Lecture 2: Magic Square Game and XOR Games

In this lecture, we introduce the magic square game, the XOR games and their implications to quantum multi-prover proof systems.

2.1 Magic Square Game

The magic square game is an example whose quantum value is not only larger than the classical value, but also equals to 1, the maximally possible value as a winning probability. It presents a more striking difference between the quantum and the classical value of a game than that of the CHSH game for example.

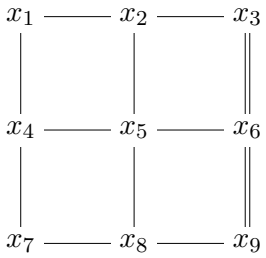

FIGURE 2.1: Magic Square

Consider the 3×3 square consisting of nine variables $x_1, x_2, \ldots, x_9$ as in Figure 2.1. The variables take values from $\{\pm 1\}$. Each row and column corresponds to a constraint as follows. For the last column on the doubled line, the constraint is that the three variables of the column have product -1. For the other rows and columns with single lines, the constraints are that the variables on them have product 1. More explicitly, the constraints are

$$\begin{aligned} x_1x_2x_3 &= 1, \quad x_4x_5x_6 = 1, \quad x_7x_8x_9 = \quad 1, \\ x_1x_4x_7 &= 1, \quad x_2x_5x_8 = 1, \quad x_3x_6x_9 = -1, \end{aligned} \tag{2.1}$$

in addition to the conditions $x_i^2 = 1$ specifying the domain of variables. As a constraint system, it has no satisfying assignment. Otherwise, taking the product of the first line in Eq. 2.1, the nine variables has product 1 and taking the product of the second line of equations, the nine variables has product -1, a contradiction.

Using the oracularization technique, the six constraints of the magic square define a game, called the magic square game, as in Figure 2.2.

The classical value of the magic square game is 17/18 as at least one of the 18 question pairs will be rejected by the referee, and it is easy to find a strategy that satisfies 17 of them simultaneously (see Eq. (1.2) of Lecture 1). Surprisingly, however, there is a perfect quantum strategy for the game. The provers use two shared EPR pairs

$$\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)^{\otimes 2}.$$

Magic Square Game

1. The referee samples one of the six rows and columns called $j \in \{1,2,\ldots,6\}$, and one variable x_i form that row or column.
2. The referee sends j to Alice and i to Bob.
3. Receives $a_1, a_2, a_3 \in \{\pm 1\}$ from Alice and $b \in \{\pm 1\}$ from Bob.
4. Accepts if and only if (a_1, a_2, a_3) has the designated product of the j-th constraint and b is consistent with (a_1, a_2, a_3).

FIGURE 2.2: The Constraint-Variable Magic Square Game

The measurement operators are defined by the operators X_i in Figure 2.3, where X, Y, and Z stand for the Pauli matrices. Alice measures the three observables in the row or column she receives. For example, if she receives 1, she will measure the observables X_1, X_2, X_3 in the first row sequentially, and answer with the measurement results. Bob will measure observable $\overline{X}_i$ when receiving variable index i. To see that Alice and Bob always give consistent result, it suffices to note that any two X_i operators in the same row or column are commuting, and the identity $A \otimes B|\Psi\rangle = AB^T \otimes I|\Psi\rangle$ for all A, B and maximally entangled state $|\Psi\rangle$. The fact that Alice always answer correctly for each constraint C_j follows from the observation that the X_i operators in each row and column have product I in the three rows and first two columns and product $-I$ in the last column.

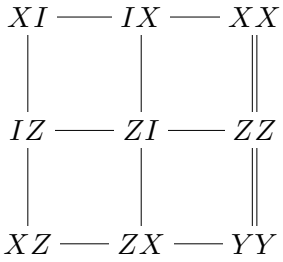

FIGURE 2.3: Operator solution for the magic square game

Here is an interesting observation: although Eq. 2.1 has no solution in ± 1, and therefore no perfect classical strategy, it does have an "operator solution" X_i, each of which is an observable of eigenvalue ± 1, explaining the existence of a quantum strategy of the game. For the constraint in the first row for example, the operators satisfies $X_1 X_2 X_3 = I$, an operator version of $x_1 x_2 x_3 = 1$. This is not a coincidence for the magic square game and actually holds in a very general setting called the binary constraint system games, which we will discuss later in the module.

