

Quantum bounds on linear games and applications

Ravishankar Ramanathan

National Quantum Information Centre of Gdansk
University of Gdansk

with R. Augusiak, G. Murta, Horodecki³

Dec 2015, NCKU



XOR Games

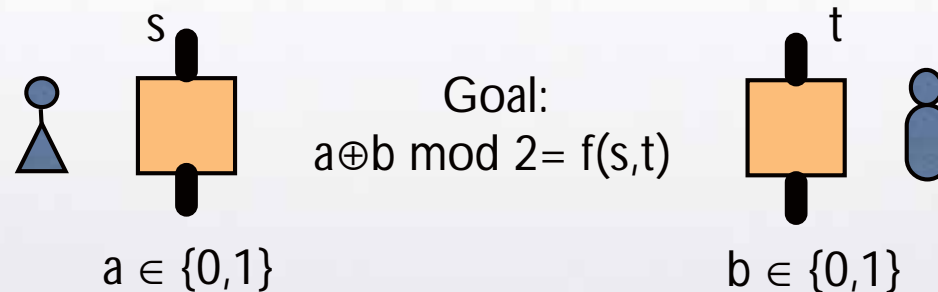
- XOR game: correlation Bell ineq. 2 parties, m settings, 2 outcomes.

$$\sum_{\substack{s \in S \\ t \in T}} P(s, t) \sum_{a, b \in \{0,1\}} P(a \oplus b = f(s, t) | s, t) \leq \omega_c(G) \leq \omega_q(G)$$

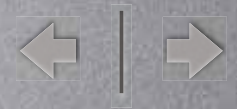
Classical Value
Deterministic assignments ($a = h(s), b = g(t)$)

Quantum value
Measurements on quantum states

$$\langle A_s B_t \rangle = P(a \oplus b = 0 | s, t) - P(a \oplus b = 1 | s, t)$$

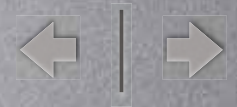


- CHSH: $f(s, t) = s \cdot t$ for $s, t \in \{0,1\}$.



XOR games

- XOR games: CHSH, Chain inequality, non-local computation game, GHZ-Mermin, Svetlichny ineq.
- Useful for:
 - Randomness Amplification (Chain Inequality, GHZ-Mermin game)
 - Quantum key distribution against no-signaling adversaries (Chain Inequality), against quantum adversaries (CHSH)
 - Randomness Expansion (CHSH, GHZ and other “self-testing” XOR games)
- Efficient computation of $\omega_q(G)$ for 2-party XOR games: semidefinite program from Tsirelson’s theorem

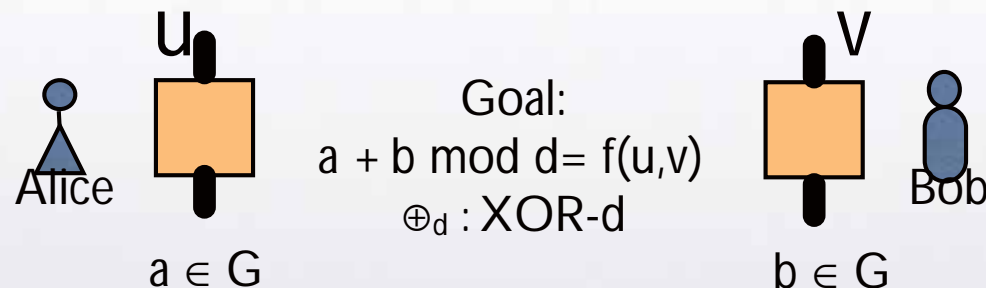


Linear game: XOR game with d outcomes

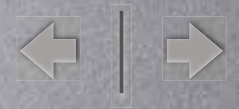
- Generalization of XOR games: “Linear games” with d outcomes.

