Grothendieck Inequalities, XOR games, and Communication Complexity

Troy Lee
Rutgers University

Joint work with: Jop Briët, Harry Buhrman, and Thomas Vidick

Overview

- Introduce XOR games, Grothendieck's inequality, communication complexity, and their relation in the two-party case.

- Explain what of this relation survives in the three-party case.

- Final result will be that discrepancy method also lower bounds three-party quantum communication complexity with limited forms of entanglement.

XOR games

- Simple model of computing a function $f : \{-1,+1\}^n \times \{-1,+1\}^n \to \{-1,+1\}$.

- Verifier chooses inputs $x, y \in \{-1,+1\}^n$ with probability $\pi(x,y)$ and sends x to Alice, y to Bob.

- Without communicating, Alice outputs a bit $a_x \in \{-1,+1\}$ and Bob a bit b_y, aiming for $a_x b_y = f(x,y)$.

- Unless matrix $[f(x,y)]_{x,y}$ is rank one, will not always succeed. Measure performance
$$\beta(f \circ \pi) = \sum_{x,y} \pi(x,y) f(x,y) a_x b_y.$$

XOR games: basic observations

- As described above the model is deterministic. A convexity argument shows that model is unchanged if allow Alice and Bob to share randomness.

- The bias of a game (f, π) is exactly the $\infty \to 1$ norm of $f \circ \pi$:

$$\begin{aligned} \|A\|_{\infty \to 1} &= \max_{\substack{x \in \{-1,+1\}^m \\ y \in \{-1,+1\}^n}} x^t A y \\ &= \max_{\substack{y \\ \ell_\infty(y) \leq 1}} \ell_1(Ay). \end{aligned}$$

XOR games with entanglement

- Entanglement is an interesting resource allowed by quantum mechanics. Already can see its effects in the model of XOR games.

- Alice and Bob share a state $|\Psi\rangle \in H_A \otimes H_B$.

- Now instead of choosing bits, Alice and Bob choose Hermitian matrices A_x, B_y with eigenvalues in $\{-1, +1\}$.

- Expected value of the output on input x, y is given by

$$\langle \Psi | A_x \otimes B_y | \Psi \rangle$$

XOR games with entanglement

- The maximum bias in an XOR game (f, π) with entanglement $|\Psi\rangle$ is thus given by

$$\beta^*_{|\psi\rangle}(f \circ \pi) = \max_{\{A_x\},\{B_y\}} \sum_{x,y} f(x,y)\pi(x,y)\langle\Psi|A_x \otimes B_y|\Psi\rangle$$

- The bias is $\beta^*(f \circ \pi) = \max_{|\Psi\rangle} \ \beta_{|\psi\rangle}(f \circ \pi)$.

Tsirelson's Characterization

Tsirelson gave a very nice vector characterization of XOR games with entanglement.

$$\beta^*(f \circ \pi) = \max_{\substack{u_x, v_y \\ \|u_x\| = \|v_y\| = 1}} \sum_{x,y} \pi(x,y) f(x,y) \langle u_x, v_y \rangle.$$

That the RHS upper bounds the LHS is easy to see:

$$\langle \Psi | A_x \otimes B_y | \Psi \rangle = \langle u_x, v_y \rangle$$

where $u_x = A_x \otimes I|\Psi\rangle$, and $v_y = I \otimes B_y|\Psi\rangle$ are unit vectors.

Example: CHSH game

- What physicists call the CHSH game, a.k.a. the 2-by-2 Hadamard matrix. Goal is for $a_x b_y = x \wedge y$. Under the uniform distribution, game matrix looks as follows:

$$\frac{1}{4}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- Classically best thing to do is always output 1. Achieves bias $\frac{1}{2}$.

Example: CHSH game

- With entanglement can achieve bias $\frac{\sqrt{2}}{2}$. Recall that

$$\begin{aligned} \|A\|_{tr} &= \max_{\substack{U,V \\ \text{unitaries}}} \operatorname{Tr}(UAV^*) \\ &= \max_{\substack{\{u_x\},\{v_y\} \\ \text{orthonormal}}} \sum_{x,y} A(x,y)\langle v_y, u_x \rangle \\ &\leq \beta^*(A). \end{aligned}$$

- Trace norm of Hadamard matrix is $2\sqrt{2}$.

Grothendieck's Inequality

- Hadamard example shows a gap of $\sqrt{2}$ between bias of a game with entanglement and without. How large can this gap be?

- Grothendieck's Inequality shows this gap is at most constant

$$\sum_{x,y} A(x,y)\langle u_x, v_y\rangle \leq K_G \|A\|_{\infty\to 1}.$$

where $1.6770 \leq K_G \leq 1.7822$ [Lower: Davie, Reeds, Upper: Krivine].

Connection to Communication Complexity

- Upper bounds on the bias in an XOR game for f (under any distribution) imply lower bounds on the communication complexity of f.

- Proof: Say that f has deterministic communication complexity c. We design an XOR game for f where the players share a random string of length c which achieves bias 2^{-c}, for any distribution.

- Players interpret the random string as the transcript of their communication and look for inconsistencies.