An interesting consequence of the magic square game is that one can construct games whose quantum value is 1, while the classical value can be made arbitrarily small. This follows by considering the parallel repetition of the game and applying the parallel repetition theorem to the classical value. More concretely, for any $\epsilon > 0$, there is a game G such that $\omega^*(G) = 1$ and $\omega(G) \leq \epsilon$.

The existence of games whose quantum value is 1 while the classical value is bounded way from

1 has an important implication to the power of quantum multi-prover interactive proofs. As the quantum value of a game is always larger than or equal to the classical value, any interactive proof that is complete remains complete with the presence of quantum provers. However, a classically sound interactive proof may not be sound against quantum provers.

For example, the perfect quantum strategy for the magic square game indicates that the proof system based on the 3-SAT game introduced in the last lecture is no longer sound at all with quantum provers. To see this, let's reformulate the magic square game in the $0,1$ domain instead of the ± 1 domain. The product form constraints translate easily to the parity form constraints. The first constraint for example is now simply $x_1 \oplus x_2 \oplus x_3 = 0$. This parity constraint is equivalent to the conjunction of four 3-SAT clauses $\neg x_1 \vee x_2 \vee x_3$, $x_1 \vee \neg x_2 \vee x_3$, $x_1 \vee x_2 \vee \neg x_3$, and $\neg x_1 \vee \neg x_2 \vee \neg x_3$. Similarly, one can also translate all other constraints to four 3-SAT clauses each and the constraint system of the magic square is equivalent to an instance of 3-SAT of 24 clauses. The 3-SAT game for this instance also has a perfect quantum strategy and the provers only need to follow the strategy for the magic square game. Hence, the soundness of this particular proof system for the 3-SAT problem is now totally broken.

This raises the question of what are the consequences to the power of interactive proofs when quantum strategies are allowed. We will see in the next part that, for some special form of interactive proof systems, the "harm" of entanglement is probably permanent.

2.2 XOR Games

XOR game is a special class of games with binary answers and the verifier's acceptance is determined solely by the XOR of the two answer bits. So for an XOR game, the predicate $V(a,b|s,t)$ has the form $V(a\oplus b|s,t)$. The CHSH game, for example, is an XOR game, while the magic square game is not as it is not even a binary game (games with binary answers).

For any quantum strategy $(\rho, \{X_s^a\}, \{Y_t^b\})$ of an XOR game, define

$$X_s = X_s^0 - X_s^1, \quad Y_t = Y_t^0 - Y_t^1.$$

By the completeness of POVMs $\{X_s^a\}$, $\{Y_t^b\}$,

$$X_s^a = \frac{I + (-1)^a X_s}{2}, \quad Y_t^b = \frac{I + (-1)^b Y_t}{2}.$$

Therefore, we can express the game value of an XOR game as

$$\begin{aligned}
\omega^* &= \mathop{\mathbb{E}}_{(s,t)} \sum_{a,b} V(a\oplus b|s,t) \operatorname{tr}_\rho (X_s^a \otimes Y_t^b) \\
&= \mathop{\mathbb{E}}_{(s,t)} \sum_{a,b} V(a\oplus b|s,t) \operatorname{tr}_\rho \frac{(I + (-1)^a X_s) \otimes (I + (-1)^b Y_t)}{4} \\
&= \mathop{\mathbb{E}}_{(s,t)} \sum_{a,b} \frac{V(a\oplus b|s,t)}{4} + \mathop{\mathbb{E}}_{(s,t)} \sum_{a,b} \frac{V(a\oplus b|s,t)(-1)^{a\oplus b}}{4} \operatorname{tr}_\rho (X_s \otimes Y_t) \\
&= \mathop{\mathbb{E}}_{(s,t)} \sum_{a,b} \frac{V(a\oplus b|s,t)}{4} + \mathop{\mathbb{E}}_{(s,t)} \frac{V(0|s,t) - V(1|s,t)}{2} \operatorname{tr}_\rho (X_s \otimes Y_t).
\end{aligned}$$

Denoting the first term in the summation as τ, which is independent of the strategy and equals to the value of the uniformly random strategy, we have

$$\omega^* - \tau = \mathop{\mathbb{E}}_{(s,t)} \frac{V(0|s,t) - V(1|s,t)}{2} \operatorname{tr}_\rho(X_s \otimes Y_t). \tag{2.2}$$

It suffices to focus on this quantity when analyzing XOR games.