Definition 1. A two-player linear game (g^1, q) is one where two players Alice and Bob receive questions u, v from sets Q_A and Q_B respectively, chosen from a probability distribution $q(u, v)$ by a referee. They reply with respective answers $a, b \in (G, +)$ where G is a finite Abelian group with associated operation $+$. The game is defined by a winning constraint $a + b = f(u, v)$ for some function $f : Q_A \times Q_B \rightarrow G$.

$$\omega(g) = \sum_{\substack{u \in Q_A \\ v \in Q_B}} \sum_{a, b \in G} q(u, v) P(a + b = f(u, v) | u, v).$$



- **XOR-d games** : Linear games with $G = \mathbb{Z}_d$, \oplus_d : addition modulo d.



Quantum value $\omega_q(\mathbf{G})$ of Linear games

- We propose an efficiently computable (norm-based) bound on $\omega_q(\mathbf{G})$ of linear games using Fourier transforms on finite abelian groups.

Theorem 2. *The quantum value of a linear game g^J with input sets Q_A, Q_B can be bounded as*

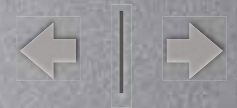
$$\omega_q(g^J) \leq \frac{1}{|G|} \left[1 + \sqrt{|Q_A||Q_B|} \sum_{x \in G \setminus \{e\}} \|\Phi_x\| \right], \quad (3)$$

where $\Phi_x = \sum_{(u,v) \in Q_A \times Q_B} q(u,v) \chi_x(f(u,v)) |u\rangle\langle v|$ are the game matrices, χ_x are the characters of the group G and $\|\cdot\|$ denotes the spectral norm. In particular, for an XOR- d game with m_A and m_B inputs for the two parties, the quantum value can be bounded as

$$\omega_q(g^\oplus) \leq \frac{1}{d} \left[1 + \sqrt{m_A m_B} \sum_{k=1}^{d-1} \|\Phi_k\| \right], \quad (4)$$

with $\Phi_k = \sum_{\substack{u \in [m_A] \\ v \in [m_B]}} q(u,v) \zeta^{kf(u,v)} |u\rangle\langle v|$ and $\zeta = \exp(2\pi i/d)$.

-

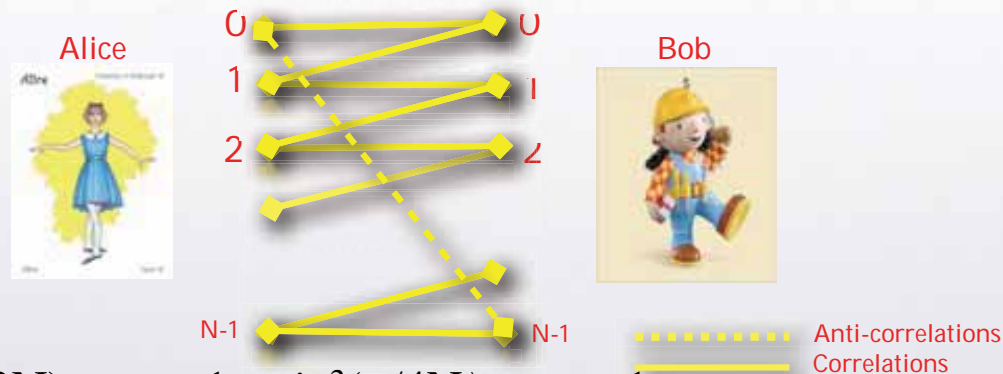


XOR-d

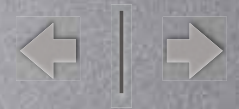
- Exists an optimal quantum strategy with fully random, correlated outputs.
 $P(a|u) = P(b|v) = 1/d$

- $a \longrightarrow a \oplus_d r,$ r : shared random dit
- $b \longrightarrow b \ominus_d r$

- For $w_q \longrightarrow 1$ (e.g. chained BI with $d=2$) , perfectly correlated outputs

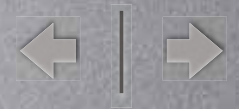


○ $w_c = 1 - 1/(2N), w_Q = 1 - \sin^2(\pi/4N), w_{ns} = 1.$



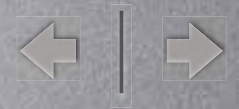
Questions

- Approx. asymptotic quantum and classical values of BIs.
- Identify BIs with unbounded violations. Open: 3 party, d outcome.
- Identify BIs that obey perfect parallel repetition for their quantum value.
- Are there finite BI with algebraic quantum violation, with random, correlated outputs for all no-signaling strategies?
- Can we identify BIs with no quantum advantage? Tightness.
- ...



