NONLOCAL GAMES FROM QUANTUM CODES

ZHENGFENG JI

UNIVERSITY OF TECHNOLOGY SYDNEY

OUTLINE

- Nonlocal Games
- There Different Designs of Games for Codes
- Rigidity: Techniques and Applications
- Conclusions

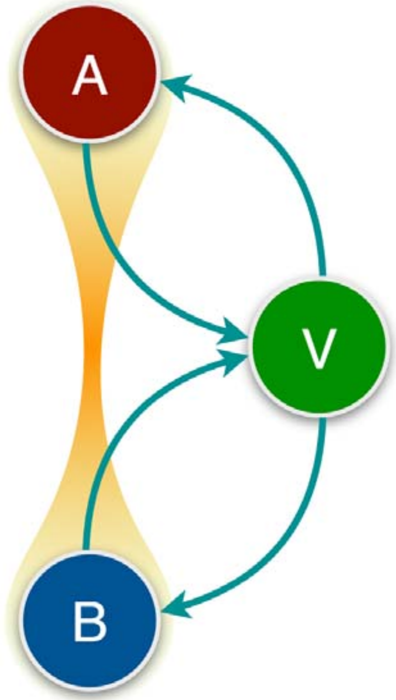
NONLOCAL GAMES

INTRODUCTION

Nonlocal Games

One-round multi-player game with **entangled** players

1. Referee V samples a pair of questions (s, t), sends s, t to the players A and B respectively.
2. Players A and B measure their **entangled** systems and respond with answers a, b.
3. The referee accepts or rejects using predicate $V(a, b|s, t)$.



BACKGROUND

- Computer Science

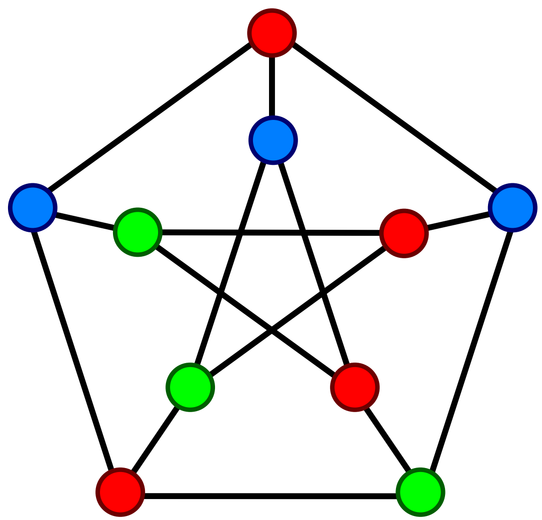
  Multi-prover interactive proofs (MIP), PCP theorem (PCP), parallel repetition theorem

