CS286.2 Lecture 8: A variant of QPCP for multiplayer entangled games

Scribe: Zeyu Guo

In the first lecture, we saw three equivalent variants of the classical PCP theorems in terms of CSP, proof checking, and multiplayer games respectively. In the last lecture we formulated quantum analogues of the CSP and proof checking variants, and proved their equivalence. Today we introduce a quantum analogue of the games variant. Unlike the classical case, it is not known if this formulation is equivalent to the CSP or proof-checking variants of the quantum PCP conjecture.

First we briefly recall the classical PCP theorem in terms of multiplayer games: In a k-player game G, the verifier picks a random number $i \in \{1, \ldots Q\}$ according to some distribution π and uses it to determine a tuple of k questions $\varphi_i = (\varphi_{i,1}, \ldots, \varphi_{i,k})$, each containing $p \leq \log Q$ bits. For $1 \leq j \leq k$, it asks the j-th player question $\varphi_{i,j}$ and obtains an a-bit answer. The players are not allowed to communicate with each other when preparing the answers. The verifier then decides to accept or not. Let $w(G)$ be the maximum probability that the players could convince the verifier to accept, ranging over all possible strategies.

Theorem 1 (PCP theorem, games variant)**.** *Let the notations be as above, and let L be any language in* NP. *There exists a polynomial time computable mapping, sending $x \in \{0,1\}^n$ to a k-player game G_x with parameters $k = O(1)$, $Q = \mathrm{poly}(n)$, $p = O(\log n)$, $a = O(1)$, such that*

- $x \in L \implies w(G_x) \geq 2/3$,
- $x \notin L \implies w(G_x) \leq 1/3$.

Our goal is to formulate a quantum analogue of Theorem 1. To do so we first seek an appropriate notion of quantum game, which generalizes classical multiplayer games.

Definition 2 (Quantum multiplayer games)**.** *A quantum k-player game G with parameters k, Q, p, a is given by*

- *a distribution π on $\{1, \ldots, Q\}$,*
- *states $|\varphi_i\rangle$ on $k \times p$ qubits for each $i \in \{1, \ldots, Q\}$,*
- *measurements $\{\Pi_i, \mathbb{I} - \Pi_i\}$ on $k \times a$ qubits for each $i \in \{1, \ldots, Q\}$.*

The game is played as follows. The verifier randomly selects $i \in \{1, \ldots, Q\}$ according to π and sends $|\varphi_i\rangle$ to the k players (sending each chunk of p qubits to one of the players). The players each send a qubits back. The verifier measures the answer qubits using $\{\Pi_i, \mathbb{I} - \Pi_i\}$ and accepts iff the output is Π_i.

The value $w(G)$ of the game is defined to be the maximum probability that the verifier accepts, ranging over all possible strategies for the players. Here the strategy of the j-th player P_j is specified by a unitary *operator U_j acting on the corresponding p qubits of $|\varphi_i\rangle$, together with ancilla qubits that P_j could possibly use. Formally,*

$$w(G) = \sup_{U_1,\ldots,U_k} \sum_{i=1}^{q} \pi(i) \left\| \left(\sqrt{\Pi_i} \otimes \mathbb{I} \right) U_1 \otimes \cdots \otimes U_k |\varphi_i\rangle |0\rangle \right\|^2 .$$

Here each measurement Π_j is applied to a qubits out of the p qubits seen by P_j and they correspond to the answer of P_j. And $|0\rangle = |0\rangle_{P'_1} \cdots |0\rangle_{P'_k}$ are the ancilla qubits used by the k players.

Remark. *Quantum games contain classical games as a special case: to simulate a classical game, the verifier just represent the classical questions as quantum states via the embedding $\{0,1\}^{k\times p} \to (\mathbb{C}^2)^{\otimes k\times p}$. Even though the players may return answers that are in an arbitrary quantum state, if the verifier measures them in the standard basis then this does not increase their odds of winning.*

Remark. *As a consequence, it is* NP*-hard to distinguish the two cases $w(G) = 1$ and $w(G) \leq 1/3$ for quantum games with $k = O(1)$, $Q = \mathrm{poly}(n)$, $p = O(\log n)$, $a = O(1)$, since this holds for classical games by the classical* PCP *theorem (Theorem 1).*

Given this new notion of quantum game we are tempted to formulate a games variant of the quantum PCP conjecture, as follows.

