CS286.2 Lecture 17: NP-hardness of computing $\omega^*(G)$

Scribe: Thomas Vidick

In the past lecture we introduced 3-player variants of both the CHSH and Magic Square games. These have the property that, even though from the point of view of classical players the new games are exactly as hard as the 2-player variants ($\omega(CHSH_2) = \omega(CHSH_3)$ and $\omega(MS_2) = \omega(MS_3)$), for quantum players the 3-player variants proved much more challenging: we showed $\omega^*(CHSH_3) = \omega(CHSH_3) < \omega^*(CHSH_2)$ and $\omega(MS_3) \leq \omega^*(MS_3) < \omega^*(MS_2) = 1$.

The intuition behind the three-player variants is that they make it harder for the quantum players to coordinate. In particular, for the case of CHSH the second player, B, is not told if he is playing CHSH with A or with C: even if he shares EPR pairs with each one of them, which pair should he measure?

In this lecture we show that a similar transformation applied to the clause-vs-variable game from our first lecture works, in the following sense. Recall that given any instance φ of a k-CSP on alphabet $\mathcal{A}$ we defined a game G_φ as follows:

2-player clause-vs-variable game G_φ. Given a constraint satisfaction problem $\varphi = (C_1, \ldots, C_m)$ on n variables x_i,

1. The referee selects an index $j \in [m]$ uniformly at random. Let $\{x_{i_1}, \ldots, x_{i_k}\}$ be the variables on which constraint C_j acts. The referee selects $t \in \{1, \ldots, k\}$ uniformly at random. He sends C_j to the first player, and t to the second player.

2. The first player replies with an assignment $(a_1, \ldots, a_k) \in \mathcal{A}^k$. The second player replies with an assignment $b \in \mathcal{A}$.

3. The referee accepts the players' answers if and only if the first player's answers satisfy clause C_j and the players' answers are consistent: $a_t = b$.

If $\omega(\varphi)$ denotes the maximum fraction of clauses of φ that are simultaneously satisfiable, we proved

$$\omega(\varphi) \leq \omega(G_\varphi) \leq 1 - \frac{1 - \omega(G_\varphi)}{k}, \tag{1}$$

and in particular φ is satisfiable if and only if there is a classical strategy for the players in G_φ that succeeds with probability 1. We also saw this is no longer true for quantum strategies, as the example of the magic square MS_2 demonstrates.

We will describe two other constructions of games, T_φ and F_φ, for which (1) also holds of the entangled value ω^* (at least in a weak sense). As a corollary we'll obtain NP-hardness results for the entangled value of the corresponding class of games.

Three-player games

We start with the construction of T_φ, which is a 3-player game.

3-player clause-vs-variable game T_φ. Given an instance $\varphi = (C_1, \ldots, C_m)$ of a k-CSP over alphabet $\mathcal{A}$, the referee proceeds as follows. He selects a random permutation of the three players, and names the first "Alice", the second "Bob", and the third "Charlie". He plays the 2-player clause-vs-variable game G_φ with Alice and Bob, ignoring Charlie. He accepts if and only if the referee in G_φ would have accepted. (The questions in G_φ can be sent at the same time as the players are revealed their respective names, so there is only one round of interaction. Charlie is not asked to provide any answer; if he does the answer is ignored.)

We show the following.

Proposition 1. *φ is satisfiable if and only if $\omega^*(T_\varphi) = 1$.*

Using the same proof as we will give below but carefully keeping track of approximations one can prove a more quantitative statement: there exists a constant $c > 1$ such that

$$\omega(\varphi) \;\leq\; \omega^*(T_\varphi) \;\leq\; 1 - \Big(\frac{1-\omega(\varphi)}{n}\Big)^c.$$

As an immediate corollary, we get that it is NP-hard to approximate $\omega^*(T_\varphi)$ to within inverse polynomial factors. This is our first hardness result for the entangled value ω^*, and it shows that the case of 2-player XOR games (for which ω^* could be approximated to within exponential precision in polynomial time via semidefinite programming) is very special.

Proof of Proposition 1. One implication is easy: if φ is satisfiable then there is a perfect classical strategy (simply answer the referee's questions according to a satisfying assignment), hence $\omega^(T_\varphi) \geq \omega(T_\varphi) = 1$.