Background

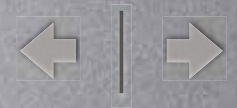
- Buhrman & Massar. Introduced the CHSH-3 game $a + b \bmod 3 = u.v \bmod 3$.
$$w_{q(\text{CHSH-3})} \leq 1/3 + 2/(3\sqrt{3})$$
- Liang et al. and Ji et al.. Numerically computed classical and quantum value up to $d = 13$ for CHSH-d. Upper bound from SDP hierarchy, lower bound
- Kempe, Regev and Toner. Showed quantum version of UGC false! For linear game with value $1 - \epsilon$, round an SDP to give quantum strategy that achieves $\geq 1 - 4\epsilon$.
- Bavarian and Shor: Asymptotic value of CHSH-d. Quantum bias: $\Omega(d^{-1/2})$. Classical bias: $\Omega(d^{-1/2})$ for $d = p^{2k}$ (prime p , integer k) and $O(d^{-1/2-\delta})$ for $d = p^{2k-1}$



CHSH-d

- **CHSH-d game:** Generalization of CHSH to $d > 2$ outputs.
- Alice and Bob are asked questions (u,v) from a finite field F_d of size d with input distribution $q(u,v) = 1/d^2$, where d is a prime or prime power.
- They return answers $a, b \in F_d$ to satisfy $a \oplus b = x \cdot y$, the arithmetic operations taken from the field F_d .
- Open question: Asymptotic separation between quantum and classical values for $d = p^{2k-1}$ for prime p , integer k ? Related to security of Bourgain's two-source extractor in the presence of quantum memory.

Problem 1.5 (Open). Does there exist an infinite family of $d = p^{2k-1}$ such that $\omega_q(\text{CHSH-d}) = \Omega(d^{-1/2})$, or some $\delta > 0$ and an infinite family of $d = p^{2k-1}$ such that $\omega_q(\text{CHSH-d}) = O(d^{-1-2\delta})$?



CHSH-d

- Recovers the quantum bound on CHSH-d obtained by Bavarian and Shor (arXiv: 1311.5186) using a different method.

Example [see also [20]] *The quantum value of the CHSH-d game for prime and prime power d , i.e., $d = p^r$ where p is prime and $r \geq 1$ is an integer, can be bounded as*

$$\omega_q(\text{CHSH} - d) \leq \frac{1}{d} + \frac{d-1}{d\sqrt{d}}. \quad (5)$$

Game Cost Matrix

		Bob's settings		
		0	1	2
Alice's settings	u \ v	0	1	2
	0	1	1	1
	1	1	ζ	ζ^2
	2	1	ζ^2	ζ

$\Phi_1 =$

$$\zeta = \exp(2i \pi/3)$$

$$a \oplus b \text{ mod } 3 = u.v \text{ mod } 3$$

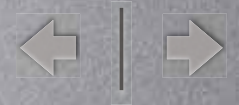


Pseudo-telepathy

- Which functions have a quantum but not classical winning strategy, i.e., $\omega_c(G) < \omega_q(G) = \omega_{ns}(G) = 1$?

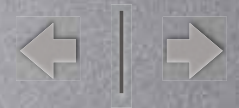
Lemma 4. For XOR-d games g^\oplus corresponding to total functions with m questions per player, when the input distribution is uniform $q(u, v) = 1/m^2$, $\omega_q(g^\oplus) = 1$ iff $\omega_c(g^\oplus) = 1$, i.e., when $\text{rank}(\Phi_1) = 1$.

