = B_y^b \otimes I$ for all y, b,
- $U \otimes V|\varphi'\rangle = |\varphi\rangle \otimes |\theta\rangle$ for some state $|\theta\rangle \in \mathbf{C}^s \otimes \mathbf{C}^s$.

This is a rigidity result: the optimal quantum strategy for G is essentially unique.

Interest: A classical verifier (the referee) can certify that quantum provers (the players) perform a specific procedure (specific measurements on a specific state).
$\longrightarrow$ Relevant to design certified device-independent protocols in quantum information theory (randomness generation, delegated computation etc.)
$\longrightarrow$ Can be used as an "entanglement dimension witness": If the provers achieve a given performance, then they must share an entangled state of a given local dimension.

Seminal example: The CHSH game self-tests

- the maximally entangled state on $\mathbf{C}^2 \otimes \mathbf{C}^2$: $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$,
- measurements in the basis $(|0\rangle, |1\rangle)$ and its rotation by $\pi/4$ for Alice, measurements in the rotation by $\pi/8$ of these for Bob.

The Magic Square game

Goal: Find $v_1, \ldots, v_9 \in \{0, 1\}$ s.t.

$$(e_1) \quad v_1 \oplus v_2 \oplus v_3 = 0$$

$$(e_4) \quad v_1 \oplus v_4 \oplus v_7 = 0$$

$$(e_2) \quad v_4 \oplus v_5 \oplus v_6 = 0$$

$$(e_5) \quad v_2 \oplus v_5 \oplus v_8 = 1$$

$$(e_3) \quad v_7 \oplus v_8 \oplus v_9 = 0$$

$$(e_6) \quad v_3 \oplus v_6 \oplus v_9 = 0$$

	$e_4 \downarrow$	$e_5 \downarrow$	$e_6 \downarrow$
$e_1 \longrightarrow$	v_1	v_2	v_3
$e_2 \longrightarrow$	v_4	v_5	v_6
$e_3 \longrightarrow$	v_7	v_8	v_9

The Magic Square game

Goal: Find $v_1, \ldots, v_9 \in \{0,1\}$ s.t.

$$(e_1) \quad v_1 \oplus v_2 \oplus v_3 = 0$$
$$(e_4) \quad v_1 \oplus v_4 \oplus v_7 = 0$$
$$(e_2) \quad v_4 \oplus v_5 \oplus v_6 = 0$$
$$(e_5) \quad v_2 \oplus v_5 \oplus v_8 = 1$$
$$(e_3) \quad v_7 \oplus v_8 \oplus v_9 = 0$$
$$(e_6) \quad v_3 \oplus v_6 \oplus v_9 = 0$$

	$e_4 \downarrow$	$e_5 \downarrow$	$e_6 \downarrow$
$e_1 \rightarrow$	v_1	v_2	v_3
$e_2 \rightarrow$	v_4	v_5	v_6
$e_3 \rightarrow$	v_7	v_8	v_9

This is impossible!

The Magic Square game

Goal: Find $v_1, \ldots, v_9 \in \{0,1\}$ s.t.

$$(e_1)\quad v_1 \oplus v_2 \oplus v_3 = 0$$
$$(e_4)\quad v_1 \oplus v_4 \oplus v_7 = 0$$
$$(e_2)\quad v_4 \oplus v_5 \oplus v_6 = 0$$
$$(e_5)\quad v_2 \oplus v_5 \oplus v_8 = 1$$
$$(e_3)\quad v_7 \oplus v_8 \oplus v_9 = 0$$
$$(e_6)\quad v_3 \oplus v_6 \oplus v_9 = 0$$

	$e_4 \downarrow$	$e_5 \downarrow$	$e_6 \downarrow$
$e_1 \rightarrow$	v_1	v_2	v_3
$e_2 \rightarrow$	v_4	v_5	v_6
$e_3 \rightarrow$	v_7	v_8	v_9

This is impossible!

Equivalent: Find $v_1, \ldots, v_9 \in \{-1,1\}$ s.t.

$$(e_1)\quad v_1 \times v_2 \times v_3 = 1$$
$$(e_4)\quad v_1 \times v_4 \times v_7 = 1$$
$$(e_2)\quad v_4 \times v_5 \times v_6 = 1$$
$$(e_5)\quad v_2 \times v_5 \times v_8 = -1$$
$$(e_3)\quad v_7 \times v_8 \times v_9 = 1$$
$$(e_6)\quad v_3 \times v_6 \times v_9 = 1$$

The Magic Square game

Goal: Find $v_1, \ldots, v_9 \in \{0,1\}$ s.t.

$$(e_1) \quad v_1 \oplus v_2 \oplus v_3 = 0$$
$$(e_4) \quad v_1 \oplus v_4 \oplus v_7 = 0$$
$$(e_2) \quad v_4 \oplus v_5 \oplus v_6 = 0$$
$$(e_5) \quad v_2 \oplus v_5 \oplus v_8 = 1$$
$$(e_3) \quad v_7 \oplus v_8 \oplus v_9 = 0$$
$$(e_6) \quad v_3 \oplus v_6 \oplus v_9 = 0$$

	$e_4 \downarrow$	$e_5 \downarrow$	$e_6 \downarrow$
$e_1 \longrightarrow$	v_1	v_2	v_3
$e_2 \longrightarrow$	v_4	v_5	v_6
$e_3 \longrightarrow$	v_7	v_8	v_9

This is impossible!