The converse requires more work. Suppose $\omega^*(T_\varphi) = 1$. Our goal is to show $\omega(\varphi) = 1$, i.e. there exists a satisfying assignment. Suppose given a quantum strategy for the player that succeeds in T_φ with probability 1. The strategy is specified by a shared entangled state $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$ and POVM for each player. Because the game treats them symmetrically, we can assume that they always apply the same POVM when asked the same type of question: the players have some "Alice" POVMs $\{A_j^{a_1,\ldots,a_k}\}_{a_1,\ldots,a_k \in \mathcal{A}}$ for each possible clause C_j, $j \in [m]$, and "Bob" POVMs $\{B_i^b\}_{b\in\mathcal{A}}$ for every possible variable x_i, $i \in [n]$. For simplicity we will assume that all POVMs are projective, i.e. the measurement operators are projectors $(A_j^{a_1,\ldots,a_k})^2 = A_j^{a_1,\ldots,a_k}$ and $(B_i^b)^2 = B_i^b$ (in fact these conditions are easily seen to hold without loss of generality). The strategy's success probability in the game can be expressed as

$$\begin{aligned} 1 = \frac{1}{6}\Big(\frac{1}{m}\sum_{j\in[m]}\frac{1}{k}\sum_{i\in C_j}\sum_{(a_1,\ldots,a_k)\vdash C_j} \big(&\langle\Psi|A_j^{a_1,\ldots,a_k}\otimes B_i^{a_i}\otimes \mathrm{Id}\,|\Psi\rangle + \langle\Psi|B_i^{a_i}\otimes A_j^{a_1,\ldots,a_k}\otimes \mathrm{Id}\,|\Psi\rangle \\ &+ \langle\Psi|\,\mathrm{Id}\otimes A_j^{a_1,\ldots,a_k}\otimes B_i^{a_i}|\Psi\rangle + \langle\Psi|\,\mathrm{Id}\otimes B_i^{a_i}\otimes A_j^{a_1,\ldots,a_k}|\Psi\rangle \\ &+ \langle\Psi|A_j^{a_1,\ldots,a_k}\otimes B_i^{a_i}\otimes \mathrm{Id}\,|\Psi\rangle + \langle\Psi|B_i^{a_i}\otimes A_j^{a_1,\ldots,a_k}\otimes \mathrm{Id}\,|\Psi\rangle\big)\Big), \end{aligned} \quad (2)$$

where we used the notation $i \in C_j$ to mean that i is the index of one of the k variables on which C_j acts, and $(a_1,\ldots,a_k) \vdash C_j$ means that the tuple $(a_1,\ldots,a_k)$ is an assignment to the k variables on which C_j acts that satisfies the clause. Note the six terms, which simply correspond to the six possibilities for which player plays "Alice" and which plays "Bob".

Using that $(A_j^{a_1,\ldots,a_k})_{a_1,\ldots,a_k}$ and $(B_i^b)_b$ are POVM, and hence the measurement operators are positive and sum to identity, each term of the form $\sum_{(a_1,\ldots,a_k)\vdash C_j}\langle\Psi|A_j^{a_1,\ldots,a_k}\otimes B_i^{a_i}\otimes \mathrm{Id}\,|\Psi\rangle$ is at most 1. Eq. (2) thus

implies that each of them must equal exactly 1, so that for every $j \in [m]$, $i \in C_j$, and $a_i \in \mathcal{A}$ the following equality of vectors must hold:

$$\sum_{(a_1,\ldots,a_k)\vdash C_j} A_j^{a_1,\ldots,a_k} \otimes \mathrm{Id} \otimes \mathrm{Id}\,|\Psi\rangle \;=\; \mathrm{Id} \otimes B_i^{a_i} \otimes \mathrm{Id}\,|\Psi\rangle, \tag{3}$$

where to get equality for each possible $a_i \in \mathcal{A}$ we used that the $\mathrm{Id} \otimes B_i^{a_i} \otimes \mathrm{Id}\,|\Psi\rangle$ are orthogonal vectors for different a_i. Analogues of (3) hold where the A and B operators are positioned on any combination of the subsystems, and as a consequence we also have that for every $i \in [n]$ and $b \in \mathcal{A}$

$$B_i^b \otimes \mathrm{Id} \otimes \mathrm{Id}\,|\Psi\rangle \;=\; \mathrm{Id} \otimes B_i^b \otimes \mathrm{Id}\,|\Psi\rangle \;=\; \mathrm{Id} \otimes \mathrm{Id} \otimes B_i^b|\Psi\rangle. \tag{4}$$