Conjecture 3 (Quantum PCP conjecture, games variant, first attempt)**.** *Let L be any language in* QMA. *There exists a polynomial time computable mapping, sending $x \in \{0,1\}^n$ to a quantum k-player game G_x with parameters $k = O(1)$, $Q = \mathrm{poly}(n)$, $p = O(\log n)$, $a = O(1)$, such that*

- $x \in L \implies w(G_x) \geq 2/3$,
- $x \notin L \implies w(G_x) \leq 1/3$.

This is not a reasonable conjecture, however: we claim that the problem of distinguishing $w(G_x) \geq 2/3$ and $w(G_x) \leq 1/3$ lies in NP! Note that this claim implies that Conjecture 3 is false, assuming QMA $\neq$ NP.

Claim 4. *There exists a non-deterministic polynomial-time algorithm that distinguishes the cases $w(G_x) \geq 2/3$ and $w(G_x) \leq 1/3$ for a given quantum game G_x with parameters k, Q, p, a as in Conjecture 3.*

Proof. The non-deterministic algorithm just guesses the unitary operators U_j, simulates U_j and Π_i on $|\varphi_i\rangle|0\rangle$ for each $1 \leq i \leq q$ and computes the probability of acceptance.

To show that this verification algorithm can be run in polynomial time we need to argue that the dimension of the vector space that U_j acts on can be assumed to be polynomially bounded. This is not obvious due to the presence of ancillas. However we can show it with the following lemma:

Lemma 5 (Schmidt decomposition)**.** *Given a state $|\varphi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^{d'}$, there exists orthogonormal bases $\{|u_i\rangle\}$ for $\mathbb{C}^d$ and $\{|v_i\rangle\}$ for $\mathbb{C}^{d'}$ such that*

$$|\varphi\rangle = \sum_{i=1}^{\min(d,d')} \lambda_i |u_i\rangle \otimes |v_i\rangle$$

for some $\lambda_i \in \mathbb{R}_{\geq 0}$, $\sum_i \lambda_i^2 = 1$.

Before proving the lemma we show how to apply it to conclude the claim. Suppose one of the players, call it player A, applies the unitary operator U that sends $|i\rangle_A|0\rangle_{A'}$ to $|\psi_i\rangle_{AA'}$ where $\{|i\rangle_A\}$ is an arbitrary basis of the player's message space $(\mathbb{C}^2)^{\otimes p}$ and $|0\rangle_{A'} \in (\mathbb{C}^2)^{\otimes m}$ is the ancilla. Our goal is to show that without loss of generality m can be taken to be polynomial in n. By Lemma 5, we can write

$$|\psi_i\rangle_{AA'} = \sum_{k=1}^{\min(2^p,2^m)} \lambda_k^i |u_k^i\rangle \otimes |v_k^i\rangle, \qquad |u_k^i\rangle \in (\mathbb{C}^2)^{\otimes p}, |v_k^i\rangle \in (\mathbb{C}^2)^{\otimes m}.$$

Let V be the vector space spanned by $|v_k^i\rangle$. Its dimension is at most the number of vectors, which is bounded by $2^p \times \min(2^p, 2^m) = \mathrm{poly}(n)$. Whether the provers' strategy is accepted or rejected only depends on how U_j acts on $(\mathbb{C}^2)^{\otimes p} \otimes V \subseteq (\mathbb{C}^2)^{\otimes p} \otimes (\mathbb{C}^2)^{\otimes m}$, whose dimension is $2^p \cdot \mathrm{poly}(n) = \mathrm{poly}(n)$. So we may always assume that the initial ancilla space has polynomial dimension, and the NP procedure only need to check for players whose strategy is implemented by a unitary in polynomial dimension. □

