

CS286.2 Lecture 16: 3-player entangled games and the role of monogamy

Scribe: Brenden Roberts

Recall Tsirelson's theorem, which we saw last time. The strong equivalent characterizations of bipartite quantum correlations it establishes provide an alternative characterization of the entangled value of XOR games, which as we saw takes the form $\omega^*(G) = \tau(G) + \frac{1}{2}\beta^*(G)$, where $\tau(G)$ is the win probability of a strategy of random answers by the players and $\beta^*(G)$ the bias acquired from entanglement. Using Tsirelson's theorem, we were able to express the bias in the form

$$\beta^*(G) = \sup_{\mathbf{x}_s, \mathbf{y}_t \in \mathbb{R}^{n+2}, \|\mathbf{x}_s\| = \|\mathbf{y}_t\| = 1} \mathbb{E}_{(s,t) \sim \pi} g_{s,t} \mathbf{x}_s \cdot \mathbf{y}_t,$$

which is a far more tractable formulation. In fact, it leads to an efficient computation algorithm. We show that we may rewrite

$$\beta^*(G) = \sup_{\substack{Z \in \mathbb{R}^{2n \times 2n} \\ Z \geq 0 \\ Z_{ii} = 1 \forall i}} \text{Tr}(\hat{G}Z), \quad \hat{G} = \frac{1}{2} \begin{bmatrix} 0 & (g_{s,t}) \\ (g_{s,t})^\top & 0 \end{bmatrix} \quad (1)$$

The direction \leq follows by choosing the specific

$$Z = \begin{bmatrix} \mathbf{x}_s \\ \mathbf{y}_t \end{bmatrix} \cdot \begin{bmatrix} \mathbf{x}_s & \mathbf{y}_t \end{bmatrix},$$

which clearly satisfies all of the conditions on Z . Conversely, any real positive semidefinite Z has a factorization $Z = W^\top W$. If $[\mathbf{x}_s]$ are the first n columns of W and $[\mathbf{y}_t]$ the last n columns, we recover our unit vectors.

Recall the concept of a linear program (LP), in which one seeks to optimize a linear objective function under a given set of linear constraints on the variables. Symbolically, an LP can be written as

$$\begin{aligned} \min \sum_{i=1}^n c_i x_i \text{ subject to } & x_i \in \mathbb{R} \\ & x_i \geq 0 \\ & A_j x = b_j, j = 1, \dots, n, \end{aligned}$$

where $c_i \in \mathbb{R}$, $A_j \in \mathbb{R}^{n \times n}$, $b_j \in \mathbb{R}^{n \times 1}$ for all i, j . An LP is solvable in poly time. A broader class of optimization problems that we know how to efficiently solve are semidefinite programs (SDP). In an SDP the objective function remains linear, but the constraints are allowed to include positive semidefiniteness constraints on matrix variables. An SDP takes the form

$$\begin{aligned} \min \text{Tr}(CZ) \text{ subject to } & Z \in \mathbb{R}^{n \times n} \\ & Z \geq 0 \\ & \text{Tr}(A_j Z) = b_j, j = 1, \dots, n. \end{aligned}$$

Note that in case C and all the A_j are diagonal matrices the optimal Z can also be taken to be diagonal, and the SDP becomes an LP. The expression of $\beta^*(G)$ given in (1) is an example of an SDP: optimization of a linear function, with PSD constraints. It can be solved to within additive error ϵ in time $\text{poly}(n, \log 1/\epsilon)$. This observations has a complexity-theoretic consequence on the computability of $\beta^*(G)$. In order to explain it, introduce the following complexity class:

Definition 1. For any $c < s$, $\oplus \text{MIP}_{\log}(c, s)$ is the set of all languages L such that there exists a poly time mapping from x to an XOR game G_x such that

- $x \in L \implies \omega(G_x) \geq c$,
- $x \notin L \implies \omega(G_x) \leq s$.

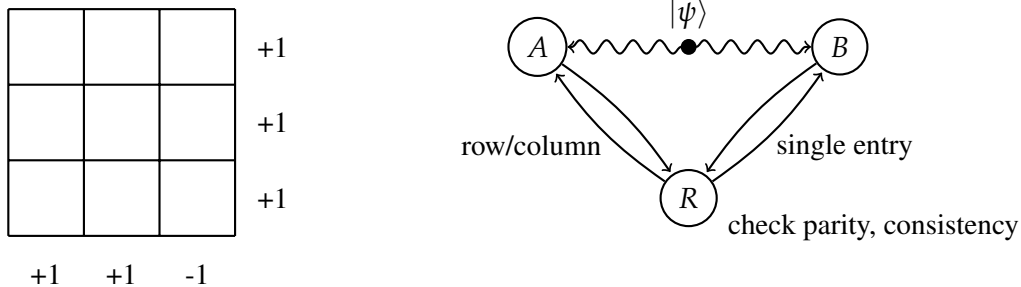
The class $\oplus \text{MIP}_{\log}^*(c, s)$ is defined equivalently, replacing $\omega(G_x)$ by $\omega^*(G_x)$.