- Any no-signaling box that wins a non-trivial xor-d game trivializes communication complexity. In particular, boxes $P(a,b|u,v) = 1/|G|$ for $a+b = f(u,v)$ and 0 otherwise.
- Extended to partial functions in Gnacinski et al. (arXiv: 1511.05415). Chained Bell inequalities are the best one can do.



When does $\omega_c(G) = \omega_q(G)$?

- Which functions have no quantum advantage over classical, i.e., $\omega_c(G) = \omega_q(G) < \omega_{ns}(G) = 1$?
- No quantum advantage in general Non-Local Computation: functions $f(z_1, \dots, z_n)$ from n dits to 1 dit.
 - Alice and Bob are given inputs x_i and y_i obeying $x_i \oplus_d y_i = z_i$ for $i \in [n]$ with each $p(x_i) = p(y_i) = 1/d$.
 - Goal: Output $a, b \in \{0, \dots, d-1\}$ such that $a \oplus_d b = f(x_1 \oplus_d y_1, \dots, x_n \oplus_d y_n)$.
 - Here we restrict to $f(x_1 \oplus_d y_1, \dots, x_{n-1} \oplus_d y_{n-1}) \cdot (x_n \oplus_d y_n)$.
 - Max. success prob. for any $p(z_1, \dots, z_n) = (1/d^{n+1}) p(x_1 \oplus_d y_1, \dots, x_{n-1} \oplus_d y_{n-1})$.

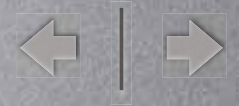


Non-Local Computation

- Non-Local Computation of functions NLC_d :
 - $a \oplus_d b = f(x_1 \oplus_d y_1, \dots, x_{n-1} \oplus_d y_{n-1}) \cdot (x_n \oplus_d y_n)$
 - Input distribution: $\frac{1}{d^{n+1}} p(x_{n-1} \oplus_d y_{n-1})$ (8)

Theorem 5. *The games NLC_d for arbitrary prime d and for input distribution satisfying (8) have no quantum advantage, i.e., $\omega_c(NLC_d) = \omega_q(NLC_d)$.*

- **Proof Idea:** Game matrices are diagonal in a basis composed of tensor products of Fourier vectors, we present a classical strategy which achieves this value.
- Open: Classify tasks with no quantum advantage beyond NLC.



Device-independent witness of genuine multipartite entanglement

- Biseparable state of three parties

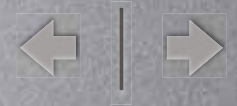
$$\rho_B = p_1 \rho_A \otimes \rho_{BC} + p_2 \rho_B \otimes \rho_{AC} + p_3 \rho_C \otimes \rho_{AB},$$

- Use the bound to detect genuine tripartite entanglement in qudit systems.
- Max. success prob. in a tripartite symmetric linear game using a biseparable state (Charlie has a deterministic strategy)

$$\omega_B^C(g_3^l) \leq \max_{\{c_z\}} \frac{1}{|G|} \left(1 + \sqrt{Q_1 Q_2} \sum_{k \in G \setminus \{e\}} \|\Phi_k^B(c_z)\| \right),$$

$$\Phi_k^B(c_z) = \sum_{x,y} \left(\sum_z p(x,y,z) \chi_k(f(x,y,z) - c_z) \right) |x\rangle\langle y|.$$

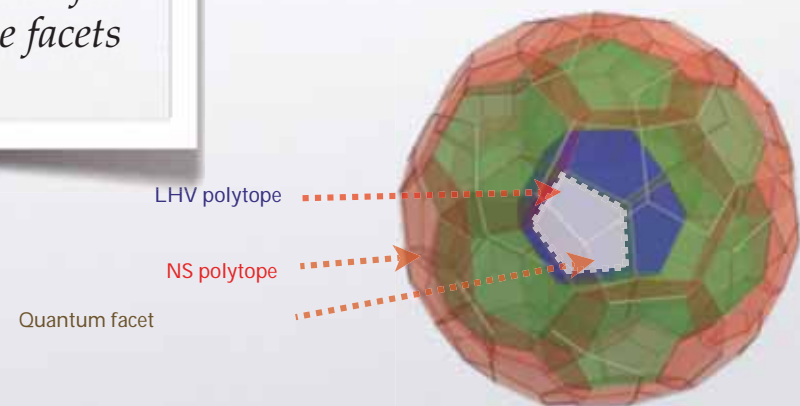
- Example: For the game $a \oplus_3 b \oplus_3 c = x \cdot y \cdot z$ s.t. $x \oplus_3 y \oplus_3 z = 0$, we get $\omega_B \leq 0.896$
- Qutrit GHZ state wins the game with prob. 1 $|GHZ_3\rangle = \frac{|000\rangle + |111\rangle + |222\rangle}{\sqrt{3}}$