Proof of Lemma 5. Pick arbitrary bases $\{|i\rangle\}$ of $\mathbb{C}^d$ and $\{|j\rangle\}$ of $\mathbb{C}^{d'}$ and expand $|\varphi\rangle = \sum_{i,j} \alpha_{i,j}|i\rangle \otimes |j\rangle$ for some $\alpha_{i,j} \in \mathbb{C}$, $\sum_{i,j} |\alpha_{i,j}|^2 = 1$. Let $(\alpha_{ij}) = UDV$ be the SVD decomposition of the matrix (α_{ij}) where $D = (d_{ij})$ is a $\min(d, d') \times \min(d, d')$ diagonal matrix with real non-negative eigenvalues. And suppose $U = (u_{ij})$, $V = (v_{ij})$. Then

$$|\varphi\rangle = \sum_{i,j}\sum_{k,i} u_{ik} d_{kk} v_{kj} |i\rangle \otimes |j\rangle = \sum_{k=1}^{\min(d,d')} d_{kk} \left(\sum_i u_{ik}|i\rangle\right)\left(\sum_j v_{kj}|j\rangle\right).$$

Finally we set $\lambda_k = d_{kk}$, $|u_k\rangle = \sum_i u_{ik}|i\rangle$, and $|v_k\rangle = \sum_i v_{kj}|j\rangle$ for $1 \leq k \leq \min(d, d')$. □

The proof of Claim 4 (implying that Conjecture 3 is uninteresting) essentially works by showing that the number of ancilla qubits needed is bounded by $O(\log n)$. But what if we are allowed to initialize the ancilla as an arbitrary (in particular, possibly entangled) state, instead of $|0\rangle$? We will see that this modified notion of quantum games helps us formulate a more plausible quantum analogue of the PCP conjecture.

Definition 6 (entangled quantum games)**.** *An entangled quantum game G is modified from an ordinary quantum game (c.f. Definition 2) by allowing the players to use an arbitrary state $|\psi\rangle$ as the initial ancilla. The "entangled" value $w^\star(G)$ is defined to be the maximum probability that the verifier accepts, ranging over all possible strategies of the players, where now a strategy includes the choice of the initial ancilla in addition to the unitary operators. Formally,*

$$w^\star(G) = \sup_{|\psi\rangle, U_1,\ldots,U_k} \sum_{i=1}^{q} \pi(i) \left\| \left(\sqrt{\Pi_i} \otimes \mathbb{I}\right) U_1 \otimes \cdots \otimes U_k |\varphi_i\rangle|\psi\rangle \right\|^2.$$

Conjecture 7 (Quantum PCP conjecture, games variant, second attempt)**.** *Let L be any language in* QMA. *There exists a polynomial time computable mapping, sending $x \in \{0,1\}^n$ to an entangled quantum k-player game G_x with parameters $k = O(1)$, $Q = \mathrm{poly}(n)$, $p = O(\log n)$, $a = O(1)$, such that*

- $x \in L \implies w^\star(G_x) \geq 2/3$,
- $x \notin L \implies w^\star(G_x) \leq 1/3$.

Interestingly, unlike the case of $w(G)$, the classical PCP theorem has no implication about the hardness of computing $w^\star(G)$. The only obvious relation between the two quantities is that $w^\star(G) \geq w(G)$. But this does not rule out the possibility that computing $w^\star(G)$ could be easy, for example, if $w^\star(G) = 1$ for all games G whose verifiers do not trivially always reject. But computing $w^\star(G)$ could also be harder: as we showed, to achieve $w(G)$ the (unentangled) players only need $O(\log n)$ ancilla qubits, and this is what places the problem in NP. But in the case where entanglement is allowed, we do not know any upper bound on the number of ancilla qubits that are needed in order to achieve a success probability that is close to $w^\star(G)$. In fact, we do have simple examples of games for which the optimum strategy requires the use of infinite-dimensional entanglement, as in the following example:

Example 8. *Consider the following two-player quantum game. As his question the verifier picks one of the two states*

$$|\varphi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_B + \frac{1}{2}\big(|1\rangle_A|1\rangle_B + |2\rangle_A|2\rangle_B\big), \quad |\varphi_2\rangle = \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_B - \frac{1}{2}\big(|1\rangle_A|1\rangle_B + |2\rangle_A|2\rangle_B\big)$$

with equal probability. Players A and B are given their respective half of the question, a 3-dimensional state each. They are required to return answers $a, a' \in \{0, 1\}$ respectively, such that the XOR of a and a' equals zero if the question is $|\varphi_1\rangle$, and otherwise equals one.