- Constraint-Variable Game for SAT problems

  $(x_1 \lor x_2 \lor x_4) \land (\neg x_2 \lor x_3 \lor x_4) \land \cdots$

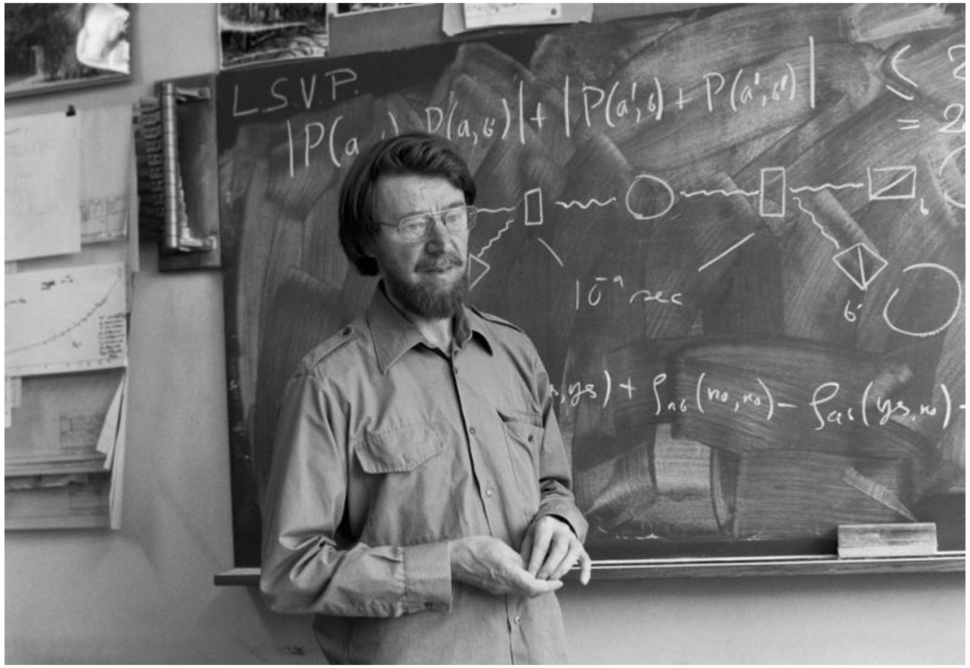
- Graph Coloring Game for graphs

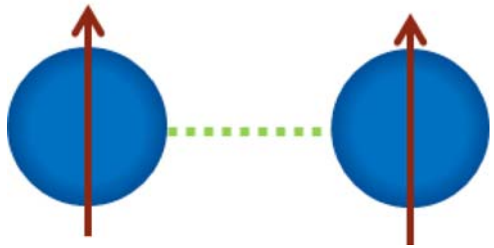
- The power of the second player
- The power of entangled players



- Physics

  Bell inequalities: quantum mechanics versus local hidden variable theories





$$\langle A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1 \rangle \leq 2$$

[Bell '64]

[Clauser, Horne, Shimony and Holt '69]