Facets with no quantum advantage

- Significant to find a non-trivial boundary of the quantum set, information-theoretic principles such as the Local Orthogonality principle.
- We study whether xor games without quantum advantage are facets of the classical polytope, find a negative answer for a restricted class of functions.
- Proof is by decomposition to multiple face-defining inequalities so that they cannot define facets.

Theorem 6. *The non-local computation game inequalities for functions of the form in Eq. (7) for $d = 2$ do not define facets of the local polytope for any input size 2^n .*



M. L. Almeida, J.-D. Bancal, N. Brunner, A. Acin, N. Gisin and S. Pironio, Phys. Rev. Lett. 104, 230404 (2010)

R. Augusiak, T. Fritz, Ma. Kotowski, Mi. Kotowski, M. Pawłowski, M. Lewenstein and A. Acin, Phys. Rev. A 85, 042113 (2012).



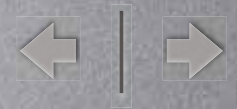
Open Questions

- Identify functions when the proposed quantum bound is tight?
- Bounds on classical value? Incidence combinatorics, operator space?
- Optimal witnesses of genuine qudit multipartite entanglement.
- Perfect Parallel repetition of linear games, additivity?
- DI Protocols using linear games? E.g.: Relativistic bit commitment.

Thank you!

* This work is supported by: ERC grant QOLAPS and the FNP TEAM project.



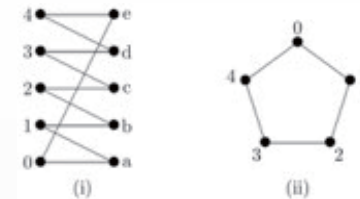


Shannon zero-error capacity

- Relation between the quantum value of a game and the Shannon zero-error capacity of a channel.
- **Shannon zero-error capacity:** For sequential uses of a memoryless channel, maximum rate at which information can be sent through the channel with zero probability of error.

- Capacity is computed through the confusability graph of the channel:

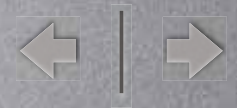
- Vertices correspond to letters of the encoding alphabet
- Edges connect two vertices if the corresponding inputs can be confused by the receiver



- Maximum number of 1-letter messages that can be sent is the independence number $\alpha(G)$. Denote by $\alpha(G^k)$ the maximum number of k-letter messages that can be sent (two k-letter words are confusable if every letter in the two words is confusable).

$$\Theta(G) = \sup_k \sqrt[k]{\alpha(G^k)}.$$

- Shannon capacity of a graph $\Theta(G)$ is notoriously difficult to compute. Breakthrough result by Lovasz for the pentagon graph using the SDP relaxation known as Lovasz theta $\vartheta(G)$ number. $\Theta(G) \leq \vartheta(G)$.



Shannon zero-error capacity and quantum value of games

- Relation between the quantum value of a game and the Shannon zero-error capacity of a channel.
- Let us consider the xor game matrix:

$$\tilde{\Phi} = \sum_{x,y \in [m]} (-1)^{f(x,y)} P(x,y) |x\rangle\langle y|.$$

- Associate to every game an "orthogonality graph":

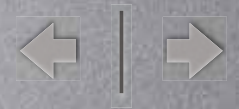
1	1
1	-1

CHSH

Definition 1. The graph G associated with the XOR game matrix Φ consists of $2m^2$ vertices $v \in V$. Each label v can be expressed as (x, y, a) where $x, y \in [m]$ and $a \in \{0, 1\}$. Two vertices $v, v' \in V$ form an edge of the graph if $(x = x'$ and $a \neq a')$ or $(y = y'$ and $(-1)^{a \oplus a'} \neq \Phi_{xy} \Phi_{x'y})$.