Eqs. (3) and (4) are all we need to complete the proof. Define the following distribution on assignments to the n variables:

$$p(a_1,\ldots,a_n) \;=\; \left\| B_n^{a_n} \cdots B_1^{a_1} \otimes \mathrm{Id} \otimes \mathrm{Id}\,|\Psi\rangle \right\|^2.$$

To see that this is a distribution we use the following fact:

Fact 2. *Let $|u\rangle$ be any vector and $P_1,\ldots,P_k$ orthogonal projections that sum to identity. Then $\sum_i \|P_i|u\rangle\|^2 = \||u\rangle\|^2$.*

We will show the following: for any clause C_j acting on variables $\{x_{i_1},\ldots,x_{i_k}\}$,

$$p(a_{i_1},\ldots,a_{i_k}) \;=\; \sum_{a_i : i \notin \{i_1,\ldots,i_k\}} p(a_1,\ldots,a_n) \;=\; \left\| A_j^{a_{i_1},\ldots,a_{i_k}} \otimes \mathrm{Id} \otimes \mathrm{Id}\,|\Psi\rangle \right\|^2. \tag{5}$$

Eq. (5) implies that for any clause j, any assignment that has nonzero probability under p is an assignment that Alice could have returned when asked about clause j. Since the players win with certainty, the assignment must satisfy clause C_j. And since this holds for every j, the assignment satisfies φ. Hence any assignment in the support of p satisfies φ; since p is a distribution there is at least one such assignment and φ is satisfiable.

We prove (5) in two steps. First, using (4) repeatedly we get

$$B_n^{a_n} \cdots B_1^{a_1} \otimes \mathrm{Id} \otimes \mathrm{Id}\,|\Psi\rangle \;=\; \mathrm{Id} \otimes B_{i_k}^{a_{i_k}} \cdots B_{i_1}^{a_{i_1}} \otimes \prod_{i \notin \{i_1,\ldots,i_k\}} B_i^{a_i}|\Psi\rangle,$$

from which by taking squared norms and using Fact 2 repeatedly we deduce

$$p(a_{i_1},\ldots,a_{i_k}) \;=\; \left\| \mathrm{Id} \otimes B_{i_k}^{a_{i_k}} \cdots B_{i_1}^{a_{i_1}} \otimes \mathrm{Id}\,|\Psi\rangle \right\|^2. \tag{6}$$

Next using (3) repeatedly,

$$\begin{aligned}
\mathrm{Id}\otimes B_{i_k}^{a_{i_k}}\cdots B_{i_1}^{a_{i_1}}\otimes \mathrm{Id}\,|\Psi\rangle &= \Big(\sum_{\substack{(a'_1,\ldots,a'_k)\vdash C_j\\ a'_1=a_{i_1}}} A_j^{a'_1,\ldots,a'_k}\Big)\otimes B_{i_k}^{a_{i_k}}\cdots B_{i_2}^{a_{i_2}}\otimes \mathrm{Id}\,|\Psi\rangle \\
&= \Big(\sum_{\substack{(a'_1,\ldots,a'_k)\vdash C_j\\ a'_1=a_{i_1}}} A_j^{a'_1,\ldots,a'_k}\Big)\Big(\sum_{\substack{(a'_1,\ldots,a'_k)\vdash C_j\\ a'_2=a_{i_2}}} A_j^{a'_1,\ldots,a'_k}\Big)\otimes B_{i_k}^{a_{i_k}}\cdots B_{i_3}^{a_{i_3}}\otimes \mathrm{Id}\,|\Psi\rangle \\
&= \Big(\sum_{\substack{(a'_1,\ldots,a'_k)\vdash C_j\\ a'_1=a_{i_1},a'_2=a_{i_2}}} A_j^{a'_1,\ldots,a'_k}\Big)\otimes B_{i_k}^{a_{i_k}}\cdots B_{i_3}^{a_{i_3}}\otimes \mathrm{Id}\,|\Psi\rangle \\
&= \quad\cdots \\
&= \Big(\sum_{\substack{(a'_1,\ldots,a'_k)\vdash C_j\\ a'_1=a_{i_1},\ldots,a'_k=a_{i_k}}} A_j^{a'_1,\ldots,a'_k}\Big)\otimes \mathrm{Id}\otimes \mathrm{Id}\,|\Psi\rangle \\
&= A_j^{a_{i_1},\ldots,a_{i_k}}\otimes \mathrm{Id}\otimes \mathrm{Id}\,|\Psi\rangle,
\end{aligned}$$