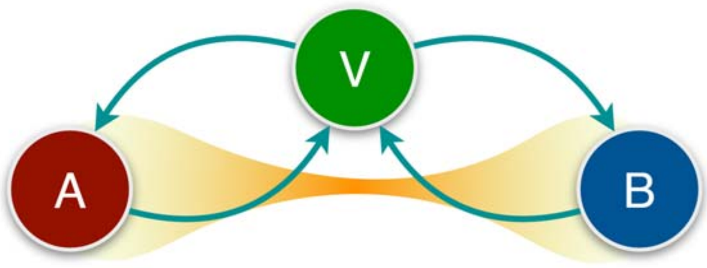
CHSH GAME

CHSH GAME

V randomly samples $s, t \in \{0,1\}$
and accepts if and only if

$$a \oplus b = s \wedge t.$$

CHSH: $a \oplus b = s \wedge t$

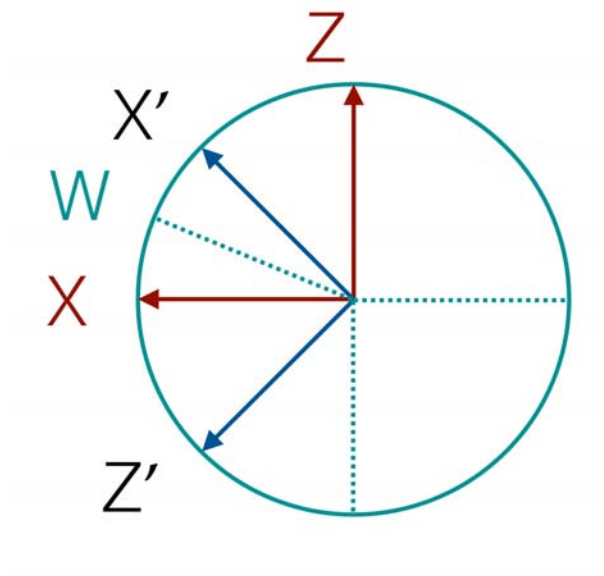


- Optimal strategy

EPR state: $(|00\rangle + |11\rangle)/\sqrt{2}$

Alice: X, Z

Bob: $X' = \frac{X+Z}{\sqrt{2}}, \quad Z' = \frac{X-Z}{\sqrt{2}}$



- Rigidity

CHSH RIGIDITY

- Optimal strategy

  EPR state: $(|00\rangle + |11\rangle)/\sqrt{2}$

  Alice: X, Z

  Bob: $X' = \frac{X+Z}{\sqrt{2}}, Z' = \frac{X-Z}{\sqrt{2}}$

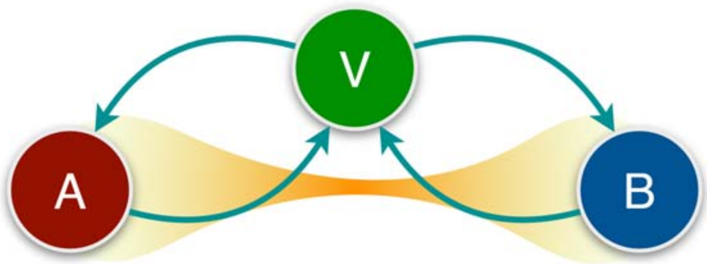
- Rigidity

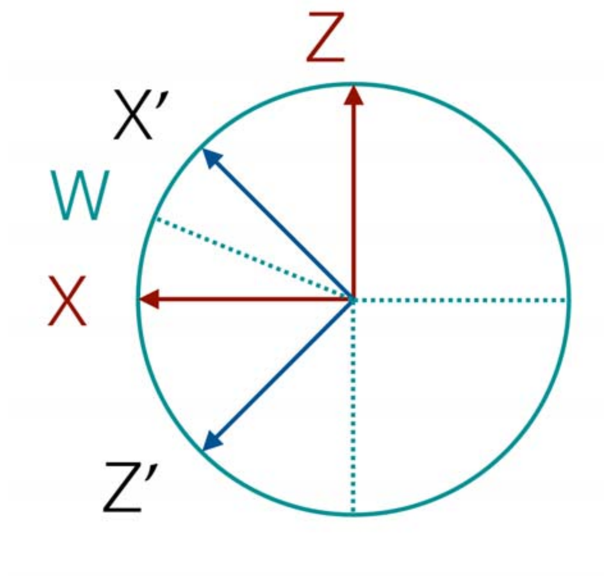
  Ask Alice to measure X, Z; ask Bob to measure X', Z'

  Jordan's Lemma

  Measurement specification questions

CHSH: $a \oplus b = s \wedge t$





FROM STATES TO SUBSPACES

- Stabilizer formalism

[Gottesman '97]

- Pauli group:

$$\left\{ e^{i\phi} \bigotimes_{j=1}^{n} D_j,\ \text{for } \phi \in \{0, \pi/2, \pi, 3\pi/2\},\ D_j \in \{I, X, Y, Z\} \right\}.$$

- A stabilizer is an abelian subgroup of the Pauli group not containing $-I$.
- The subspace stabilized by the stabilizer

Examples	Stabilizer
EPR	$\langle XX, ZZ \rangle$
GHZ	$\langle XXX, ZIZ, ZZI \rangle$
[4, 2, 2] Code	$\langle XXXX, ZZZZ \rangle$
Graph states	$\langle X_u \otimes \bigotimes_{v \sim u} Z_v \rangle$
[5, 1, 3] Code	$\langle XZZXI, IXZZX, XIXZZ, ZXIXZ \rangle$

CHSH GAME REVISITED

- Stabilizer formalism

CHSH: $a \oplus b = s \wedge t$

The EPR state is stabilized by XX, ZZ.

$$\langle XX + ZZ \rangle = 2$$

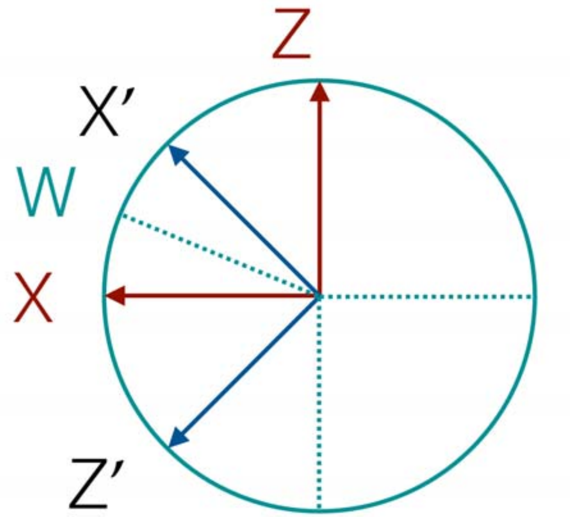
$$X = \frac{X' + Z'}{\sqrt{2}}, Z = \frac{X' - Z'}{\sqrt{2}}$$

$$\langle XX' + XZ' + ZX' - ZZ' \rangle = 2\sqrt{2}$$

X	X
Z	Z

+	X	X'
+	X	Z'
+	Z	X'
-	Z	Z'