XOR quantum games are among the few cases that we have a complete understanding. And this is all because of the following theorem due to Tsirelson.

Theorem 2.1 (Tsirelson's theorem)**.** *For any $m \times n$ matrix $C = (C_{s,t})$, the following are equivalent:*

1. *There exist Hermitian operators $X_1, X_2, \ldots, X_m$ on Hilbert space $\mathcal{H}_A$, $Y_1, Y_2, \ldots, Y_n$ on Hilbert space $\mathcal{H}_B$, and density matrix ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ such that the spectrum of each of the operator lies in $[-1,1]$ and $C_{s,t} = \operatorname{tr}_\rho(X_s \otimes Y_t)$.*
2. *There exist Hermitian operators $X_1, X_2, \ldots, X_m$ on Hilbert space $\mathcal{H}_A$, $Y_1, Y_2, \ldots, Y_n$ on Hilbert space $\mathcal{H}_B$, and a pure state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ such that the dimensions of the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are at most $2^{\lceil (m+n)/2 \rceil}$, $X_s^2 = I$ and $Y_t^2 = I$ for all s and t and $C_{s,t} = \langle \Psi | X_s \otimes Y_t | \Psi \rangle$.*
3. *There exist real unit vectors $x_1, x_2, \ldots, x_m$ and $y_1, y_2, \ldots, y_n$ in a Euclidean space of dimension at most $m+n$, such that $C_{s,t} = x_s \cdot y_t$.*

Proof. It is obvious that the second item implies the first. We first show that the first item implies the third. Purifying the state ρ and performing local unitary operations if necessary, one can assume that $\mathcal{H}_A$ and $\mathcal{H}_B$ has the same dimension, and that the state is pure and of the form

$$|\Psi\rangle = \sum_i \sqrt{\lambda_i} |i,i\rangle.$$

With this assumption, $\operatorname{tr}_\rho(X_s \otimes Y_t)$ equals to $\operatorname{tr}(X_s \Lambda Y_t^T \Lambda)$, for $\Lambda = \sum_i \sqrt{\lambda_i} |i\rangle\langle i|$. The choices $x'_s = \sqrt{\Lambda} X_s \sqrt{\Lambda}$ and $y'_t = \sqrt{\Lambda} Y_t^T \sqrt{\Lambda}$ give $C_{s,t} = \langle x'_s, y'_t \rangle$ and $\|x'_s\| \le 1$, $\|y'_t\| \le 1$. These are Hermitian matrices and can be mapped to real vectors preserving the inner product. By extending the space if necessary, we can choose two vectors x and y that are orthogonal to each other and orthogonal to all the x'_s and y'_t vectors. Finally, choose appropriate coefficients α_s and β_t so that $x_s = x'_s + \alpha_s x$ and $y_t = y'_t + \beta_t y$ are unit vectors. The dimension upper bound of $m+n$ follows by taking the span of the vectors x_s and y_t.

To prove item three implies item two in the theorem, we need the following construction of pairwise anti-commuting reflections. For any integer $k \ge 1$, define $2k$ operators T_i for $i = 1, 2, \ldots, 2k$ as follows

$$\begin{aligned} T_{2j-1} &= I^{\otimes(j-1)} \otimes \sigma_x \otimes \sigma_y^{\otimes(k-j)}, \\ T_{2j} &= I^{\otimes(j-1)} \otimes \sigma_z \otimes \sigma_y^{\otimes(k-j)}, \end{aligned}$$

where $\sigma_x, \sigma_y, \sigma_z$ are Pauli matrices. It is easy to verify that $T_i^2 = I$ and T_i, T_j anti-commute for all $i \ne j$. We can proceed the proof now as follows. Choose $k = \lceil (m+n)/2 \rceil$ and construct operators T_i accordingly. For each unit vector x_s, define operator $X_s = \sum_i x_{s,i} T_i$ and operators $Y_t = \sum_i y_{t,i} \overline{T}_i$. It is easy to verify that indeed $X_s^2 = I$ and $Y_t^2 = I$. Choosing the state $|\Psi\rangle$ to be the maximally entangled state of local dimension 2^k, we have

$$\langle \Psi | X_s \otimes Y_t | \Psi \rangle = \frac{1}{2^k} \operatorname{tr}(X_s Y_t^T) = x_s \cdot y_t.$$

□

2.2.1 Tsirelson's Bound

We start illustrating the power of Tsirelson's theorem by showing that the $\sqrt{2}$ violation in the CHSH inequality is optimal.

