Positivstellensatz, SDPs and Entangled Games

Today we are going to talk about an infinite hierarchy of semidefinite programmings which attempts to approximate the entangled value of multi-prover games [1]. This work is based on a recent result called non-commutative Positivstellensatz [2] about the representation of positive polynomials.

In a one-round two-prover cooperative game, a verifier asks questions to two provers, Alice and Bob, who cooperate with each other. A game $G = G(\pi, V)$ is specified by the set of questions S, T and answers A, B for Alice and Bob, a probability distribution $\pi : S \times T \to [0, 1]$, and a predicate $V : A \times B \times S \times T \to \{0, 1\}$. The referee samples $(s, t) \in S \times T$ according to π, and sends question s to Alice and questions t to Bob. Alice replies with an answer $a \in A$, and Bob replies with an answer $b \in B$. The provers win if and only if $V(a, b|s, t) = 1$. The provers are allowed to agree on a strategy before the game starts, but not allowed to communicate with each other after receiving their questions. The classical value of this game, denoted by $\omega_c(G)$, is the maximum probability with which the provers can win.

In the entangled version of this game, we allow the provers to share arbitrary prior entanglement and perform arbitrary local quantum operations. We use $\omega^*(G)$ to denote the maximum probability with which any entangled provers can win.

For example, CHSH game is a two-prover game in which $A = B = S = T = \{0, 1\}$ and $V(a, b|s, t) = 1$ if $a \oplus b = s \wedge t$, and 0 otherwise. For this game, any classical provers can win with probability at most $\omega_c(G) = 3/4$, but entangled provers can win with probability $\omega^*(G) = cos^2(\pi/8) \approx 0.85$.

Without loss of generality, we can assume the entangled prover's strategy as follows. They share a pure state $|\psi\rangle \in \mathbb{C}^{d\times d}$ for some $d \geq 1$. If Alice receives question s, then she performs a POVM $\{A_s^a\}$ on her part of $|\psi\rangle$, (i.e. $\sum_a A_s^a = I$, $A_s^a \geq 0$), and replies with answer a if the measurement outcome corresponds to A_s^a. Similarly, we define POVMs $\{B_t^b\}$ for Bob. So the probability that Alice answers a and Bob answers b is given by

$$P[a, b|s, t] = \langle\psi|A_s^a \otimes B_t^b|\psi\rangle. \tag{1}$$

Thus, the entangled value of this game is given by

$$\omega^*(G) = \lim_{d\to\infty} \max_{|\psi\rangle\in\mathbb{C}^{d\times d}} \max_{A_s^a, B_t^b} \sum_{a,b,s,t} \pi(s, t)V(a, b|s, t)\langle\psi|A_s^a \otimes B_t^b|\psi\rangle. \tag{2}$$

We are going to show that, there exists an infinite hierarchy of SDPs whose solutions converge to the field-theoretic value $\omega^f(G)$ defined below, which is conjectured to equal the entangled value $\omega^*(G)$.

Theorem 1. *There exists a hierarchy of SDPs whose solutions converge to $\omega^f(G)$.*

Lemma 2. $\omega^f(G) \geq \omega^*(G)$.

Conjecture 3. $\omega^*(G) = \omega^f(G)$.

In what follows, we will first define $\omega^f(G)$ and give the intuition why it seems to equal $\omega^*(G)$. Then, we reduce the problem of computing $\omega^f(G)$ to the problem of determining whether a polynomial (in the measurement operators) is positive, i.e. $q(\{A_s^a, B_t^b\}) > 0$, under some polynomial constraints $p_j(\{A_s^a, B_t^b\}) \geq 0$. Next, we apply the recent result of non-commutative Positivstellensatz, which basically states that this is true only if q lies in the convex cone generated by p_j's. At last, we show that testing the membership of a convex cone can be solved using a hierarchy of SDPs.

1 Field-theoretical value

The field-theoretic value of a game $G = G(\pi, V)$ defined as follows:

$$\omega^f(G) = \sup_{A_s^a, B_t^b} \| \sum_{a,b,s,t} \pi(s,t) V(a,b|s,t) A_s^a B_t^b \|, \tag{3}$$

where $A_s^a, B_t^b \in \mathbb{B}(\mathcal{H})$ for some Hilbert space $\mathcal{H}$, $\sum_a A_s^a = \sum_b B_t^b = I$, $A_s^a, B_t^b \geq 0$, and $[A_s^a, B_t^b] = 0$.