Theorem 2 (Håstad). There exists constants $s < c$ (e.g., $c = \frac{12}{16}$, $s = \frac{11}{16} + \epsilon$) such that $\text{NP} = \oplus \text{MIP}_{\log}(c, s)$.

Theorem 3 (CHTW). For all $s < c$ such that $c - s > \frac{1}{2^n}$, $\oplus \text{MIP}_{\log}^*(c, s) \subseteq \text{P}$.

We saw last time, using the example of MAXCUT, that exact solutions for unentangled XOR games are NP-hard. Theorem 2 shows that even approximation remains NP-hard. However, for this class of games, entanglement has a drastic collapsing effect: in the entangled case XOR games prove to be too easy to be interesting. A better class of games is one for which computing the quantum value is NP-hard.

In order to obtain an interesting hardness result for ω^* we extend beyond the class of XOR games by considering 3-player games. As an example, consider the following 3-player variant of the magic square. Recall first the 2-player magic square game:



We saw that players sharing entanglement could win with probability 1: $\omega^*(\text{MS}_2) = 1$. The proof relies on:

1. A “quantum assignment” (4×4 Hermitian matrices that square to Id) X_1, \dots, X_9 to the entries, satisfying the appropriate parity constraints ($X_1 X_2 X_3 = +\mathbb{I}$, etc.)
2. The shared quantum state $|\psi\rangle$ is the maximally entangled state on $\mathbb{C}^4 \otimes \mathbb{C}^4$, and in particular it holds that for any A, B ,

$$\langle \psi | A \otimes B | \psi \rangle = \frac{1}{4} \text{Tr}(AB).$$

A 3-player XOR game MS_3 can be constructed in a natural way from MS_2 . The referee chooses a row or column at random, then asks each of the three players A, B, C for distinct entries and checks the parity of the answers. This game is completely symmetric in the players. It is clear that if one can obtain a tripartite $|\phi\rangle \in \mathbb{C}^4 \otimes \mathbb{C}^4 \otimes \mathbb{C}^4$ satisfying $\langle \phi | A \otimes B \otimes C | \phi \rangle = \frac{1}{4} \text{Tr}(ABC)$, then using the same ingredients as above it would follow that $\omega^*(\text{MS}_3) = 1$.

However, we claim that $\omega^*(\text{MS}_3) < 1$. The intuitive reason is the monogamy of entanglement: in the three-player game, the quantum correlations required to win have to be “diluted” between the three players. And there simply does not exist a tripartite analogue of the strong correlations that are provided by the bipartite maximally entangled state – as we now demonstrate.

Assume for the sake of contradiction that we have both: observables X_1, \dots, X_9 , which are the same for all of A, B, C ; and a quantum state $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$, for some d , which give $\omega^*(\text{MS}_3) = 1$. Then it must be the case that the following equalities all simultaneously hold:

$$\begin{aligned} \langle \psi | X_1 \otimes X_2 \otimes X_3 | \psi \rangle &= +1 \\ &\vdots \\ \langle \psi | X_3 \otimes X_6 \otimes X_9 | \psi \rangle &= -1. \end{aligned}$$

Since $\|X_i\| \leq 1$ for every $i \in \{1, \dots, 9\}$, this implies

$$\begin{aligned} X_1 \otimes X_2 \otimes X_3 | \psi \rangle &= | \psi \rangle \\ &\vdots \\ X_3 \otimes X_6 \otimes X_9 | \psi \rangle &= -| \psi \rangle \end{aligned}$$

We may multiply the operators X_i however we wish. Using the above, together with the fact that $X_i^2 = \mathbb{I}$ for $i = 1, \dots, 9$,

$$\begin{aligned} X_1 \otimes \mathbb{I} \otimes \mathbb{I} | \psi \rangle &= \mathbb{I} \otimes X_2 \otimes X_3 | \psi \rangle && \text{(row 1)} \\ &= X_5 \otimes \mathbb{I} \otimes X_3 X_8 | \psi \rangle && \text{(column 2)} \\ &= X_5 X_7 \otimes X_9 \otimes X_3 | \psi \rangle && \text{(row 3)} \\ \\ X_1 \otimes \mathbb{I} \otimes \mathbb{I} | \psi \rangle &= \mathbb{I} \otimes X_4 \otimes X_7 | \psi \rangle && \text{(column 1)} \\ &= X_5 \otimes \mathbb{I} \otimes X_6 X_7 | \psi \rangle && \text{(row 2)} \\ &= -X_5 X_3 \otimes X_9 \otimes X_7 | \psi \rangle && \text{(column 3)} \end{aligned}$$