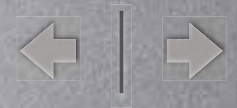
- The classical and quantum values of any game can be bounded in terms of the graph parameters

$$m^2 \omega_c = \alpha(G),$$
$$\alpha(G) \leq m^2 \omega_q \leq \theta(G)$$



Games with no quantum advantage

- Information-theoretic principles designed to capture the set of quantum non-local correlations: **Local Orthogonality**, Information Causality, Macroscopic Locality, **No advantage in Non-Local Computation**, Trivialization of Communication Complexity.
- Formulation of LO and NLC based on finding games with no quantum advantage.
- **No advantage in Non-Local Computation** of a boolean function from n bits to 1 bit $f(z_1, \dots, z_n)$.
 - Alice and Bob are given inputs x_i and y_i obeying $x_i \oplus y_i = z_i$ for $i = 1, \dots, n$, with each $p(x_i = 0) = p(y_i = 0) = 1/2$.
 - Goal: Output a and b such that $a \oplus b = f(x_1 \oplus y_1, \dots, x_n \oplus y_n)$.
 - Maximize probability of success for any $p(z_1, \dots, z_n) = p(x_1 \oplus y_1, \dots, x_n \oplus y_n)$.
- Quantum theory provides no advantage in the distributed non-local computation of boolean functions. Optimal is simply a linear approximation of the function.
- Can we characterize the games with no quantum advantage?



xor games with no advantage

- Phrase the SDP in terms of the bias of the game ($\varepsilon_q = 2 \omega_q - 1$)

$$\tilde{\Phi}_s = \begin{pmatrix} 0 & \frac{1}{2}\tilde{\Phi} \\ \frac{1}{2}\tilde{\Phi}^T & 0 \end{pmatrix}$$

$$\begin{aligned} \varepsilon_q = \max \quad & \text{Tr}[\tilde{\Phi}_s X] \\ \text{s.t.} \quad & \text{diag}(X) = |j\rangle, \quad X \succeq 0, \end{aligned}$$

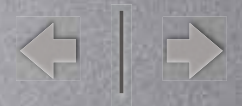
$$X = \begin{pmatrix} A & S \\ S^T & B \end{pmatrix} \quad \begin{aligned} S_{x,y} &= \langle u_x | v_y \rangle \\ A_{x,y} &= \langle u_x | u_y \rangle \\ B_{x,y} &= \langle v_x | v_y \rangle \end{aligned}$$

- We give a necessary and sufficient condition for the lack of quantum advantage in an xor game $\tilde{\Phi} = \sum_{x,y \in [m]} (-1)^{f(x,y)} P(x,y) |x\rangle\langle y|$.

Theorem 1. Consider a two-party XOR game with game matrix $\tilde{\Phi}$ with no all-zero row or column for which $S_c = |s^A\rangle\langle s^B|$ represents the optimal classical strategy. Let $\Sigma = \text{diag}(\{\langle i | \tilde{\Phi} | s^B \rangle \langle s^A | i \rangle\}_{i=1}^m)$ and $\Lambda = \text{diag}(\{\langle s^A | \tilde{\Phi} | i \rangle \langle i | s^B \rangle\}_{i=1}^m)$. There is no quantum advantage for $\tilde{\Phi}$ if and only if $\Sigma, \Lambda \succ 0$, or $\Sigma, \Lambda \prec 0$, and

$$\rho(\Lambda^{-1} \tilde{\Phi}^T \Sigma^{-1} \tilde{\Phi}) = 1, \quad (3)$$

where $\rho(\cdot)$ denotes the spectral radius.



