6.S979: Problem Set 2 Solutions

Due: November 6, 2020

1. **SDP duality, Tsirelson's characterization, and NPA** In this problem we will explore the connection between the "primal" view of the NPA hierarchy in terms of extended correlation matrices, and the "dual" view in terms of sums of squares. We'll do this for the special case of the Tsirelson characterization for XOR games.

   Let $\mathcal{X}$ and $\mathcal{Y}$ be Alice and Bob's respective input sets. Recall that an extended correlation matrix C with rows and columns indexed by $\mathcal{X} \cup \mathcal{Y}$ is allowed by Tsirelson's characterization if

   - $C \succeq 0$ (i.e. C is a Hermitian, positive semidefinite matrix).
   - $C_{ii} = 1$ for all $i \in \mathcal{X} \cup \mathcal{Y}$.
   - $C_{xy} = C_{yx}$ for all x, y.

   (a) Suppose we are given an extended correlation matrix C. For any product PQ where $P, Q \in \{A_x\}_{x \in \mathcal{X}} \cup \{B_y\}_{y \in \mathcal{Y}}$, define the *pseudo-expectation* $\tilde{\mathbf{E}}[PQ]$ to be the value of the corresponding entry of C:

   $$\tilde{\mathbf{E}}[A_x A_{x'}] = C_{xx'}, \quad \tilde{\mathbf{E}}[A_x B_y] = \tilde{\mathbf{E}}[B_y A_x] = C_{xy}, \quad \tilde{\mathbf{E}}[B_y B_{y'}] = C_{yy'}.$$

   We can extend this by linearity to define the pseudo-expectation of any linear combination of such products. Given a polynomial of the form

   $$p = (\alpha A_x + \beta B_y)^\dagger (\alpha A_x + \beta B_y),$$

   show that there exists a vector v such that

   $$\tilde{\mathbf{E}}[p] = v^\dagger C v.$$

   Take $v = \alpha |x\rangle + \beta |y\rangle$. Then

   $$\begin{aligned} v^\dagger C v &= (\alpha^* \langle x| + \beta^* \langle y|) C (\alpha |x\rangle + \beta |y\rangle) \\ &= |\alpha|^2 C_{xx} + \alpha^* \beta C_{xy} + \beta^* \alpha C_{yx} + |\beta|^2 C_{yy} \\ &= \tilde{\mathbf{E}}[|\alpha|^2 A_x A_x + \alpha^* A_x B_y + \beta^* \alpha B_y A_x + |\beta|^2 B_y B_y] \\ &= \tilde{\mathbf{E}}[p]. \end{aligned}$$

(b) Suppose we have an SoS certificate that the bias of some XOR game is at most ν of the form

$$\nu \cdot I - \sum_{x,y} s_{xy} A_x B_y = \sum_{i=1}^{k} r_i^\dagger r_i + \sum_x \alpha_x (I - A_x^2) + \sum_y \beta_y (I - B_y^2) + \sum_{x,y} \gamma_{x,y} ([A_x, B_y]),$$

where $s_{xy} \in \{\pm 1\}$, each r_i is a linear combination of A_x and B_y operators, and $\alpha_x, \beta_y, \gamma_{xy}$ are complex numbers. Show that this implies that for every correlation matrix C satisfying Tsirelson's criteria,

$$\tilde{\mathbf{E}}[\sum_{x,y} s_{xy} A_x B_y] \leq \nu.$$

This is known as "weak duality": it says that any SoS certificate of this form also upper-bounds the value attained by a Tsirelson correlation. In fact, it is true (but you need not prove) that "strong duality" holds: the optimal game value attained for a Tsirelson correlation is equal to the optimal upper-bound that can be proven by an SoS certificate of this form. *The idea is to apply $\tilde{\mathbf{E}}$ to both sides of the expression. First, let's extend $\tilde{\mathbf{E}}$ to polynomials that have a constant term by defining $\tilde{\mathbf{E}}[I] = 1$, and using linearity. Then, observe that for any x and y:*

$$\tilde{\mathbf{E}}[I - A_x^2] = 1 - C_{xx} = 0$$
$$\tilde{\mathbf{E}}[I - B_y^2] = 1 - C_{yy} = 0$$
$$\tilde{\mathbf{E}}[[A_x, B_y]] = C_{xy} - C_{yx} = 0.$$