Without any entanglement this game is hard to win; one can show that $\omega(G) = 1/2 + 1/(2\sqrt{2})$. Intuitively, this is because locally the two states $|\varphi_1\rangle$ and $|\varphi_2\rangle$ look identical: they are uniformly mixed over $\mathbb{C}^3$. However one can show that $\omega^*(G) = 1$, but if the players are restricted to using an ancilla space of dimension d each then $\omega^*(G) \leq 1 - \Omega(\log^{-2} d)$. In other words, achieving a success probability of $1 - \varepsilon$ requires the players to use about $1/\sqrt{\varepsilon}$ qubits of entanglement each, no less!

In spite of the comments above some hardness results are known for entangled games. These results place the computational study of entangled games precisely at the same level as what is known for the local Hamiltonian problem. Indeed, the following two results are known:

- Distinguishing $w^\star(G) = 1$ and $w^\star(G) \leq 1/2$, i.e. approximating $w^\star(G)$ within constant accuracy, is NP-hard.
- Distinguishing $w^\star(G) = 1$ and $w^\star(G) \leq 1 - 1/\text{poly}(n)$, i.e. approximating $w^\star(G)$ within inverse polynomial accuracy, is QMA-hard.

The first result is an analogue of the classical PCP theorem for $\omega^\star$. As we argued above, the result does *not* follow from the classical theorem, but requires a nontrivial adaptation of the proof. The second result is an analogue of the quantum Cool-Levin theorem (Kitaev's theorem on QMA-completeness of LH), but the proof is completely different and would take us too far.

The Magic Square game. We end this lecture with the discussion of an example of a quantum game (in fact, a classical game) for which $\omega(G) < 1$ but $\omega^\star(G) = 1$. This example is particularly relevant for us because it will show that the clause/variable game we used to prove that (PCP, CSP variant) $\implies$ (PCP, game variant) no longer works in the quantum case.

Consider a 3×3 grid containing nine variables x_{ij}.

x_{11}	x_{12}	x_{13}
x_{21}	x_{22}	x_{23}
x_{31}	x_{32}	x_{33}

The variables take value from $\{\pm 1\}$. We design a 2-player game MS to check the satisfiability of the following six parity constraints, one for each row and one for each column:

$$x_{11}x_{12}x_{13} = 1, x_{21}x_{22}x_{23} = 1, x_{31}x_{32}x_{33} = 1,$$
$$x_{11}x_{21}x_{31} = 1, x_{12}x_{22}x_{32} = 1, x_{13}x_{23}x_{33} = -1.$$

The verifier is totally classical and proceeds in the same way as in the clause/variable game: it picks a random row or column, and asks the first player ("Alice") for the values of the three variables on it. It also picks a random entry on that row or column, and asks the second player ("Bob") for its value. The verifier then check the corresponding constraint and accepts iff it is satisfied and the answers of the two players are consistent.

Note that the six constraints can never be all satisfied: taking the product of the row constraints shows that the product of all variables equals $+1$, but doing the same for the column constraints shows that the product equals -1. And we also know that this kind of clause/variable game is sound, in the sense that for an unsatisfiable set of constraints, the provers can't convince the verifier to accept with probability one. So in this case we know $w(\mathsf{MS}) < 1$. Indeed, it is not hard to show that $w(G) = 17/18$, achieved by the following strategy: Alice answers $(1, 1, 1)$ all the time except that she answers $(1, 1, -1)$ for the third column. And Bob always answers 1.