In the CHSH game, the value τ of random strategy is $1/2$. The coefficients on the right hand side of Eq. (2.2) are $V(0|s,t) - V(1|s,t) = (-1)^{st}$. Hence the right hand side is equal to

$$\omega^* - \tau = \frac{1}{8}\big[\mathrm{tr}_\rho(X_0 \otimes Y_0) + \mathrm{tr}_\rho(X_0 \otimes Y_1) + \mathrm{tr}_\rho(X_1 \otimes Y_0) - \mathrm{tr}_\rho(X_1 \otimes Y_1)\big].$$

As the operators satisfies the condition in the first item of Theorem 2.1, the item three of the theorem states that there exist real unit vectors x_0, x_1, y_0 and y_1 such that

$$\begin{aligned}
\omega^* - \tau &= \frac{1}{8}(x_0 \cdot y_0 + x_0 \cdot y_1 + x_1 \cdot y_0 - x_1 \cdot y_1) \\
&= \frac{1}{8}(x_0 \cdot (y_0 + y_1) + x_1 \cdot (y_0 - y_1)) \\
&\leq \frac{1}{8}\big(\|y_0 + y_1\| + \|y_0 - y_1\|\big) \\
&\leq \frac{1}{4}\sqrt{\frac{\|y_0 + y_1\|^2 + \|y_0 - y_1\|^2}{2}} \\
&= \frac{1}{4}\sqrt{\|y_0\|^2 + \|y_1\|^2} = \frac{\sqrt{2}}{4}.
\end{aligned}$$

This completes the proof that the CHSH game has quantum value at most $1/2 + \sqrt{2}/4$. This or the $2\sqrt{2}$ bound of E is called Tsirelson's bound [1]. Together with the particular construction witnessing $\omega^* \geq 1/2 + \sqrt{2}/4$, we know that the quantum value of the CHSH game is exactly $1/2 + \sqrt{2}/4 \approx .85$.

2.2.2 SDP Characterization

From Eq. (2.2), the optimization for the quantum game value of an XOR game is an optimization over the convex set of matrices C whose s,t-th entry is $\mathrm{tr}_\rho(X_s \otimes Y_t)$. The Tsirelson's theorem gives an alternative, easy-to-use, characterization of this convex set.

Let $\alpha_{s,t} = \mu(s,t)(V(0|s,t) - V(1|s,t))/2$. Optimizing the right hand side of Eq. (2.2), the value of $\omega^* - \tau$ is equal to the value of the following mathematical programming problem.

$$\begin{aligned}
\text{maximize:} \quad & \sum_{s,t} \alpha_{s,t} C_{s,t} \\
\text{subject to:} \quad & C_{s,t} = \mathrm{tr}_\rho(X_s \otimes Y_t), \\
& \rho \text{ is a density matrix on the A,B system,} \\
& -I \leq X_s, Y_t \leq I.
\end{aligned}$$

[1] Not to be confused with Bell-CHSH's bound of 2 on E.

By Tsirelson's theorem, the optimization problem is equivalent to

$$\begin{aligned} \text{maximize:} \quad & \sum_{s,t} \alpha_{s,t} C_{s,t} \\ \text{subject to:} \quad & C_{s,t} = x_s \cdot y_t, \\ & x_s, y_t \text{ are unit real vectors.} \end{aligned}$$

This is obviously a semidefinite programming problem. To see this, let matrix G be the Gram matrix of the $m+n$ vectors x_s and y_t. Note that G is positive semidefinite and has all 1's on the diagonal. Conversely, for any such matrix G, the Cholesky decomposition of it gives the real unit vectors x_s, y_t. Therefore, the optimization problem is further transformed to the following semidefinite programming form

$$\begin{aligned} \text{maximize:} \quad & \sum_{s,t} \alpha_{s,t} G_{s,t+m} \\ \text{subject to:} \quad & G \geq 0, \\ & G_{i,i} = 1 \text{ for } i = 1, 2, \ldots, m+n, \\ & G \text{ is a symmetric matrix of size } m+n. \end{aligned}$$

Efficient algorithms solving semidefinite programming problems exist and imply that one can approximate the quantum game value within additive error ϵ in time polynomial in $|S|+|T|$, and $\log(1/\epsilon)$. The approximation of the classical value of an XOR game is believed, however, to be hard (**MAXSNP**-hard). Roughly, it means that, unless **P**=**NP**, computing the quantum value of an XOR game is easier than computing the classical value.