+	0	0
+	0	1
+	1	0
-	1	1



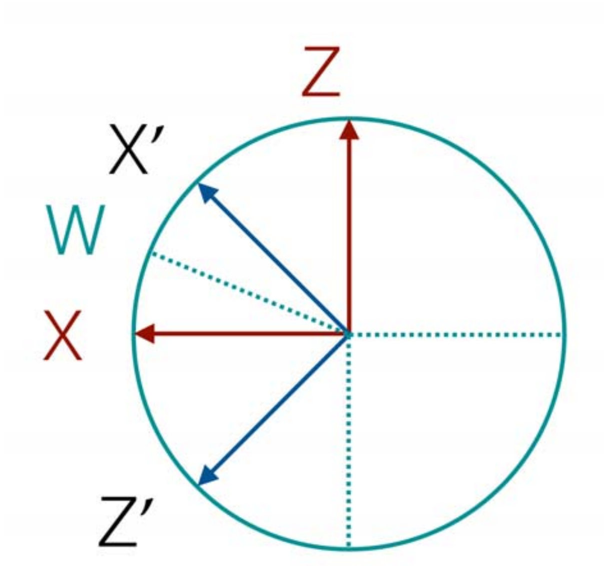
CHSH GAME REVISITED

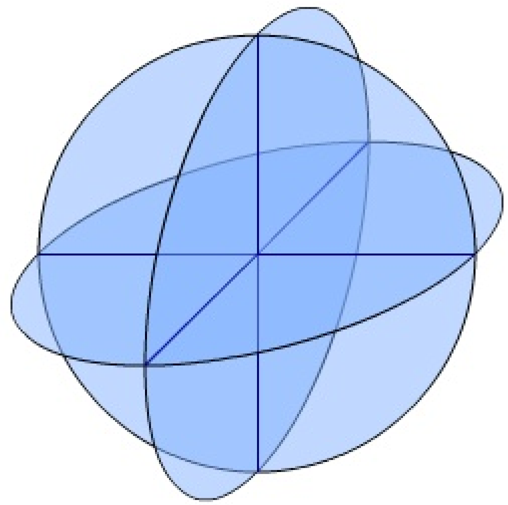
- The twist of the $\pi/4$ basis rotation in the optimal strategy

$$X' = \frac{X+Z}{\sqrt{2}}, Z' = \frac{X-Z}{\sqrt{2}}$$

- Why measurement specifications XX, ZZ won't work directly?
- For the singlet state $(|01\rangle - |10\rangle)/\sqrt{2}$

	I	X	Y	Z
I	1	0	0	0
X	0	-1	0	0
Y	0	0	-1	0
Z	0	0	0	-1





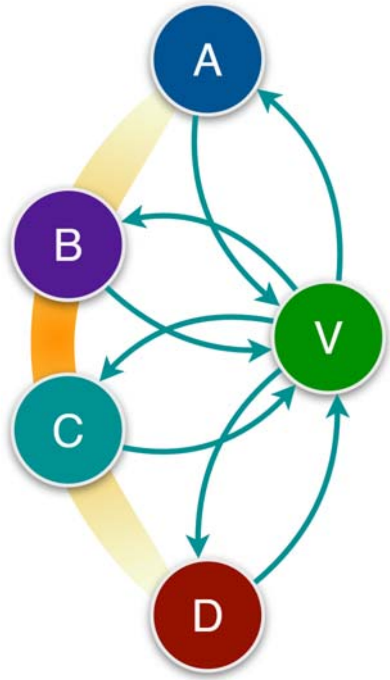
STABILIZER GAMES: METHOD I

- Special-player Stabilizer Game: apply the $\pi/4$ twist to the special player

X	X	X	X
Z	Z	Z	Z

+	X	X	X'	X
+	X	X	Z'	X
+	Z	Z	X'	Z
-	Z	Z	Z'	Z

+	0	0	2	0
+	0	0	3	0
+	1	1	2	1
-	1	1	3	1



- Special player: the third player
- Another view

  Regrouping the players: $(1, 2, 4)$ versus (3).
- No full rigidity, but partial rigidity

  The special player must measure honestly!