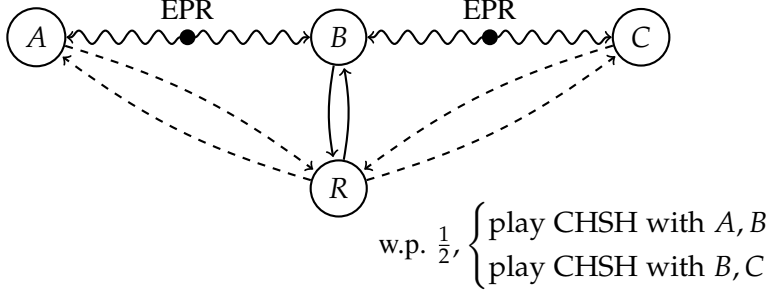
Multiplying by the inverse of $X_5 \otimes X_9$ we thus obtain

$$X_7 \otimes \mathbb{I} \otimes X_3 | \psi \rangle = -X_3 \otimes \mathbb{I} \otimes X_7 | \psi \rangle$$

By symmetry, this anticommutation-like property extends to any pair of registers, and we can write

$$X_7 \otimes X_3 \otimes X_3 | \psi \rangle = -X_3 \otimes X_7 \otimes X_3 | \psi \rangle = X_3 \otimes X_3 \otimes X_7 | \psi \rangle = -X_7 \otimes X_3 \otimes X_3 | \psi \rangle$$

Because observables are invertible, we find $|\psi\rangle = -|\psi\rangle$, which is a contradiction. By going through the same proof but keeping track of approximations a more quantitative result can be obtained, bounding $\omega^*(\text{MS}_3)$ away from 1 by some constant — though we do not know what the optimal value $\omega^*(\text{MS}_3)$ is.



For an even more striking example of the confounding effect of adding a player to an XOR game, we revisit the CHSH game. Consider the following 3-player variant of the CHSH game. The referee simply chooses at random whether to play CHSH_2 with A, B or B, C . He does not inform B whether he is playing with A or C , and the player not chosen is not asked any questions. The rest of the game proceeds as before; recall that for CHSH_2 , the winning condition is $a \oplus b = s \wedge t$, $s, t \in \{0, 1\}$.

Claim 4. $\omega^*(\text{CHSH}_3) = \omega(\text{CHSH}_3) = \frac{3}{4} < \frac{1}{2}\omega^*(\text{CHSH}_{2(A,B)}) + \frac{1}{2}\omega^*(\text{CHSH}_{2(B,C)})$. That is, the addition of the third player, even though a priori inoffensive, reduces the optimal quantum strategy to a classical one.

Proof. Suppose for the sake of contradiction that there exists an optimal quantum strategy for the players such that

$$\frac{1}{2} \Pr(A, B \text{ win}) + \frac{1}{2} \Pr(B, C \text{ win}) > \frac{3}{4}.$$

We will show this is impossible by making use of a further relaxation of the entangled win probability called the “no-signaling” win probability and denoted by $\omega^{NS}(G)$. The no-signaling value corresponds to the maximum success probability of players that are allowed to use resources that go even beyond those allowed by quantum mechanics, while still not communicating in-between themselves. More precisely, the players are allowed to “play”, i.e. provide answers, according to any family of probability distributions $\{p(a, b, c|x, y, z)\}_{x, y, z}$, where x, y, z are questions, satisfying

$$\sum_{b,c} p(a, b, c|x, y, z) = \sum_{b,c} p(a, b, c|x, y', z') \quad \forall x, y, y', z, z', \quad (2)$$

along with symmetric conditions for the other players. Note that if the distributions p are quantum, i.e. $p(a, b, c|x, y, z) = \langle \psi | A_x^a \otimes B_y^b \otimes C_z^c | \psi \rangle$ for some state $|\psi\rangle$ and POVM A_x, B_y and C_z , then since $\sum_b B_y^b = \sum_c C_z^c = \text{Id}$ we see that p satisfies the no-signaling conditions. In particular, we have that for any game G , $\omega(G) \leq \omega^*(G) \leq \omega^{NS}(G)$.¹ Because of the linear form of the no-signaling constraints (2), one can show that the computation of $\omega^{NS}(G)$ can be expressed as an LP. This makes bounding ω^{NS} in practice often much easier than ω^* . For the particular case of the game CHSH_3 one can explicitly write down what the LP is and construct a dual certificate showing that $\omega^{NS}(G) = 3/4$. This readily gives a bound on $\omega^*(G)$, and in this case we find that $\omega(\text{CHSH}_3) = \omega^*(\text{CHSH}_3) = \omega^{NS}(\text{CHSH}_3) = \frac{3}{4}$. \square

We note in conclusion that $\omega(\text{CHSH}_2) = \frac{3}{4}$, $\omega^*(\text{CHSH}_2) = \cos^2 \frac{\pi}{8}$, $\omega^{NS}(\text{CHSH}_2) = 1$.

¹Each of these inequalities can be strict, as is demonstrated by the 2-player CHSH game: as an exercise, show that $\omega^{NS}(\text{CHSH}_2) = 1$!