Equivalent: Find $v_1, \ldots, v_9 \in \{-1,1\}$ s.t.

$$(e_1) \quad v_1 \times v_2 \times v_3 = 1$$
$$(e_4) \quad v_1 \times v_4 \times v_7 = 1$$
$$(e_2) \quad v_4 \times v_5 \times v_6 = 1$$
$$(e_5) \quad v_2 \times v_5 \times v_8 = -1$$
$$(e_3) \quad v_7 \times v_8 \times v_9 = 1$$
$$(e_6) \quad v_3 \times v_6 \times v_9 = 1$$

Magic Square (MS) game (Mermin, Peres, Cleve/Høyer/Toner/Watrous):

The referee picks an equation (e_x) uniformly at random and a variable v_y appearing in (e_x) uniformly at random. Alice gets (e_x) and has to answer with an assignment to the variables appearing in it. Bob gets v_y and has to answer with an assignment to it. They win if the assignments of Alice satisfy (e_x) and if her assignment for v_y matches the one of Bob.

$\longrightarrow$ $X = \{1,\ldots,6\}$, $Y = \{1,\ldots,9\}$ and $A = \{0,1\}^3, B = \{0,1\}$.

$\pi(x,y) = 1/18$ if v_y appears in (e_x), $\pi(x,y) = 0$ otherwise.

$V(a,b,x,y) = 1$ iff $a = (a(v_y), a(v_{y'}), a(v_{y''}))$ satisfies (e_x) and $b = a(v_y)$.

The Magic Square game

Goal: Find $v_1, \dots, v_9 \in \{0,1\}$ s.t.

$(e_1)\ v_1 \oplus v_2 \oplus v_3 = 0$

$(e_4)\ v_1 \oplus v_4 \oplus v_7 = 0$

$(e_2)\ v_4 \oplus v_5 \oplus v_6 = 0$

$(e_5)\ v_2 \oplus v_5 \oplus v_8 = 1$

$(e_3)\ v_7 \oplus v_8 \oplus v_9 = 0$

$(e_6)\ v_3 \oplus v_6 \oplus v_9 = 0$

	$e_4 \downarrow$	$e_5 \downarrow$	$e_6 \downarrow$
$e_1 \longrightarrow$	v_1	v_2	v_3
$e_2 \longrightarrow$	v_4	v_5	v_6
$e_3 \longrightarrow$	v_7	v_8	v_9

This is impossible!

Equivalent: Find $v_1, \dots, v_9 \in \{-1,1\}$ s.t.

$(e_1)\ v_1 \times v_2 \times v_3 = 1$

$(e_4)\ v_1 \times v_4 \times v_7 = 1$

$(e_2)\ v_4 \times v_5 \times v_6 = 1$

$(e_5)\ v_2 \times v_5 \times v_8 = -1$

$(e_3)\ v_7 \times v_8 \times v_9 = 1$

$(e_6)\ v_3 \times v_6 \times v_9 = 1$

Magic Square (MS) game (Mermin, Peres, Cleve/Høyer/Toner/Watrous):

The referee picks an equation (e_x) uniformly at random and a variable v_y appearing in (e_x) uniformly at random. Alice gets (e_x) and has to answer with an assignment to the variables appearing in it. Bob gets v_y and has to answer with an assignment to it. They win if the assignments of Alice satisfy (e_x) and if her assignment for v_y matches the one of Bob.

$\longrightarrow X = \{1,\dots,6\}, Y = \{1,\dots,9\}$ and $A = \{0,1\}^3, B = \{0,1\}$.

$\pi(x,y) = 1/18$ if v_y appears in (e_x), $\pi(x,y) = 0$ otherwise.

$V(a,b,x,y) = 1$ iff $a = (a(v_y), a(v_{y'}), a(v_{y''}))$ satisfies (e_x) and $b = a(v_y)$.

Claim: The maximum winning probability for classical players is $17/18$, while quantum players can win with probability 1.

Optimal quantum strategy for the Magic Square game

Alice and Bob share the maximally entangled state on $\mathbf{C}^4 \otimes \mathbf{C}^4 \equiv (\mathbf{C}^2 \otimes \mathbf{C}^2) \otimes (\mathbf{C}^2 \otimes \mathbf{C}^2)$, i.e.

$$|\psi\rangle_{AB} = \frac{1}{2}\left(|00\rangle_A \otimes |00\rangle_B + |01\rangle_A \otimes |01\rangle_B + |10\rangle_A \otimes |10\rangle_B + |11\rangle_A \otimes |11\rangle_B\right).$$

Optimal quantum strategy for the Magic Square game

Alice and Bob share the maximally entangled state on $\mathbf{C}^4 \otimes \mathbf{C}^4 \equiv (\mathbf{C}^2 \otimes \mathbf{C}^2) \otimes (\mathbf{C}^2 \otimes \mathbf{C}^2)$, i.e.

$$|\psi\rangle_{AB} = \frac{1}{2}\left(|00\rangle_A \otimes |00\rangle_B + |01\rangle_A \otimes |01\rangle_B + |10\rangle_A \otimes |10\rangle_B + |11\rangle_A \otimes |11\rangle_B\right).$$

After receiving their equation or variable, they both perform binary PVMs on their share of $|\psi\rangle_{AB}$ (three for Alice, one for Bob) and answer with the obtained outcomes. They choose the measurements to be performed (on $\mathbf{C}^4 \equiv \mathbf{C}^2 \otimes \mathbf{C}^2$) according to the following rule:

$I \otimes Z$	$Z \otimes Z$	$Z \otimes I$
$X \otimes Z$	$ZX \otimes XZ$	$Z \otimes X$
$X \otimes I$	$X \otimes X$	$I \otimes X$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \; Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$X^2 = Z^2 = I$, $XZ = -ZX$.