Connection to Communication Complexity

- If Alice notices an inconsistency, she outputs a random bit. Same for Bob.

- If Alice does not notice an inconsistency, she outputs the answer given by the transcript. If Bob does not notice an inconsistency, he outputs 1.

- Let $P(x, y)$ denote the expectation of the output of this protocol on input (x, y).

$$\beta(f \circ \pi) \geq \sum_{x,y} \pi(x, y) f(x, y) P(x, y) = \frac{1}{2^c} \sum_{x,y} \pi(x, y) f(x, y)^2 = \frac{1}{2^c}$$

Bounded-error protocols

- The same idea also works if we start out with a communication protocol with bounded-error ϵ.

- Expected output of communication protocol will be between $[1-2\epsilon, 1]$ when $f(x,y)=1$ and $[-1,-1+2\epsilon]$ when $f(x,y)=-1$.

- Plugging this into previous argument gives a bias at least $\frac{1-2\epsilon}{2^c}$ under any distribution π, if f has bounded-error communication complexity c.

$$R_\epsilon(f) \geq \max_\pi \log\left(\frac{1-2\epsilon}{\beta(f\circ\pi)}\right).$$

Protocols with entanglement

- We can similarly relate the bias in an XOR game with entanglement to communication protocols with classical communication where the players share entanglement.
- In XOR game, players make same measurements on entangled state as in communication protocol, assuming communication from other player is given by shared random string.

$$R^*_\epsilon(f) \geq \max_\pi \log\left(\frac{1-2\epsilon}{\beta^*(f \circ \pi)}\right) \geq \max_\pi \log\left(\frac{1-2\epsilon}{\beta(f \circ \pi)}\right) - 1$$

Protocols with entanglement and quantum communication

- Lower bounds on protocols with entanglement already imply lower bounds on protocols with quantum communication. It is known that $Q^*_\epsilon(f) \geq \frac{R^*_\epsilon(f)}{2}$.

- Idea is teleportation. If Alice and Bob share a Bell state

$$|00\rangle + |11\rangle$$

  Alice can transfer Bob a state $\alpha|0\rangle + \beta|1\rangle$ by doing local operations and communicating two classical bits which direct local operations to be done by Bob.

Discrepancy method

- What we have described is precisely the discrepancy method in communication complexity

- Discrepancy is usually formulated in terms of the cut norm

$$\|A\|_C = \max_{\substack{x \in \{0,1\}^m \\ y \in \{0,1\}^n}} |x^t A y|.$$

- Not hard to show that these are closely related

$$\|A\|_C \leq \|A\|_{\infty \to 1} \leq 4\|A\|_C.$$

Generalized discrepancy method

- General argument to leverage more out of the discrepancy method [Klauck, Razborov].

- Instead of showing that f itself has small bias under π, show that g has small bias under π and that f and g are correlated under π.

- Working out the bias that you get under this argument gives

$$Q_\epsilon^*(f) \geq \frac{1}{2} \max_{g,\pi} \log \left(\frac{\langle f, g \circ \pi \rangle - 2\epsilon}{\beta(g \circ \pi)} \right)$$

  This bound is due to [Linial, Shraibman] who show it from the dual perspective.

How far do XOR games go?

- An XOR game has no communication. Surely these bounds can't be good!
- Does not show tight bound for randomized complexity of disjointness. Here information theoretic techniques and corruption bounds do better.
- It does subsume a large class of "geometric" techniques [Linial, Shraibman].
- Generalized discrepancy bound is polynomially related to approximate rank [L, Shraibman].

Summary

- Upper bounds on bias in XOR games give rise to communication complexity lower bounds.

- Grothendieck's inequality shows bias with entanglement can be at most constant factor larger than without.

- Implies that classical bias, or discrepancy, can be used to lower bound quantum communication complexity with entanglement.

Three-party case: NIH or NOF?

- Two popular models of multiparty complexity.

- We can transform a number-on-the-forehead problem into a number-in-the-hand problem.

- Alice gets input (y, z), Bob (x, z) and Charlie (x, y). A tuple gets zero probability if pairs are not consistent—that is, if union of sets is more than 3 strings.

- Bias under such a probability distribution corresponds to normal notion of NOF discrepancy.

Three-party case: what carries over

- Classical XOR bias still corresponds to discrepancy method.

- Relationship between XOR bias and communication complexity still holds. In particular, showing upper bounds on XOR bias with entanglement $|\Psi\rangle$ gives lower bounds on communication complexity with entanglement $|\Psi\rangle$.

- But showing upper bounds on bias with entanglement becomes much harder.

Three-party case: previous work

- Many complications arise in the three-party case . . .
- Pérez-García et al. give an example of a three-party XOR game where the ratio between bias with entanglement and without is unbounded.
- They also show that when the entanglement is of a special form known as GHZ state, there is at most a constant gap.
- What kinds of states allow for unbounded gaps?

Three-party case: why so different?

- In three-party case we no longer have a nice vector characterization analogous to Tsirelson.

- Also multilinear extensions of Grothendieck's inequality do not always hold.