PARTIAL RIGIDITY OF THE SPECIAL-PLAYER GAME

Lemma (Partial Rigidity). For any quantum strategy $\mathcal{S} = (\rho, \{R_w^{(i)}\})$ of the special-player stabilizer game whose value is ϵ-close to the optimal value (nonlocal value), there exists an isometry $V : \mathcal{H}_3 \to \mathbb{C}^2 \otimes \hat{\mathcal{H}}_3$ such that

$$\begin{aligned} R_3^{(3)} &= \quad V^*(Z' \otimes I)V, \\ R_2^{(3)} &\approx_{\sqrt{\epsilon}} V^*(X' \otimes I)V. \end{aligned}$$

Follows the CHSH rigidity proof very closely.

STABILIZER GAME I

- The stabilizer game is a 4-player game with 2-bit questions and single-bit answers
- With equal probability, the verifier performs
  1. Random special-player games
  2. Direct checking of the stabilizer encoding

+	0	2	0	0
+	0	3	0	0
+	1	2	1	1
-	1	3	1	1

+	0	0	0	0
+	1	1	1	1

- Optimal strategy: share any state in the code space and measure honestly
- Recover full rigidity

MERMIN'S GHZ GAME

MERMIN'S GHZ GAME REVISITED

- Mermin's GHZ Game

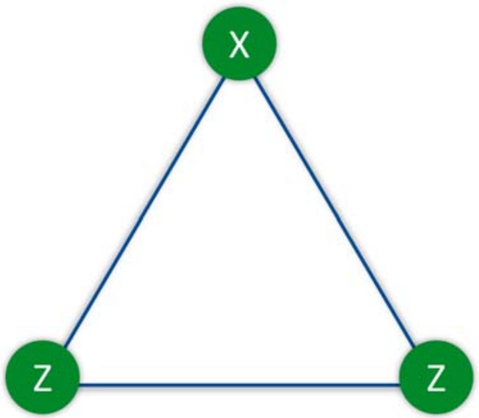
> 1. A game between the referee and Alice, Bob and Charlie,
> 2. The referee samples questions $(s, t, u) \in \{000, 011, 101, 110\}$ uniformly at random,
> 3. The referee accepts if the parity of the answers equals the half of the Hamming weight of all questions.

- Stabilizer for the triangle graph state

X	Z	Z
Z	X	Z
Z	Z	X

+	X	Z	Z
+	Z	X	Z
+	Z	Z	X
-	X	X	X

+	0	1	1
+	1	0	1
+	1	1	0
-	0	0	0



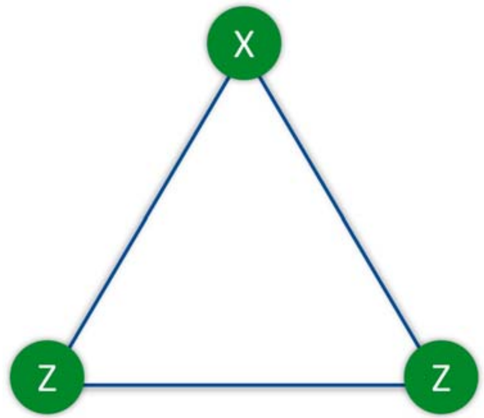
ANTI-COMMUTATIVITY FROM STABILIZERS

- Stabilizer for the graph state of the triangle graph

X	Z	Z
Z	X	Z
Z	Z	X

+	X	Z	Z
+	Z	X	Z
+	Z	Z	X
-	X	X	X

+	0	1	1
+	1	0	1
+	1	1	0
-	0	0	0



- Think of the X, Z operators in the stabilizer as the players' observables and may not be anti-commuting at all
- Magic: Take the product of the stabilizer operators!