Binary PVM corresponding to an observable W with eigenvalues $\{+1, -1\}$: projectors $\{P^+, P^-\}$ on its $+1$ and -1 eigenspaces.

Optimal quantum strategy for the Magic Square game

Alice and Bob share the maximally entangled state on $\mathbf{C}^4 \otimes \mathbf{C}^4 \equiv (\mathbf{C}^2 \otimes \mathbf{C}^2) \otimes (\mathbf{C}^2 \otimes \mathbf{C}^2)$, i.e.

$$|\psi\rangle_{AB} = \frac{1}{2}\left(|00\rangle_A \otimes |00\rangle_B + |01\rangle_A \otimes |01\rangle_B + |10\rangle_A \otimes |10\rangle_B + |11\rangle_A \otimes |11\rangle_B\right).$$

After receiving their equation or variable, they both perform binary PVMs on their share of $|\psi\rangle_{AB}$ (three for Alice, one for Bob) and answer with the obtained outcomes. They choose the measurements to be performed (on $\mathbf{C}^4 \equiv \mathbf{C}^2 \otimes \mathbf{C}^2$) according to the following rule:

$I \otimes Z$	$Z \otimes Z$	$Z \otimes I$
$X \otimes Z$	$ZX \otimes XZ$	$Z \otimes X$
$X \otimes I$	$X \otimes X$	$I \otimes X$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \; Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$X^2 = Z^2 = I, \; XZ = -ZX.$$

Binary PVM corresponding to an observable W with eigenvalues $\{+1, -1\}$: projectors $\{P^+, P^-\}$ on its $+1$ and -1 eigenspaces.

- The operators in a given line (row or column) commute.
  $\longrightarrow$ The outcomes of Alice's three measurements are well defined.
- The product of the operators in a given line is I, except for the central column where it is $-I$.
  $\longrightarrow$ The outcomes of Alice's measurements always satisfy the equation.
- The state of Alice and Bob is left invariant by the operators that they perform on their common input.
  $\longrightarrow$ The outcomes of Alice's and Bob's measurements are always consistent.

Generalization: binary linear system games

Let $Mv = \mu$ be a binary linear system (BLS) with p equations in n variables, i.e. $M \in \mathbf{Z}_2^{p \times n}$, $\mu \in \mathbf{Z}_2^p$.

Associated BLS game (Cleve/Mittal):
Alice receives as input $x \in \{1, \ldots, p\}$, Bob receives as input $y \in \{1, \ldots, n\}$ s.t. $M_{x,y} = 1$ (i.e. v_y appears in equation x).
Alice has to output an assignment to the variables v_z's s.t. $M_{x,z} = 1$ (i.e. those appearing in equation x), Bob has to output an assignment to the variable v_y.
They win if Alice's assignment satisfies equation x and their assignments for variable v_y coincide.

Generalization: binary linear system games

Let $Mv = \mu$ be a binary linear system (BLS) with p equations in n variables, i.e. $M \in \mathbf{Z}_2^{p\times n}$, $\mu \in \mathbf{Z}_2^p$.

Associated BLS game (Cleve/Mittal):
Alice receives as input $x \in \{1,\dots,p\}$, Bob receives as input $y \in \{1,\dots,n\}$ s.t. $M_{x,y} = 1$ (i.e. v_y appears in equation x).
Alice has to output an assignment to the variables v_z's s.t. $M_{x,z} = 1$ (i.e. those appearing in equation x), Bob has to output an assignment to the variable v_y.
They win if Alice's assignment satisfies equation x and their assignments for variable v_y coincide.

Important observation:
A perfect quantum strategy for Alice and Bob in this BLS game (i.e. one which allows them to win with probability 1) can be described by a quantum state $|\varphi\rangle \in \mathbf{C}^d \otimes \mathbf{C}^d$ and observables $A_{x,y}, B_y$ on $\mathbf{C}^d$, $x \in \{1,\dots,p\}, y \in \{1,\dots,n\}$ s.t. $M_{x,y} = 1$, satisfying the following:

- for all x, y s.t. $M_{x,y} = 1$, $A_{x,y}^2 = B_y^2 = I$ (observables have eigenvalues $\{+1,-1\}$ and can thus define binary PVMs).
- for all x, y, y' s.t. $M_{x,y} = M_{x,y'} = 1$, $A_{x,y}A_{x,y'} = A_{x,y'}A_{x,y}$ (Alice's observables commute, so that her outcomes are well defined).
- for all x, $\langle\varphi|A_{x,1}^{M_{x,1}} \cdots A_{x,n}^{M_{x,n}} \otimes I|\varphi\rangle = (-1)^{\mu_x}$ (Alice's outcomes satisfy the equation).
- for all x, y s.t. $M_{x,y} = 1$, $\langle\varphi|A_{x,y} \otimes B_y|\varphi\rangle = 1$ (Alice's and Bob's outcomes are consistent).

Generalization: binary linear system games

Let $Mv = \mu$ be a binary linear system (BLS) with p equations in n variables, i.e. $M \in \mathbf{Z}_2^{p\times n}$, $\mu \in \mathbf{Z}_2^p$.

Associated BLS game (Cleve/Mittal):
Alice receives as input $x \in \{1,\ldots,p\}$, Bob receives as input $y \in \{1,\ldots,n\}$ s.t. $M_{x,y} = 1$ (i.e. v_y appears in equation x).
Alice has to output an assignment to the variables v_z's s.t. $M_{x,z} = 1$ (i.e. those appearing in equation x), Bob has to output an assignment to the variable v_y.
They win if Alice's assignment satisfies equation x and their assignments for variable v_y coincide.