- As inner product can be viewed as a linear functional on $H_A \otimes H_B$, multilinear extensions of Grothendieck look at linear functionals on $H_A \otimes H_B \otimes H_C$.

- Approach: look at the linear functional "induced" by sharing entanglement $|\Psi\rangle$ and see if corresponding Grothendieck inequality holds.

Our contributions

- We simplify the proof of the GHZ case.
- We enlarge the class of states for which we can show a constant gap to Schmidt states.
- We show how a generalization of Grothendieck's inequality due to Carne can be used to allow subsets of players to share GHZ states.
- This allows us to show that the generalized discrepancy method also lower bounds multiparty quantum communication complexity with shared entanglement of the above patterns. Extends a result of [L, Schechtman, Shraibman] who show this for quantum communication but cannot handle entanglement.

Generalized discrepancy method

- This gives a way to port old lower bounds to more powerful models.

- Especially nice in the number-on-the-forehead model where all lower bounds (in the general model) can be shown by the generalized discrepancy method.

- Examples: Lower bound of $n/2^{2k}$ for k-party generalized inner product function [Babai-Nisan-Szegedy]. Lower bound of $n^{1/(k+1)}/2^{2^k}$ for disjointness function [L-Shraibman, Chattopadhyay-Ada].

Multilinear generalization of Grothendieck's inequality

- The most naive extension of Grothendieck's inequality does hold. Consider a generalized inner product

$$\langle u, v, w \rangle = \sum_i u(i)v(i)w(i).$$

- As was first shown by Blei and later simplified and improved by Tonge, there is a constant C such that for any tensor M

$$\sum_{x,y,z} M(x,y,z)\langle u_x, v_y, w_z \rangle \leq C \max_{a_x, b_y, c_z \in \{-1,+1\}} \sum_{x,y,z} M(x,y,z) a_x b_y c_z.$$

XOR bias with GHZ state

- GHZ state $|\Psi\rangle \in H_A \otimes H_B \otimes H_C$ where $|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle|i\rangle|i\rangle$.
- Fix Hermitian matrices with eigenvalues in $\{-1, +1\}$ which maximize bias. Bias in a game with shared GHZ state is given by

$$\beta^*_{|\Psi\rangle}(f \circ \pi) = \frac{1}{d} \sum_{x_1, x_2, x_3} (f \circ \pi)(x_1, x_2, x_3) \langle \Psi | A(x_1) \otimes B(x_2) \otimes C(x_3) | \Psi \rangle.$$

- Let $M = f \circ \pi$. Writing out definition of GHZ state, the above equals

$$\frac{1}{d} \sum_{x_1, x_2, x_3} M(x_1, x_2, x_3) \sum_{i,j=1}^{d} \langle i | A(x_1) | j \rangle \langle i | B(x_2) | j \rangle \langle i | C(x_3) | j \rangle.$$

XOR bias with GHZ state

From the last slide we have

$$\frac{1}{d}\sum_{x_1,x_2,x_3} M(x_1,x_2,x_3)\sum_{i,j=1}^{d}\langle i|A(x_1)|j\rangle\langle i|B(x_2)|j\rangle\langle i|C(x_3)|j\rangle =$$

$$\frac{1}{d}\sum_{i=1}^{d}\sum_{x_1,x_2,x_3} M(x_1,x_2,x_3)\sum_{j=1}^{d}\langle i|A(x_1)|j\rangle\langle i|B(x_2)|j\rangle\langle i|C(x_3)|j\rangle$$

$$\leq \max_{u(x_1),v(x_2),w(x_3)}\sum_{x_1,x_2,x_3} M(x_1,x_2,x_3)\langle u(x_1),v(x_2),w(x_3)\rangle.$$

Extension to Schmidt states

- We can build on this argument to show a similar result when the entanglement is of the form

$$|\Psi\rangle = \sum_{i=1}^{d} \alpha_i |\sigma_i\rangle |\phi_i\rangle |\chi_i\rangle$$

  for orthonormal sets $\{\sigma_i\}, \{\phi_i\}, \{\chi_i\}$.

- In the bipartite case, every state can be so expressed (by SVD). Not so in tripartite case!

- Essentially proof works by reducing this case to convex combination of GHZ-like states.

Carne's theorem and combining states

- Roughly speaking, Carne's theorem gives a way to compose Grothendieck inequalities.

- Example: $H_A = H_A^0 \otimes H_A^1$ and $u_x = u_x^0 \otimes u_x^1$. Define

$$\phi(u_x, v_y, w_z) = \langle u_x^0, v_y^0 \rangle \langle u_x^1, w_z^0 \rangle \langle v_y^1, w_z^1 \rangle.$$

- We can use this theorem to show that even when k-many coalitions of up to r-players each share a GHZ state, there is at most a constant gap in the bias with entanglement and without. Constant goes like $O(2^{kr})$.

Open questions

- How powerful is entanglement for communication complexity in the multiparty case?
- Can we leverage separation of Pérez-García et al.in XOR game bias into a separation for a communication problem?
- Obtain a nice classification of what states lead to functionals for which we have Grothendieck inequalities.