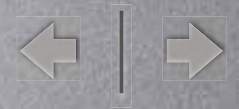
New class of channels for which Shannon capacity can be computed

- We derive a simpler sufficient condition to obtain games with no quantum advantage

Corollary 2. *If the vectors corresponding to the maximum singular value of $\tilde{\Phi}$ only contain elements that are ± 1 , then there is no quantum advantage for players of the game $\tilde{\Phi}$.*

- We use the Theorem to derive new class of communication channels (graphs) for which the Shannon zero-error capacity can be computed.

Theorem 3. *Every two-party XOR game with m uniformly chosen inputs for each party, and satisfying Cor. 2 has a game graph which is class-1 (has $\Theta(G) = \alpha(G)$).*

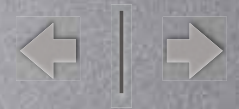


New class of channels for which Shannon capacity can be computed

- We study the properties of these channels in terms of the graphs:
 - The graphs are $(2m-1)$ regular, triangle-free, and have a perfect matching.
 - Their spectrum and corresponding degeneracies are found to be

$$\text{spec}(A(G)) = \left\{ \begin{array}{cc} 2m-1 & 1 \\ m-1 & 2m-2 \\ -1 & (m-1)^2 \\ 1-m \pm \lambda_z & 1 \\ 1 & m(m-2) \end{array} \right.$$

- We show that this family of graphs is distinct from previously known families: König-Egervary graphs, Kneser graphs and the simple perfect graphs.



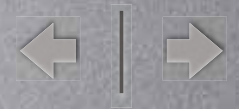
Motivation

- Hard to compute classical, quantum values of BIs. UGC: Unique game (classical value) is inapproximable, gap-preserving reductions give inapproximability for NP-complete problems. Efficient bounds?
- Operator space: Large ratio of quantum bias to classical bias for non-local games. Three party, d -outcome Bell inequalities with exponential separation?
- Device-independent applications: Crypto, randomness, entanglement witness.
- Beyond XOR games, implications for information-theoretic principles.

S. Khot, Proc. of 34th ACM STOC, 767 (2002).

S. Khot and N. Vishnoi, Proc. of 46th IEEE FOCS, 53 (2005).

J. Hastad, J. of ACM 48 (4), 798 (2001).



Quantum Value $\omega_q(G)$

- Efficient computation of $\omega_q(G)$ for XOR games: Semidefinite program from Tsirelson's theorem

Proposition 5. Let $G(V, \pi)$ be an XOR game and let $m = \min(|S|, |T|)$. Then

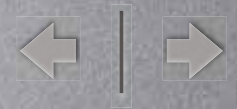
Semi-definite Program

$$\omega_q(G) - \tau(G) = \frac{1}{2} \max_{\{|u_s\rangle\}, \{|v_t\rangle\}} \sum_{s,t} \pi(s,t) (V(0|s,t) - V(1|s,t)) \langle u_s | v_t \rangle,$$

where the maximum is over all choices of unit vectors $\{|u_s\rangle : s \in S\} \cup \{|v_t\rangle : t \in T\}$ in \mathbb{R}^m .

$$\tau(G) = \frac{1}{2} \sum_{c \in \{0,1\}} \sum_{s,t} \pi(s,t) V(c|s,t).$$

- XOR games are the only known class of games whose quantum value can be computed so efficiently



Outline

- Motivation
- **Linear games:**
 - d-outcome generalization of XOR games.
 - Bound on the quantum value.
 - E.g. CHSH-d game.
 - Non-local computation.
 - Device-independent multipartite entanglement witness.
 - Pseudo-telepathy.
- Open Questions.

R. R, R. Augusiak and G. Murta, arXiv: 1502.02974 (2015).

G. Murta, R. R., N. Moller and M. T. Cunha, arXiv: 1510.09210 (2015).

P. Gnacinski, M. Rosicka, R. R., K. Horodecki, M. Horodecki, P. Horodecki, S. Severini, arXiv: 1511.05415 (2015).