Important observation:
A perfect quantum strategy for Alice and Bob in this BLS game (i.e. one which allows them to win with probability 1) can be described by a quantum state $|\varphi\rangle \in \mathbf{C}^d \otimes \mathbf{C}^d$ and observables $A_{x,y}, B_y$ on $\mathbf{C}^d$, $x \in \{1,\ldots,p\}, y \in \{1,\ldots,n\}$ s.t. $M_{x,y} = 1$, satisfying the following:

- for all x, y s.t. $M_{x,y} = 1$, $A_{x,y}^2 = B_y^2 = I$ (observables have eigenvalues $\{+1,-1\}$ and can thus define binary PVMs).
- for all x, y, y' s.t. $M_{x,y} = M_{x,y'} = 1$, $A_{x,y}A_{x,y'} = A_{x,y'}A_{x,y}$ (Alice's observables commute, so that her outcomes are well defined).
- for all x, $\langle\varphi|A_{x,1}^{M_{x,1}}\cdots A_{x,n}^{M_{x,n}} \otimes I|\varphi\rangle = (-1)^{\mu_x}$ (Alice's outcomes satisfy the equation).
- for all x, y s.t. $M_{x,y} = 1$, $\langle\varphi|A_{x,y} \otimes B_y|\varphi\rangle = 1$ (Alice's and Bob's outcomes are consistent).

$\longrightarrow$ Perfect quantum strategies for BLS games have a very specific form.

Perfect quantum strategies for binary linear system games

Definition [Solution group of a BLS (Cleve/Mittal)]

The solution group of a BLS $Mv = \mu$ is the group Γ generated by $g_1, \ldots, g_n$ and f, satisfying the following relations:

- Generators are involutions: $g_i^2 = e$ for all $1 \leqslant i \leqslant n$ and $f^2 = e$.
- f commutes with all other generators: $[g_i, f] = e$ for all $1 \leqslant i \leqslant n$.
- Local compatibility: if there exists $1 \leqslant k \leqslant p$ s.t. $M_{k,i} = M_{k,j} = 1$, then $[g_i, g_j] = e$.
- Constraint satisfaction: $g_1^{M_{k,1}} \cdots g_n^{M_{k,n}} = f^{\mu_k}$ for all $1 \leqslant k \leqslant p$.

Notation: e is the identity of Γ and $[a, b] = aba^{-1}b^{-1}$ is the commutator of a, b.

Perfect quantum strategies for binary linear system games

Definition [Solution group of a BLS (Cleve/Mittal)]

The solution group of a BLS $Mv = \mu$ is the group Γ generated by $g_1, \ldots, g_n$ and f, satisfying the following relations:

- Generators are involutions: $g_i^2 = e$ for all $1 \leqslant i \leqslant n$ and $f^2 = e$.
- f commutes with all other generators: $[g_i, f] = e$ for all $1 \leqslant i \leqslant n$.
- Local compatibility: if there exists $1 \leqslant k \leqslant p$ s.t. $M_{k,i} = M_{k,j} = 1$, then $[g_i, g_j] = e$.
- Constraint satisfaction: $g_1^{M_{k,1}} \cdots g_n^{M_{k,n}} = f^{\mu_k}$ for all $1 \leqslant k \leqslant p$.

Notation: e is the identity of Γ and $[a,b] = aba^{-1}b^{-1}$ is the commutator of a, b.

Recall the following definition: A d-dimensional representation of a finite group G is a homomorphism $\sigma : G \to \mathbf{C}^{d\times d}$ from G to the group of invertible linear operators on $\mathbf{C}^d$.

Perfect quantum strategies for binary linear system games

Definition [Solution group of a BLS (Cleve/Mittal)]

The solution group of a BLS $Mv = \mu$ is the group Γ generated by $g_1, \ldots, g_n$ and f, satisfying the following relations:

- Generators are involutions: $g_i^2 = e$ for all $1 \leqslant i \leqslant n$ and $f^2 = e$.
- f commutes with all other generators: $[g_i, f] = e$ for all $1 \leqslant i \leqslant n$.
- Local compatibility: if there exists $1 \leqslant k \leqslant p$ s.t. $M_{k,i} = M_{k,j} = 1$, then $[g_i, g_j] = e$.
- Constraint satisfaction: $g_1^{M_{k,1}} \cdots g_n^{M_{k,n}} = f^{\mu_k}$ for all $1 \leqslant k \leqslant p$.

Notation: e is the identity of Γ and $[a, b] = aba^{-1}b^{-1}$ is the commutator of a, b.

Recall the following definition: A d-dimensional representation of a finite group G is a homomorphism $\sigma : G \to \mathbf{C}^{d \times d}$ from G to the group of invertible linear operators on $\mathbf{C}^d$.

Theorem [Characterizing perfect quantum strategies for BLS games (Cleve/Liu/Slofstra)]

Let $Mv = \mu$ be a BLS. The following are equivalent:

1. There is a perfect quantum strategy for the associated game.
2. The associated solution group Γ has a finite-dimensional representation σ s.t. $\sigma(f) = -I$.