where for the third equality we used that the $A_j^{a'_1,\ldots,a'_k}$ are orthogonal for different values of $(a'_1,\ldots,a'_k)$. Taking the squared norm in the above and combining with (6) shows (5) and concludes the proof. □

Two-player games

We would like to devise a similar construction as that of the game T_φ in the previous section, but now with only two players. The role of the third player in T_φ was simply to "confuse" the players: now they don't know with which of the other two players they are playing the game, and this makes it hard for them to use their entanglement in order to coordinate (the "technical" term for this phenomenon is *monogamy of entanglement*). The following game, introduced in [IKM09], achieves the same effect by sending Bob, instead of a single variable x_i on which C_j acts, *two* variables x_i and $x_{i'}$, one of which is completely unrelated with C_j. As we will see the fact that Bob doesn't know on which variable he is being tested is enough to confuse him and establish a two-player analogue of Proposition 1.

Confuse-SAT game F_φ. Given an instance $\varphi = (C_1,\ldots,C_m)$ of a k-CSP over alphabet $\mathcal{A}$, with n variables x_i:

1. The referee selects an index $j \in [m]$ uniformly at random. Let $\{x_{i_1},\ldots,x_{i_k}\}$ be the variables on which constraint C_j acts. The referee selects $t \in \{1,\ldots,k\}$ and $\ell \in \{1,\ldots,n\}$ uniformly at random. He sends C_j to the first player, and the lexicographically ordered pair $\{i_t,\ell\}$ to the second player.

2. The first player replies with an assignment $(a_1,\ldots,a_k) \in \mathcal{A}^k$. The second player replies with an assignment $(b,b') \in \mathcal{A}^2$.

3. The referee accepts the players' answers if and only if the first player's answers satisfy clause C_j and the players' answers are consistent on the variable they were both asked: $a_t = b$.

Proposition 3. *φ is satisfiable if and only if $\omega^*(F_\varphi) = 1$.*

Proof. As before, one implication is easy: if φ is satisfiable then there is a perfect winning strategy, that simply answers all questions according to a fixed satisfying assignment.

Conversely, suppose there exists a strategy that succeeds with probability 1. This is specified by a state $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ and POVM $(A_j^{a_1,\ldots,a_k})_{a_1,\ldots,a_k}$ for Alice and $(B_{t,\ell}^{b,b'})_{b,b'}$ for Bob. For every $i \in [n]$, define a new POVM $(C_i^c)_c$ by setting $C_i^c = \frac{1}{n}\sum_{t,b} B_{t,i}^{b,c}$, and introduce a distribution

$$p(a_1,\ldots,a_n) = \big\| \operatorname{Id} \otimes C_1^{a_1} \cdots C_n^{a_n} |\psi\rangle \big\|^2.$$

As in the proof of Proposition 1, our goal is to show that for any clause C_j acting on variables $\{x_{i_1},\ldots,x_{i_k}\}$ the marginal

$$p(a_{i_1},\ldots,a_{i_k}) \;=\; \big\| A_j^{a_{i_1},\ldots,a_{i_k}} \otimes \operatorname{Id} |\psi\rangle \big\|^2, \tag{7}$$

and this will conclude the proof.