To prove lemma 2, one only needs to realize that for any A_s^a, B_t^b in Eq.(2), we can always choose $|\psi\rangle$ such that it is the eigenstate corresponding to the maximum eigenvalue of the operator

$$\sum_{a,b,s,t} \pi(s,t) V(a,b|s,t) A_s^a \otimes B_t^b = \sum_{a,b,s,t} \pi(s,t) V(a,b|s,t) \hat{A}_s^a \hat{B}_t^b,$$

where $\hat{A}_s^a = A_s^a \otimes I$ and $\hat{B}_t^b = I \otimes B_t^b$ are commutative. Then $\omega^*(G) \leq \omega^f(G)$ is obvious.

On the other hand, the following lemma states that, for finite-dimensional Hilbert spaces, the commutation relation and tensor product structure are equivalent.

Lemma 4. *Suppose $\mathcal{H}$ is a finite-dimensional Hilbert space, and $X_i, Y_j \in \mathbb{B}(\mathcal{H})$. Then the following conditions are equivalent:*
(1) $[X_i, Y_j] = 0, \ \forall i, j$;
(2) $\mathcal{H} = \bigoplus_\alpha \mathcal{H}_1^\alpha \otimes \mathcal{H}_2^\alpha$, *s.t.* $X_i \in \bigoplus_\alpha \mathbb{B}(\mathcal{H}_1^\alpha) \otimes \mathbb{I}(\mathcal{H}_2^\alpha)$, $Y_j \in \bigoplus_\alpha \mathbb{I}(\mathcal{H}_1^\alpha) \otimes \mathbb{B}(\mathcal{H}_2^\alpha)$.

As a result, if we only consider finite-dimensional spaces in the definition of $\omega^f(G)$, it should equal $\omega^*(G)$. The only possible difference may arise from the case of infinite-dimensional spaces. But, intuitively, one can imagine that there should exist some continuity and thus the field value should equal $\omega^*(G)$. It would be surprising if $\omega^f(G) > \omega^*(G)$, meaning that there is a gap between the limit of finite dimension case and the infinite dimension case.

2 Reduction to Polynomial Positivity

Our goal is to find the value of $\omega^f(G)$, which is the supremum of the operator norm of some polynomial in measurement operators $\{A_a^s, B_t^b\}$. Note that for a Hermitian operator M, $\|M\| = c$ if and only if $c'I - M > 0$ for any $c' > c$, but $c'I - M \not> 0$ for any $c' < c$. Thus, define

$$q_c = cI - \sum_{a,b,s,t} \pi(s,t) V(a,b|s,t) A_s^a B_t^b.$$

If $c > \omega^f(G)$, then: $q_c > 0$ for any A_s^a, B_t^b that satisfy

$$\begin{aligned} p_s^A &\equiv \sum_a A_s^a - I = 0, \\ p_t^B &\equiv \sum_b B_t^b - I = 0, \\ p_{a,s}^A &\equiv A_s^a \geq 0, \\ p_{b,t}^B &\equiv B_t^b \geq 0, \\ p_{a,b,s,t} &\equiv A_s^a B_t^b - B_t^b A_s^a = 0. \end{aligned}$$

On the other hand, if $c < \omega^f(G)$, this statement is not true. Note that q_c and $p_s^A, p_t^B, p_{a,s}^A, p_{b,t}^B, p_{a,b,s,t}$ are all polynomials in $\{A_a^s, B_t^b\}$.

So, suppose we have an oracle that solves the following problem: given a set of Hermitian polynomials $q, p_1, p_2, \ldots, p_m$ in Hermitian variables $X = (X_1, X_2, \ldots, X_n)$, is $q(X) > 0$ for any X that satisfies $p_j(X) \geq 0$? Then, we can approximate $\omega^f(G)$ to arbitrary accuracy by querying the oracle with q_c and $\{\pm p_s^A, \pm p_t^B, p_{a,s}^A, p_{b,t}^B, \pm i p_{a,b,s,t}\}$ for different values of c (i.e. using the binary search).

3 Positivstellensatz

Given a set of Hermitian polynomials $q, p_1, p_2, \ldots, p_m$ in Hermitian variables $X = (X_1, X_2, \ldots, X_n)$, is $q(X) > 0$ for any X that satisfies $p_j(X) \geq 0$? This question was answered in a recent paper by Helton and McCullough. They proved a non-commutative Positivstellensatz, which basically says that the answer to this question is yes only if q lies in the convex cone generated by $p_1, p_2, \ldots, p_m$. This theorem actually needs some extra conditions to hold. But these conditions hold for q_c and $\mathcal{Q}$. For a rigorous statement of non-commutative Positivstellensatz, see [2].