Idea of the proof

(2) $\Rightarrow$ (1): Let $\sigma : \Gamma \to \mathbf{C}^{d\times d}$, with $\sigma(f) = -I$, be a finite-dimensional representation of the solution group of the BLS. Fixing an orthonormal basis of $\mathbf{C}^d$, set $|\varphi\rangle := |\psi\rangle$ (the maximally entangled state on $\mathbf{C}^d \otimes \mathbf{C}^d$) and, for all x, y s.t. $M_{x,y} = 1$, $A_{x,y} := \sigma(g_y), B_y := \sigma(g_y)^T$.
This defines a perfect quantum strategy for the BLS game.
Indeed, the equation satisfaction and consistency properties are satisfied:

- for all x, $\langle\varphi|A_{x,1}^{M_{x,1}} \cdots A_{x,n}^{M_{x,n}} \otimes I|\varphi\rangle = \langle\psi|\underbrace{\sigma(g_1)^{M_{x,1}} \cdots \sigma(g_n)^{M_{x,n}}}_{=\sigma\left(g_1^{M_{x,1}}\cdots g_n^{M_{x,n}}\right)=\sigma(f^{\mu_x})=\sigma(f)^{\mu_x}=(-I)^{\mu_x}} \otimes I|\psi\rangle = (-1)^{\mu_x}$,
- for all x, y s.t. $M_{x,y} = 1$, $\langle\varphi|A_{x,y} \otimes B_y|\varphi\rangle = \langle\psi|\sigma(g_y) \otimes \sigma(g_y)^T|\psi\rangle \underset{(\star)}{=} \langle\psi|\underbrace{\sigma(g_y)^2}_{=\sigma(g_y^2)=\sigma(e)=I} \otimes I|\psi\rangle = 1$.

  $(\star)$ is because $M \otimes N^T|\psi\rangle = MN \otimes I|\psi\rangle$

Similarly, the involution and commutation properties of the g_y's imply those of the $A_{x,y}$'s, B_y's.

Idea of the proof

(2) $\Rightarrow$ (1): Let $\sigma : \Gamma \to \mathbf{C}^{d\times d}$, with $\sigma(f) = -I$, be a finite-dimensional representation of the solution group of the BLS. Fixing an orthonormal basis of $\mathbf{C}^d$, set $|\varphi\rangle := |\psi\rangle$ (the maximally entangled state on $\mathbf{C}^d \otimes \mathbf{C}^d$) and, for all x, y s.t. $M_{x,y} = 1$, $A_{x,y} := \sigma(g_y), B_y := \sigma(g_y)^T$.
This defines a perfect quantum strategy for the BLS game.
Indeed, the equation satisfaction and consistency properties are satisfied:

- for all x, $\langle\varphi|A_{x,1}^{M_{x,1}} \cdots A_{x,n}^{M_{x,n}} \otimes I|\varphi\rangle = \langle\psi|\underbrace{\sigma(g_1)^{M_{x,1}} \cdots \sigma(g_n)^{M_{x,n}}}_{=\sigma\left(g_1^{M_{x,1}} \cdots g_n^{M_{x,n}}\right) = \sigma(f^{\mu_x}) = \sigma(f)^{\mu_x} = (-I)^{\mu_x}} \otimes I|\psi\rangle = (-1)^{\mu_x}$,
- for all x, y s.t. $M_{x,y} = 1$, $\langle\varphi|A_{x,y} \otimes B_y|\varphi\rangle = \langle\psi|\sigma(g_y) \otimes \sigma(g_y)^T|\psi\rangle \underset{(\star)}{=} \langle\psi|\underbrace{\sigma(g_y)^2}_{=\sigma(g_y^2)=\sigma(e)=I} \otimes I|\psi\rangle = 1$.

  $(\star)$ is because $M \otimes N^T|\psi\rangle = MN \otimes I|\psi\rangle$

Similarly, the involution and commutation properties of the g_y's imply those of the $A_{x,y}$'s, B_y's.

(1) $\Rightarrow$ (2): Let $(\{A_{x,y}, B_y \in \mathbf{C}^{d\times d}\}_{x,y}, |\varphi\rangle \in \mathbf{C}^d \otimes \mathbf{C}^d)$ be a perfect quantum strategy for the BLS game. Set $E := \mathrm{supp}(\varphi_A) \subset \mathbf{C}^d$, where $\varphi_A := \mathrm{I}_A \otimes \mathrm{Tr}_B(|\varphi\rangle\langle\varphi|_{AB})$, and P_E the projector onto E.
By assumption, for any x, y s.t. $M_{x,y} = 1$, $\langle\varphi|A_{x,y} \otimes B_y|\varphi\rangle = 1$, which means that $|\varphi\rangle = A_{x,y} \otimes B_y|\varphi\rangle$, i.e. $A_{x,y} \otimes I|\varphi\rangle = I \otimes B_y^{-1}|\varphi\rangle$. Hence, for any x, x', y s.t. $M_{x,y} = M_{x',y} = 1$, $A_{x,y} \otimes I|\varphi\rangle = A_{x',y} \otimes I|\varphi\rangle$, which implies that $P_E A_{x,y} P_E = P_E A_{x',y} P_E =: A_y$.
The homomorphism $\sigma : \Gamma \to \mathbf{C}^{d\times d}$ defined by $\sigma(g_y) = A_y$ for all y and $\sigma(f) = -I$ is a finite-dimensional representation of Γ.

Rigidity for binary linear system games

Recall the following definitions:

- A representation of a finite group is irreducible if it cannot be decomposed into a direct sum of representations, each of non-zero dimension.
- Two representations σ_1, σ_2 of a finite group G are equivalent if there exists a unitary U s.t. $\sigma_2(g) = U\sigma_1(g)U^*$ for all $g \in G$.

Rigidity for binary linear system games

Recall the following definitions:

- A representation of a finite group is irreducible if it cannot be decomposed into a direct sum of representations, each of non-zero dimension.
- Two representations σ_1, σ_2 of a finite group G are equivalent if there exists a unitary U s.t. $\sigma_2(g) = U\sigma_1(g)U^*$ for all $g \in G$.