The semidefinite programming for the quantum game value also has implications on the power of $\oplus$**MIP***(2,1), the complexity class defined by certain scaled up version of XOR games as in Definition 2.2.

Definition 2.2. *For any $0 \leq s < c \leq 1$, $\oplus\mathbf{MIP}^*_{s,c}(2,1)$ is the class of languages L that have the following two-prover one-round quantum interactive proof systems where the two provers with shared entanglement each reply a single bit and the verifier decides either to accept or reject based only on the parity of the two replied bits such that*

- *If $x \in L$ there exists a quantum strategy for the provers so that the verifier accepts with probability at least c (completeness condition).*
- *If $x \notin L$, the verifier accepts with probability at most s, regardless of provers' strategy (soundness condition).*

The above semidefinite programming characterization of the quantum game value gives an upper bound **EXP** for the class $\oplus\mathbf{MIP}^*_{s,c}(2,1)$. The classical analog of the class $\oplus\mathbf{MIP}_{s,c}(2,1)$, however, equals to **NEXP** for certain choices of completeness and soundness probabilities s, c[2].

It is important to note that three-player XOR games have a totally different story, and it is now known **NP**-hard to determine the game value even to constant precision[3].

[2] See details in Richard Cleve et al. "Consequences and Limits of Nonlocal Strategies". In: *Proceedings of the 19th Annual IEEE Conference on Computational Complexity*. CCC '04. Washington, DC, USA: IEEE Computer Society, 2004, pp. 236–249.

[3] Thomas Vidick. "Three-Player Entangled XOR Games Are NP-Hard to Approximate". In: *2013 IEEE 54th Annual Symposium on Foundations of Computer Science* (2013), pp. 766–775.

2.2.3 Entanglement Bound

Tsirelson's theorem also gives bounds on the amount of entanglement needed for the players to play optimally or near optimally in an XOR game.

Theorem 2.3. *For any XOR game, there exists an optimal strategy for Alice and Bob in which they share a maximally entangled state of* $\lceil (|S|+|T|)/2 \rceil$ *qubits on each side.*

It is a direct corollary of Theorem 2.1 and the bound can be improved to $\lceil \min(|S|,|T|)/2 \rceil$ with little extra work (projecting one set of vectors $\{x_s\}$ and $\{y_t\}$ to the other). This is still a huge number, which is exponential in the input size of the game.

If a sub-optimal strategy is acceptable, one can show that polynomial amount of entanglement suffices making use of the so-called Johnson-Lindenstrauss lemma.

Lemma 2.4 (Johnson-Lindenstrauss)**.** *For* $\epsilon \in (0,1)$*, any set* S *of* m *points in* $\mathbb{R}^n$*, and a number* $k \geq 8\ln(m)/\epsilon^2$*, there is linear map* $f : \mathbb{R}^n \to \mathbb{R}^k$ *such that*

$$(1-\epsilon)\,\|u-v\|^2 \leq \left\|f(u)-f(v)\right\|^2 \leq (1+\epsilon)\,\|u-v\|^2,$$

for any $u, v \in S$.

The important feature of the above lemma is that the image space of f has dimension that is independent of n and only depend on the number of points and the error parameter ϵ. One obtains the following theorem by applying the lemma to vectors x_s and y_t corresponding to an optimal strategy guaranteed by Tsirelson's theorem and the zero vector 0.

Theorem 2.5. *For any XOR game whose quantum value is* ω^**, for any integer* $k \geq \Omega(\ln(|S|+|T|+1)/\epsilon^2)$*, there is a strategy for Alice and Bob using maximally entangled state on* $\lceil k/2 \rceil$ *qubits that achieves a value greater than* $\omega^* - \epsilon$.

The use of the Tsirelson's theorem in the above proof of bound on the amount of entanglement is crucial. It is an open problem to prove a similar upper bound on the amount entanglement needed for the players to play near optimally for general games as there are no such simple characterizations of quantum strategies in general.