For a set of polynomials $p_1, p_2, \ldots, p_m$, the convex cone generated by them, denoted by $C_{\{p_j\}}$ is the set of polynomials of the form

$$q = \sum_{j=1}^{L} r_j^\dagger r_j + \sum_{i=1}^{m} \sum_{j=1}^{K} s_{ij}^\dagger p_i s_{ij}, \tag{4}$$

where L, K are finite, and r_j, s_{ij} are arbitrary polynomials. One can easily see that if $p_j(X) \geq 0$, then $q(X) \geq 0$ for any $q \in C_{\{p_j\}}$. The Positivstellensatz states that, in some sense, the converse is also true. Namely, if $q(X) > 0$ for any X that satisfy $p_j(X) \geq 0$, then $q \in C_{\{p_j\}}$, i.e. q can be written the form of Eq.(4).

4 Construction of the SDP Hierarchy

Now we show that the membership of a convex cone can be tested by using a hierarchy of SDPs.

The drawback of Eq.(4) is that we do not know the degrees of r_j and s_{ij}. It is possible that they have high degrees, but eventually the high-degree terms cancel on the righthand side of Eq.(4), resulting in a low-degree polynomial q. So we can only define a hierarchy of problems, in which the level-n problem requires that each term $r_j^\dagger r_j$, $s_{ij}^\dagger p_i s_{ij}$ should have degree $\leq 2n$. For example, the first level requires that each $r_j^\dagger r_j$ and $s_{ij}^\dagger p_i s_{ij}$ should be at most quadratic.

At each level, the degree of polynomials r_j and s_{ij} are fixed. So we can represent them by matrices. Specifically, a Hermitian polynomial f of degree d in Hermitian variables $X_1, \ldots, X_n$ can be represented by

$$f = Z^\dagger \Gamma_f Z,$$

where

$$Z = [1 \quad X_1 \quad \ldots \quad X_n \quad X_1X_2 \quad X_1X_3 \quad \ldots]^\dagger$$

is a vector consisting of all the monomials of degree $\leq d$ over $X_1, \ldots, X_n$, and Γ_f is a Hermitian matrix of corresponding size. Note that Γ_f might be not unique, i.e. a polynomial can have multiple representations. Furthermore, $f = \sum_j r_j^\dagger r_j$ for some polynomials r_j if and only if it has a positive semidefinite representation $\Gamma_f \geq 0$. This because if $\Gamma_f = \sum\limits_j u_j u_j^\dagger$, then $f = \sum\limits_j Z^\dagger u_j u_j^\dagger Z = \sum\limits_j r_j^\dagger r_j$, where $r_j = u_j^\dagger Z$ is a polynomial. The other direction is trivial.

Let

$$V = \sum_j r_j^\dagger r_j,$$
$$W_i = \sum_j s_{ij}^\dagger s_{ij}.$$

Then V and W_i are all sum of squares, and thus they have positive semidefinite representations Γ_V, Γ_{W_i}. Moreover, observing Eq.(4) carefully, one can be convinced that it is equivalent to a set of linear constraints on the entries of Γ_V, Γ_{W_i}. Each constraint verifies that the coefficients of a particular monomial are the same for both sides of Eq.(4). So, we want to find $\Gamma_V, \Gamma_{W_i} \geq 0$ subject to some linear constraints on their entries. This can be solved by a SDP.

5 Conclusion

The above arguments can be straightforwardly generalized to the cases of any number of provers.

There are two interesting open questions. One is to prove or disprove conjecture 3. Another is to find out exactly how fast this hierarchy of SDPs converges to the field-theoretic value. If conjecture 3 is solved affirmative and also some bound on the convergence speed of the hierarchy is established, then we might be able to provide some upper bound on the class MIP^*.

There is another hierarchy of SDPs [3, 4] that has also been proved to converge to the field value of multi-prover games. Instead of basing on representation theory of positive polynomials, that hierarchy is based on the moment matrix. It is dual to the one presented here.

References

[1] Andrew C. Doherty, Yeong-Cherng Liang, Ben Toner, Stephanie Wehner. The quantum moment problem and bounds on entangled multi-prover games. *CCC* 2008.

[2] J. William Helton and Scott A. McCullough. A positivstellensatz for non-commutative polynomials. *Trans. Amer. Math. Soc.*, 356(9):3721–3737, 2004.

[3] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98(1):010401, 2007.

[4] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. arXiv:0803.4290.