  Proves the anti-commutativity of X, Z for the second player.
- How about other players?

STABILIZER GAMES: METHOD II

- Ideas from the Mermin's GHZ game

  Products of stabilizers such that exactly one column has the commutator product and all other columns cancel out completely

+	X	Z	Z
+	Z	X	Z
+	Z	Z	X
-	X	X	X

- Start with any quantum code, say, the [4,2,2] quantum error-detection code

X	X	X	X
Z	Z	Z	Z

- Concatenate it with [2,1,1] stabilized by YY
- A general recipe to construct rigid nonlocal games for stabilizer codes

STABILIZER GAMES: METHOD II

- An eight-qubit code with the following stabilizer generators

X	X	X	X	X	X	X	X
X	Z	X	Z	X	Z	X	Z
Y	Y	I	I	I	I	I	I
I	I	Y	Y	I	I	I	I
I	I	I	I	Y	Y	I	I
I	I	I	I	I	I	Y	Y

+	X	X	X	X	X	X	X	X
-	Z	Z	X	X	X	X	X	X
+	X	Z	X	Z	X	Z	X	Z
+	Z	X	X	Z	X	Z	X	Z

- Consider stabilizer operators without Y's
- Anti-commutativity from the products

EIGHT-PLAYER GAME: STABILIZER GAME II

Let Ξ be the subset of stabilizer operators of XZ-form for the eight-qubit code. The stabilizer game for the eight-qubit code is the eight-player nonlocal game defined as follows.

+	X	X	X	X	X	X	X	X
-	Z	Z	X	X	X	X	X	X
+	X	Z	X	Z	X	Z	X	Z
+	Z	X	X	Z	X	Z	X	Z

1. The referee selects one of the 32 operators from Ξ uniformly at random. Let $D^{(i)} \in \{X, Z\}$, $s \in \{0, 1\}$ be the i-th tensor factor and the sign of the chosen operator respectively.
2. For $i \in [8]$, the referee sends $D^{(i)}$ to player (i) and receive a bit $a^{(i)}$ back;
3. Accepts if $\bigoplus_{i=1}^{8} a^{(i)} = s$ and rejects otherwise.

RIGIDITY OF THE STABILIZER GAME II

Theorem. The nonlocal value of stabilizer game is 1. Furthermore, the game has the following rigidity property. Let $\mathcal{S} = \left(\rho, \left\{\hat{D}^{(i)}\right\}\right)$ be a strategy for the stabilizer game whose value is at least $1 - \epsilon$. Then, for all $i \in [8]$, there are isometries $V_i : \mathcal{H}_i \to \mathbb{C}^2 \otimes \hat{\mathcal{H}}_i$ such that

$$\begin{aligned} \hat{Z}^{(i)} &= \quad V_i^*(Z \otimes I)V_i, \\ \hat{X}^{(i)} &\approx_{\sqrt{\epsilon}} V_i^*(X \otimes I)V_i. \end{aligned}$$

Rigidity from anti-commutativity

EXTENDED NONLOCAL GAMES

EXTENDED NONLOCAL GAME

- Nonlocal Games versus Extended Nonlocal Games

  Question sets S, T, answer sets A, B, distribution π over $S \times T$ and a function V that specifies the acceptance rule of the referee.

Nonlocal Games	$V : A \times B \times S \times T \to [0, 1]$
Extended Nonlocal Games	$V : A \times B \times S \times T \to [0, I]$

[Johnston, Mittal, Russo and Watrous '16]
[Tomamichel, Fehr, Kaniewski and Wehner '13]

- Equivalently, the referee possesses a quantum system which the players choose how to initialize; the referee may measure and then decide
- Single-player extended nonlocal games are already interesting
- An easier way to achieve rigidity