Theorem [Rigidity for BLS games (Coladangelo/Stark)]

Let $Mv = \mu$ be a BLS with associated solution group Γ. Assume that Γ is finite and that all its irreducible finite-dimensional representations which map f to $-I$ are equivalent to a given irreducible finite-dimensional representation $\hat{\sigma} : \Gamma \to \mathbf{C}^{d\times d}$.
Suppose that $\left(|\varphi\rangle \in \mathbf{C}^{d'} \otimes \mathbf{C}^{d'}, \{A_{x,y}, B_y \in \mathbf{C}^{d'\times d'}\}_{x\in\{1,\ldots,p\}, y\in\{1,\ldots,n\}, M_{x,y}=1}\right)$ is a perfect quantum strategy for the associated game. Then, there exist $s \in \mathbf{N}$ and isometries $U, V : \mathbf{C}^{d'} \to \mathbf{C}^d \otimes \mathbf{C}^s$ s.t., for all $x \in \{1, \ldots, p\}, y \in \{1, \ldots, n\}$ s.t. $M_{x,y} = 1$, $UA_{x,y}U^* = \hat{\sigma}(g_y) \otimes I$ and $VB_yV^* = \hat{\sigma}(g_y)^T \otimes I$.

Rigidity for binary linear system games

Recall the following definitions:

- A representation of a finite group is irreducible if it cannot be decomposed into a direct sum of representations, each of non-zero dimension.
- Two representations σ_1, σ_2 of a finite group G are equivalent if there exists a unitary U s.t. $\sigma_2(g) = U\sigma_1(g)U^*$ for all $g \in G$.

Theorem [Rigidity for BLS games (Coladangelo/Stark)]

Let $Mv = \mu$ be a BLS with associated solution group Γ. Assume that Γ is finite and that all its irreducible finite-dimensional representations which map f to $-I$ are equivalent to a given irreducible finite-dimensional representation $\hat{\sigma} : \Gamma \to \mathbf{C}^{d \times d}$.
Suppose that $\left(|\varphi\rangle \in \mathbf{C}^{d'} \otimes \mathbf{C}^{d'}, \{A_{x,y}, B_y \in \mathbf{C}^{d' \times d'}\}_{x \in \{1,\ldots,p\}, y \in \{1,\ldots,n\}, M_{x,y}=1}\right)$ is a perfect quantum strategy for the associated game. Then, there exist $s \in \mathbf{N}$ and isometries $U, V : \mathbf{C}^{d'} \to \mathbf{C}^{d} \otimes \mathbf{C}^{s}$ s.t., for all $x \in \{1, \ldots, p\}, y \in \{1, \ldots, n\}$ s.t. $M_{x,y} = 1$, $UA_{x,y}U^* = \hat{\sigma}(g_y) \otimes I$ and $VB_yV^* = \hat{\sigma}(g_y)^T \otimes I$.

Proof idea:
We know that a perfect quantum strategy on $\mathbf{C}^{d'} \otimes \mathbf{C}^{d'}$ is equivalent to a representation $\sigma : \Gamma \to \mathbf{C}^{d' \times d'}$ s.t. $\sigma(f) = -I$. Decompose σ into a direct sum of irreducible representations, as $\sigma = \bigoplus_{i=1}^{s} \sigma_i$. We then have $\bigoplus_{i=1}^{s} \sigma_i(f) = \sigma(f) = -I_{d'}$, so necessarily $\sigma_i(f) = -I_{d_i}$ for each i. Hence by assumption, all σ_i's are equivalent to $\hat{\sigma}$. And thus σ is equivalent to $\bigoplus_{i=1}^{s} \hat{\sigma} \equiv \hat{\sigma} \otimes I_s$.

A few facts about the Pauli group

Definition [n-qubit Pauli group]

The n-qubit Pauli group $\mathcal{P}^{\otimes n}$, seen as "presented over $\mathbf{Z}_2$" (Slofstra), is the group which is generated by $\{x_1, \ldots, x_n, z_1, \ldots, z_n, f\}$, satisfying the relations:

- $f^2 = e$ and $x_i^2 = z_i^2 = e$ for all i
- $[x_i, f] = [z_i, f] = e$ for all i

} standard relations of a group presented over $\mathbf{Z}_2$

- $[x_i, z_i] = f$ for all i
- $[x_i, x_j] = [z_i, z_j] = [x_i, z_j] = e$ for all $i \neq j$

} additional relations

A few facts about the Pauli group

Definition [n-qubit Pauli group]

The n-qubit Pauli group $\mathcal{P}^{\otimes n}$, seen as "presented over $\mathbf{Z}_2$" (Slofstra), is the group which is generated by $\{x_1, \ldots, x_n, z_1, \ldots, z_n, f\}$, satisfying the relations:

- $f^2 = e$ and $x_i^2 = z_i^2 = e$ for all i
- $[x_i, f] = [z_i, f] = e$ for all i

} standard relations of a group presented over $\mathbf{Z}_2$

- $[x_i, z_i] = f$ for all i
- $[x_i, x_j] = [z_i, z_j] = [x_i, z_j] = e$ for all $i \neq j$

} additional relations

$\mathcal{P}^{\otimes n}$ has a natural 2^n-dimensional representation $\pi : \mathcal{P}^{\otimes n} \to (\mathbf{C}^{2\times 2})^{\otimes n}$, defined by:

- $\pi(f) = -I^{\otimes n}$
- $\pi(x_i) = I^{\otimes(i-1)} \otimes X \otimes I^{\otimes(n-i)}$ for all i
- $\pi(z_i) = I^{\otimes(i-1)} \otimes Z \otimes I^{\otimes(n-i)}$ for all i

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

This representation of $\mathcal{P}^{\otimes n}$ is irreducible. The other non-equivalent irreducible representations of $\mathcal{P}^{\otimes n}$ are 2^{2n} 1-dimensional representations, all sending f on the identity.