Most of the ingredients of the proof of (7) are similar to that of (5), and we only sketch it here. The key step consists in showing that the C_i^c commute, in the following sense: for every $i \neq i'$ and $c, c' \in \mathcal{A}$,

$$\operatorname{Id} \otimes C_i^c C_{i'}^{c'} |\psi\rangle \;=\; \operatorname{Id} \otimes C_{i'}^{c'} C_i^c |\psi\rangle. \tag{8}$$

Using (8) it is not hard to show that the marginal

$$p(a_{i_1},\ldots,a_{i_k}) = \big\| \operatorname{Id} \otimes C_{i_k}^{a_{i_k}} \cdots C_{i_1}^{a_{i_1}} |\psi\rangle \big\|^2,$$

and from there the proof of (7) concludes similarly to that of (5) of Proposition 1. We indicate how (8) is obtained. The key is to use the fact that the strategy has success probability 1 to derive the following, which is obtained analogously to (3) and (4): for any $j \in [m]$, $i \in C_j$, $t \in [n]$ and $c \in \mathcal{A}$,

$$\Big(\sum_{\substack{(a'_{i_1},\ldots,a'_{i_k}) \vdash C_j \\ a'_i = c}} A_j^{a'_{i_1},\ldots,a'_{i_k}} \Big) \otimes \operatorname{Id} |\psi\rangle \;=\; \operatorname{Id} \otimes \Big(\sum_b B_{t,i}^{b,c} \Big) |\psi\rangle \;=\; \operatorname{Id} \otimes C_i^c |\psi\rangle.$$

Applying this equation twice, together with the analogue of (3) we see that

$$\begin{aligned}
\operatorname{Id} \otimes C_{i'}^{c'} C_i^c |\psi\rangle &= \Big(\sum_{\substack{(a'_{i_1},\ldots,a'_{i_k}) \vdash C_j \\ a'_i = c}} A_j^{a'_{i_1},\ldots,a'_{i_k}} \Big) \otimes C_{i'}^{c'} |\psi\rangle \\
&= \Big(\sum_{\substack{(a'_{i_1},\ldots,a'_{i_k}) \vdash C_j \\ a'_i = c}} A_j^{a'_{i_1},\ldots,a'_{i_k}} \Big) \otimes \Big(\sum_b B_{i,i'}^{b,c'} \Big) |\psi\rangle \\
&= \operatorname{Id} \otimes B_{i,i'}^{c,c'} |\psi\rangle,
\end{aligned}$$

where for the last equality we used that the $B_{i,i'}^{b,b'}$ are orthogonal for different values of b, b'. Since this last term does not depend on the order in which i, i' appear (recall that in the game Bob's pair of variables are sent as an unordered pair), we obtain (8), and this concludes the proof. □

In order to prove a quantitative variant of Proposition 3, starting from a strategy that has success probability $1-\varepsilon$, for some small $\varepsilon > 0$, in game F_φ, it is not hard to derive the following analogue of (8):

$$\frac{1}{n^2} \sum_{i,i'} \sum_{c,c'} \big\| \operatorname{Id} \otimes \big(C_i^c C_{i'}^{c'} - C_{i'}^{c'} C_i^c \big) |\psi\rangle \big\|^2 \;=\; O(\varepsilon). \tag{9}$$

Unfortunately, using (9) and following the proof of Proposition 3 introduces an error ε each time two measurement operators have to be commuted, and the result is that one can only show that assignments sampled according to p satisfy a random clause with probability $1 - O(n^c \varepsilon^d)$, for some constants $c, d > 0$. For this to be non-trivial we need $\varepsilon = 1/poly(n)$, which only leads to inverse-polynomial hardness of approximation. A much better result (constant-factor hardness of approximation) could be obtained if one could show that from (9) it follows that there exists new measurement operators $(D_i^d)_d$ such that, first, the D_i commute: $[D_i^d, D_{i'}^{d'}] = 0$ for every i, i', d, d', and second, they closely approximate the C_i:

$$\frac{1}{n} \sum_i \sum_c \left\| \mathrm{Id} \otimes \left(C_i^c - D_i^c\right) |\psi\rangle \right\|^2 = O(\varepsilon^g),$$

for some constant $g > 0$. Unfortunately it is unknown if this is true, and the question of constant-factor NP-hardness of $\omega^*(G)$ for two-player games G remains an open problem!

References

[IKM09] Tsuyoshi Ito, Hirotada Kobayashi, and Keiji Matsumoto. Oracularization and two-prover one-round interactive proofs against nonlocal strategies. In *Proc. 24th IEEE Conf. on Computational Complexity (CCC'09)*, pages 217–228. IEEE Computer Society, 2009.