EXTENDED EPR GAME

- Extended nonlocal game based on the stabilizer for EPR directly

X	X
Z	Z

+	X	0
+	Z	1

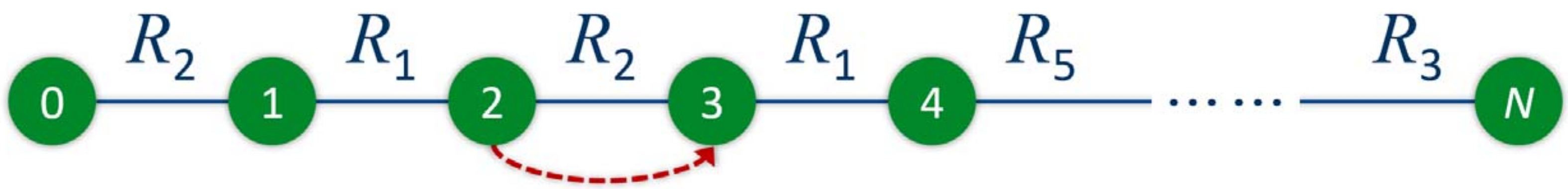
X	X
Z	Z
X	X
Z	Z

- Anti-commutativity and rigidity
- To achieve close-to-optimal value, the player must initialize the EPR state and measure honestly!

  Simplest example with rigidity?

PROPAGATION GAMES

- Reflections $R_1, R_2, \ldots, R_n$. A sequance $\mathfrak{R} = (R_{\zeta_i})_{i=1}^N$ of reflections with indices $\zeta_i \in [n]$



The propagation game is an extended nonlocal game in which the referee possesses a quantum system $\mathbb{C}^{N+1}$ and

1. selects an $i \in [N]$ uniformly at random and sends the index $j = \zeta_i \in [n]$ to the player and receives an answer bit a;
2. performs the projective measurement Π_i on his system and accepts if the outcome is 2 or equals to a.

RIGIDITY FOR PROPAGATION GAMES

- Beyond QECC: The history state subspace

$$\frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes R_{\zeta_t} R_{\zeta_{t-1}} \cdots R_{\zeta_1} |\psi\rangle,$$

  EPR is a history state of X propagation

- **Theorem**. Any strategy that has value at least $1 - \epsilon$ must use shared state that is $N^{3/2}\epsilon^{1/2}$-close to a history state in trace distance.

- Constraint Propagation Games

  Enforces the approximate linear constraints of reflections, including commutativity and anti-commutativity ($R_1 R_2 R_1 R_2 = \pm I$)

  Multi-qubit rigidity without encoding

RIGIDITY

APPROXIMATE STABILIZERS

- **Definition**. A contraction R (operator norm ≤ 1) ϵ-stabilizes state ρ if

$$\operatorname{Re}\operatorname{Tr}_\rho(R) \geq 1 - \epsilon.$$

- **Lemma**. If both R_0, R_1 ϵ-stabilize ρ, their product $R_0 R_1$ also $O(\epsilon)$-stabilizes ρ.
- What did we mean by $R_0 \approx_{\sqrt{\epsilon}} R_1$ in the statement of rigidity theorems?

$$\operatorname{Re}\operatorname{Tr}_\rho(R_0^* R_1) \approx_\epsilon 1.$$

Compare: $\|(R_0 - R_1)|\psi\rangle\|^2 \leq O(\epsilon)$.

- From the condition that a strategy has value ϵ-close to the nonlocal value, we have that the corresponding operators ϵ-stabilizer state ρ.

RIGIDITY FROM ANTI-COMMUTATIVITY

- **Definition**. Two contractions R_0, R_1 are ϵ-anti-commuting if

$$\mathrm{Re}\,\mathrm{Tr}_\rho(R_0 R_1 R_0 R_1) \approx_\epsilon -1.$$

- **Lemma**. Let R_0, R_1 be two traceless reflections such that

$$\mathrm{Re}\,\mathrm{Tr}_\rho(R_0 R_1 R_0 R_1) \approx_\epsilon -1.$$

  Then there exists a unitary $V : \mathcal{H} \to \mathbb{C}^2 \otimes \hat{\mathcal{H}}$ such that $R_1 = V^*(Z \otimes I)V$ and

$$\begin{aligned} R_1 &= \quad V^*(Z \otimes I)V, \\ R_0 &\approx_{\sqrt{\epsilon}} V^*(X \otimes I)V. \end{aligned}$$

- Qubit from anti-commutativity

  Where is the qubit?

MULTIPLE-QUBIT CASE

- Where are the qubits?
- General idea: prove commutativity between operators for different qubits.