A few facts about the Pauli group

Definition [*n*-qubit Pauli group]

The n-qubit Pauli group $\mathcal{P}^{\otimes n}$, seen as "presented over $\mathbf{Z}_2$" (Slofstra), is the group which is generated by $\{x_1, \ldots, x_n, z_1, \ldots, z_n, f\}$, satisfying the relations:

- $f^2 = e$ and $x_i^2 = z_i^2 = e$ for all i
- $[x_i, f] = [z_i, f] = e$ for all i

} standard relations of a group presented over $\mathbf{Z}_2$

- $[x_i, z_i] = f$ for all i
- $[x_i, x_j] = [z_i, z_j] = [x_i, z_j] = e$ for all $i \neq j$

} additional relations

$\mathcal{P}^{\otimes n}$ has a natural 2^n-dimensional representation $\pi : \mathcal{P}^{\otimes n} \to (\mathbf{C}^{2\times 2})^{\otimes n}$, defined by:

- $\pi(f) = -I^{\otimes n}$
- $\pi(x_i) = I^{\otimes(i-1)} \otimes X \otimes I^{\otimes(n-i)}$ for all i
- $\pi(z_i) = I^{\otimes(i-1)} \otimes Z \otimes I^{\otimes(n-i)}$ for all i

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

This representation of $\mathcal{P}^{\otimes n}$ is irreducible. The other non-equivalent irreducible representations of $\mathcal{P}^{\otimes n}$ are 2^{2n} 1-dimensional representations, all sending f on the identity.

Proof: Given a finite group G, the two following facts hold:

- A representation σ of G is irreducible iff $\sum_{g\in G} \mathrm{Tr}(\sigma(g))\,\mathrm{Tr}(\sigma(g)^{-1}) = |G|$.
- A set S of non-equivalent irreducible representations of G is maximal iff $\sum_{\sigma\in S} |\sigma|^2 = |G|$.

Applying the above to $G = \mathcal{P}^{\otimes n}$, $\sigma = \pi$, $S = \{\pi, \sigma_1, \ldots, \sigma_{2^{2n}}\}$, we do get equalities (to 2^{2n+1}).

Rigidity for the Magic Square game

Observation: The solution group of the MS game is the 2-qubit Pauli group $\mathcal{P}^{\otimes 2}$, generated by $\{x_1, x_2, z_1, z_2, f\}$. Indeed, $g_1 = z_2$, $g_2 = z_1 z_2$, $g_3 = z_1$, $g_4 = x_1 z_2$, $g_5 = z_1 x_1 x_2 z_2$, $g_6 = z_1 x_2$, $g_7 = x_1$, $g_8 = x_1 x_2$, $g_9 = x_2$ satisfy the MS solution group relations.

Rigidity for the Magic Square game

Observation: The solution group of the MS game is the 2-qubit Pauli group $\mathcal{P}^{\otimes 2}$, generated by $\{x_1, x_2, z_1, z_2, f\}$. Indeed, $g_1 = z_2$, $g_2 = z_1 z_2$, $g_3 = z_1$, $g_4 = x_1 z_2$, $g_5 = z_1 x_1 x_2 z_2$, $g_6 = z_1 x_2$, $g_7 = x_1$, $g_8 = x_1 x_2$, $g_9 = x_2$ satisfy the MS solution group relations.

Theorem [Rigidity for MS game]

Let $\left(|\varphi\rangle \in \mathbf{C}^d \otimes \mathbf{C}^d, \{A_{x,y}, B_y \in \mathbf{C}^{d\times d}\}_{x\in\{1,\dots,6\}, y\in\{1,\dots,9\}, v_y \text{ in } (e_x)}\right)$ be a perfect quantum strategy for the MS game. Then, there exist $s \in \mathbf{N}$ and isometries $U, V : \mathbf{C}^d \to \mathbf{C}^4 \otimes \mathbf{C}^s$ s.t.

- $U \otimes V|\varphi\rangle = |\psi\rangle \otimes |\theta\rangle$ for some $|\theta\rangle \in \mathbf{C}^s \otimes \mathbf{C}^s$,
- for all $x \in \{1,\dots,6\}, y \in \{1,\dots,9\}$ s.t. v_y in (e_x), $UA_{x,y}U^* = VB_yV^* = \pi(g_y) \otimes I$.
  Concretely: $\pi(g_1) = I \otimes Z$, $\pi(g_2) = Z \otimes Z$, $\pi(g_3) = Z \otimes I$, $\pi(g_4) = X \otimes Z$, $\pi(g_5) = ZX \otimes XZ$, $\pi(g_6) = Z \otimes X$, $\pi(g_7) = X \otimes I$, $\pi(g_8) = X \otimes X$, $\pi(g_9) = I \otimes X$.

Observation: The solution group of the MS game is the 2-qubit Pauli group $\mathcal{P}^{\otimes 2}$, generated by $\{x_1, x_2, z_1, z_2, f\}$. Indeed, $g_1 = z_2$, $g_2 = z_1 z_2$, $g_3 = z_1$, $g_4 = x_1 z_2$, $g_5 = z_1 x_1 x_2 z_2$, $g_6 = z_1 x_2$, $g_7 = x_1$, $g_8 = x_1 x_2$, $g_9 = x_2$ satisfy the MS solution group relations.