Amazingly, we will see that $w^\star(\mathsf{MS}) = 1$, i.e., the entangled players have a strategy for which the verifier always accepts! To describe it, we need the following notation. The Pauli matrices are given by

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

and they satisfy the relations

$$\begin{aligned} X^2 = Y^2 = Z^2 &= \mathbb{I}, \\ XZ = -ZX, \quad XY = -YX, \quad ZY &= -YZ, \\ XY = iZ, \quad XZ = -iY, \quad ZX &= iY. \end{aligned}$$

Consider the 3×3 square of matrices

$$\begin{array}{|c|c|c|c} \hline \mathbb{I} \otimes Z & Z \otimes \mathbb{I} & Z \otimes Z & +\mathbb{I} \\ \hline X \otimes \mathbb{I} & \mathbb{I} \otimes X & X \otimes X & +\mathbb{I} \\ \hline X \otimes Z & Z \otimes X & Y \otimes Y & +\mathbb{I} \\ \hline \multicolumn{1}{c}{+\mathbb{I}} & \multicolumn{1}{c}{+\mathbb{I}} & \multicolumn{1}{c}{-\mathbb{I}} & \end{array}$$

The product of the matrices in each row and column equals either $+\mathbb{I}$ or $-\mathbb{I}$, as indicated above. Note that these relations are exactly the six constraints from earlier, except that they are about 2×2 matrices with $\{\pm 1\}$ eigenvalues instead of bits. The fact that the matrix algebra $M_{2\times 2}(\mathbb{C})$ is non-commutative explains why our earlier proof of impossibility no longer works: multiplying the matrices by rows or columns gives different results, $+\mathbb{I}$ or $-\mathbb{I}$, but this is not a contradiction since the matrices are multiplied in different orders.

Based on these observations we describe a quantum strategy for the players. The ancilla state that Alice and Bob use is

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle_{A_1}|0\rangle_{B_1} + |1\rangle_{A_1}|1\rangle_{B_1}) \otimes \frac{1}{\sqrt{2}} (|0\rangle_{A_2}|0\rangle_{B_2} + |1\rangle_{A_2}|1\rangle_{B_2}) = \frac{1}{2} \sum_{i=1}^{4} |i\rangle_A |i\rangle_B.$$

This is the "maximally entangled state". Note that the Schmidt coefficients are all equal to $1/2$.

Upon receiving her question Alice proceeds as follows: suppose for example that she is asked about the second row, corresponding to $(X \otimes \mathbb{I}, \mathbb{I} \otimes X, X \otimes X)$. She then makes a measurement on her two qubits in $|\psi\rangle$ in any orthonormal basis diagonalizing these three matrices (which in this case consists of the four states $|\pm\rangle|\pm\rangle$). Note that such a basis always exists since the matrices in the same row or column commute with each other. Now let the result be $|u\rangle$. Alice sets her answers a_1, a_2, a_3 to be the eigenvalues of $X \otimes \mathbb{I}$, $\mathbb{I} \otimes X$ and $X \otimes X$ respectively, corresponding to the eigenvector $|u\rangle$ that she obtained as a result of her measurement.

Bob proceeds in the same way. For example, suppose he is asked about the entry corresponding to $X \otimes X$. He makes a measurement in an orthonormal basis diagonalizing $X \otimes X$, and returns the corresponding eigenvalue.

Claim 9. $w^{\star}(\mathsf{MS}) = 1$.

Proof. We only need to verify that, if the players implement the strategy described above, their answers always satisfy the constraints checked by the verifier. First, the fact that Alice's answers satisfy the parity constraint follows from the fact that the matrices in the same row/column commute and their product satisfies the constraint: as a result, the product of the eigenvalues associated to any eigenvector must have the correct parity.

The consistence test is also passed with probability one: to see this, we use the fact that the maximally entangled state

$$|\psi\rangle = \frac{1}{2}\sum_{i=1}^{4} |i\rangle_A |i\rangle_B = \frac{1}{2}\sum_{i=1}^{4} |u_i\rangle|u_i\rangle$$

for any choice of basis $|u_i\rangle$ of $\mathbb{C}^4$. When Alice performs the measurement on her qubits and gets output $|u\rangle$, the state collapses to $|u\rangle_A |u\rangle_B$ and hence Bob always get the same output when he measures the state. □