  NP-hardness of nonlocal games

  [Kempe, Kobayashi, Matsumoto et al. '08], [Ito, Kobayashi and Matsumoto '09], [J '13]
- Confusability test, linearity test, and constraint propagation test

CONFUSABILITY TEST

- Ask Alice to measure qubits i, j at the same time, and Bob to measure one of the qubits (either i or j).

  Intuition: as i, j are measured at the same time, the measurement operators corresponding to i and j is commuting

- **Lemma**. Let R_1, R_2, S_1, S_2 be four reflections for Alice, and U_1, U_2 be two reflections for Bob. If S_1, S_2 commute, both R_1, S_1 are ϵ-consistent with U_1, and both R_2, S_2 are ϵ-consistent with U_2, then

$$\mathrm{Re}\,\mathrm{Tr}_\rho\left(R_1 R_2 R_1 R_2\right) \approx_\epsilon 1.$$

LINEARITY TEST AND CONSTRAINT PROPAGATION

- Nonlocal linearity test

  [Natarajan and Thomas Vidick '15]

  Similar to the confusability test, but more: $A(a)A(b)A(a+b) = I$.

- Constraint propagation game

  [J '16]

  An extended nonlocal game that enforces commutativity directly as a constraint ($R_0 R_1 R_0 R_1 = I$).

$$\frac{1}{\sqrt{5}}\Big(|0\rangle|\psi\rangle + |1\rangle R_1|\psi\rangle + |2\rangle R_0 R_1|\psi\rangle + |3\rangle R_1 R_0 R_1|\psi\rangle + |4\rangle R_0 R_1 R_0 R_1|\psi\rangle\Big).$$

MULTI-QUBIT RIGIDITY FORM THE MAGIC ISOMETRY

[McKague '16], [Fitzsimons and Vidick '15], [J '15]
[Chao, Reichardt, Sutherland and Vidick '17]

For $D \in \{X, Z\}$ and $u \in [n]$, define three versions of operators

Accents	Meanings
$\hat{D}_u$	From the strategy
$\tilde{D}_u$	Exactly anti-commuting, overlapping
$\check{D}_u$	Pauli operators, up to isometry

- Isometry: Add EPRs and SWAP sequentially!

$$W_u = (I \otimes V_u^*)\,\mathrm{SWAP}_u(|\mathrm{EPR}\rangle_u \otimes V_u),$$
$$V = W_n W_{n-1} \cdots W_1,$$
$$\check{D}_u = V^*(D_u \otimes I)V.$$

- An equivalent definition:

$$\check{D}_u = \mathcal{T}_1 \circ \cdots \circ \mathcal{T}_2 \circ \mathcal{T}_{u-1}(\tilde{D}_u), \text{ where}$$
$$\mathcal{T}_v(\sigma) = \frac{\rho + \tilde{X}_v\sigma\tilde{X}_v + \tilde{Z}_v\sigma\tilde{Z}_v + \tilde{X}_v\tilde{Z}_v\sigma\tilde{Z}_v\tilde{X}_v}{4}.$$

- Prove that $\check{D}_u$ and $\tilde{D}_u$ are close by rearranging operators and the Cauchy-Schwarz inequality
- Similar to the techniques for the nonlocal games for states

Constraint propagation game: no consistency on history states

APPLICATIONS

Rigidity + Encoding

APPLICATIONS

- Quantum proofs
  - Nonlocal games are QMA-hard
  - Nonlocal games are NEXP-hard, needs more delicate constructions of extended nonlocal games
- Delegation of quantum computation

  History state of the quantum computation as the shared entangled state
- Potential application in device-independent quantum information processing
  - Self-testing of multi-qubit entanglement
  - Device-independent quantum code encoding verification
  - Other DI quantum information processing tasks? Randomness amplification?

CONCLUSIONS

- Nonlocal Games from Quantum Codes
  - Three different methods
    - $\pi/4$-rotation
    - YY concatenation
    - Extended games
  - Open Problems and Future Work
    - A complete study of stabilizer game constructions
    - Other methods?
    - Go beyond anti-commutativity?
    - Other applications?

THANKS!