Theorem [Rigidity for MS game]

Let $\left(|\varphi\rangle \in \mathbf{C}^d \otimes \mathbf{C}^d, \{A_{x,y}, B_y \in \mathbf{C}^{d\times d}\}_{x\in\{1,\dots,6\}, y\in\{1,\dots,9\}, v_y \text{ in } (e_x)}\right)$ be a perfect quantum strategy for the MS game. Then, there exist $s \in \mathbf{N}$ and isometries $U, V : \mathbf{C}^d \to \mathbf{C}^4 \otimes \mathbf{C}^s$ s.t.

- $U \otimes V|\varphi\rangle = |\psi\rangle \otimes |\theta\rangle$ for some $|\theta\rangle \in \mathbf{C}^s \otimes \mathbf{C}^s$,
- for all $x \in \{1,\dots,6\}, y \in \{1,\dots,9\}$ s.t. v_y in (e_x), $UA_{x,y}U^* = VB_yV^* = \pi(g_y) \otimes I$. Concretely: $\pi(g_1) = I \otimes Z$, $\pi(g_2) = Z \otimes Z$, $\pi(g_3) = Z \otimes I$, $\pi(g_4) = X \otimes Z$, $\pi(g_5) = ZX \otimes XZ$, $\pi(g_6) = Z \otimes X$, $\pi(g_7) = X \otimes I$, $\pi(g_8) = X \otimes X$, $\pi(g_9) = I \otimes X$.

Proof:

- Form of the observables: It follows directly from the general rigidity theorem for BLS games, together with the facts about the representation theory of $\mathcal{P}^{\otimes 2}$.
- Form of the state: By assumption we have, for all x, y s.t. v_y in (e_x), $\langle\varphi|A_{x,y} \otimes B_y|\varphi\rangle = 1$. Hence, $|\tilde{\varphi}\rangle := U \otimes V|\varphi\rangle$ is s.t., for all y, $\langle\tilde{\varphi}|\pi(g_y) \otimes \pi(g_y) \otimes I|\tilde{\varphi}\rangle = 1$, which means that $|\tilde{\varphi}\rangle = \pi(g_y) \otimes \pi(g_y) \otimes I|\tilde{\varphi}\rangle$. This implies that $|\tilde{\varphi}\rangle = |\chi_1\rangle \otimes |\chi_2\rangle \otimes |\theta\rangle$ with $|\chi_i\rangle \in \mathbf{C}^2 \otimes \mathbf{C}^2$ invariant under $X \otimes X$ and $Z \otimes Z$, and thus maximally entangled. So $|\chi_1\rangle \otimes |\chi_2\rangle = |\psi\rangle$.

Outlook

- We have seen that, given a BLS, there is a one-to-one correspondence between perfect quantum tensor product strategies for the associated game and finite-dimensional representations of the associated solution group mapping a distinguished element on $-I$. Similarly, it can be shown that perfect quantum commuting strategies are equivalent to (possibly infinite-dimensional) such representations (Cleve/Liu/Slofstra).

Outlook

- We have seen that, given a BLS, there is a one-to-one correspondence between perfect quantum tensor product strategies for the associated game and finite-dimensional representations of the associated solution group mapping a distinguished element on $-I$. Similarly, it can be shown that perfect quantum commuting strategies are equivalent to (possibly infinite-dimensional) such representations (Cleve/Liu/Slofstra).
- Through the representation theory of the n-qubit Pauli group, one can design BLS games that self-test the maximally entangled state on $\mathbf{C}^{2^n} \otimes \mathbf{C}^{2^n}$. For instance: CHSH or MS game performed in parallel, or so-called Pauli-braiding test (cf. next week).
$\longrightarrow$ Entanglement dimension certification: passing one of these tests requires an entangled state of local dimension 2^n.

Outlook

- We have seen that, given a BLS, there is a one-to-one correspondence between perfect quantum tensor product strategies for the associated game and finite-dimensional representations of the associated solution group mapping a distinguished element on $-I$. Similarly, it can be shown that perfect quantum commuting strategies are equivalent to (possibly infinite-dimensional) such representations (Cleve/Liu/Slofstra).
- Through the representation theory of the n-qubit Pauli group, one can design BLS games that self-test the maximally entangled state on $\mathbf{C}^{2^n} \otimes \mathbf{C}^{2^n}$. For instance: CHSH or MS game performed in parallel, or so-called Pauli-braiding test (cf. next week).
  $\longrightarrow$ Entanglement dimension certification: passing one of these tests requires an entangled state of local dimension 2^n.
- Need: Robust version of these results (again, cf. next week).
  Namely: Given a game G, if a strategy p' is s.t. $\omega(G, p') \geqslant \omega_q(G) - \varepsilon$, then p' is $\delta(\varepsilon)$-close to p (up to local isometries).

References

Papers:

- J. Bowles, I. Šupić. Self-testing of quantum systems: a review. 2019.
- R. Cleve, P. Høyer, B. Toner, J. Watrous. Consequences and limits of nonlocal strategies. 2004.
- R. Cleve, L. Liu, W. Slofstra. Perfect commuting-operator strategies for linear system games. 2016.
- R. Cleve, R. Mittal. Characterization of binary constraint system games. 2013.
- A. Coladangelo, J. Stark. Robust self-testing for linear constraint system games. 2017.
- D. Mayers, A. Yao. Self testing quantum apparatus. 2004.
- N.D. Mermin. Simple unified form for the major no-hidden-variables theorems. 1990.
- A. Peres. Incompatible results of quantum measurements. 1990.
- W. Slofstra. Tsirelson's problem and an embedding theorem for groups arising from non-local games. 2019.

Lecture notes:

- R. Cleve. Entanglement and non-local effects, *Lecture Notes*. 2019.
- T. Vidick. Quantum multiplayer games, testing and rigidity, *UCSD Summer School Notes*. 2018.