Moreover, by the previous part, for each r_i there exists a vector v_i such that $\tilde{\mathbf{E}}[r_i^\dagger r_i] = v_i^\dagger C v_i$, which in turn is nonnegative by the fact that C is PSD. Hence, we obtain

$$\nu - \tilde{\mathbf{E}}[\sum_{x,y} s_{xy} A_x B_y] = \sum_i \tilde{\mathbf{E}}[r_i^\dagger r_i] + 0 \geq 0.$$

2. **Embezzlement and Schmidt coefficients** In this problem we will see a fun example of the utility of Schmidt coefficients. We consider the task of *embezzlement of entanglement*, introduced by van Dam and Hayden. In this setting, we imagine that Alice and Bob go to the entanglement bank to get a state $|\psi\rangle_{AB}$. They each perform a local operation on the state and their local registers, and then send the state back to the bank. Alice and Bob's goal is to extract one EPR pair of entanglement while modifying the bank's state as little as possible, i.e. to carry out the transformation

$$|\psi\rangle_{AB} \otimes |0\rangle_{A'} \otimes |0\rangle_{B'} \xrightarrow{V^A \otimes V^B} |\psi\rangle_{AB} \otimes \frac{1}{\sqrt{2}}(|0\rangle_{A'} \otimes |0\rangle_{B'} + |1\rangle_{A'} \otimes |1\rangle_{B'}),$$

where V^A is an isometry acting only on AA' and V^B is an isometry acting only on BB'.

(a) Suppose the Schmidt coefficients of $|\psi\rangle$ are $\sigma_1, \ldots, \sigma_k$ for some $k < \infty$. Write the Schmidt coefficients of the joint states on $AA'BB'$ before and after the embezzlement transformation. *Before, the Schmidt coefficients are $\sigma_1, \ldots, \sigma_k$, and after, they are $\sigma'_1 = \frac{1}{\sqrt{2}}\sigma_1, \sigma'_2 = \frac{1}{\sqrt{2}}\sigma_1, \sigma'_3 = \frac{1}{\sqrt{2}}\sigma_2, \ldots, \sigma'_{2k} = \frac{1}{\sqrt{2}}\sigma_k$.*

(b) Is embezzlement possible for finite k? Why or why not? *It is not possible, because before you have k nonzero Schmidt coefficients, and afterwards you have $2k$, whereas a local transformation of the form $V^A \otimes V^B$ cannot change the number of Schmidt coefficients.*

3. **Testing commutation:** In this problem we're going to analyze a game to test that two measurements approximately commute. This is very useful for analyzing MIP* proofs. In the basic commutation test, Alice is sent the question 0 asked for two answers a_0, a_1. Bob is sent a bit $y \in \{0, 1\}$, and responds with an answer b. The players win the test if $a_y = b$. We denote the players' shared stated by $|\psi\rangle$, Alice's measurement elements by $\{A_{a_0,a_1}\}$ and Bob's by $\{B_b^y\}$.

(a) Write an expression for the success probability of the players in the test. (Hint: it should look like a sum of terms of the form $\langle\psi| A \otimes B |\psi\rangle$ for some operators A, B.) *The success probability is*

$$p = \frac{1}{2} \sum_y \underbrace{\sum_{a_0,a_1} \langle\psi| A_{a_0,a_1} \otimes B_{a_y}^y |\psi\rangle}_{p_y} .$$

(b) Suppose Alice and Bob win the game with certainty. Prove that for any y,

$$\sum_{a_0,a_1} A_{a_0,a_1} \otimes B_{a_y}^y |\psi\rangle = |\psi\rangle .$$

From the previous part, $p = \frac{1}{2}(p_0 + p_1)$, and each p_y is between 0 and 1. So if $p = 1$, $p_0 = p_1 = 1$, and thus

$$\underbrace{\langle\psi| \sum_{a_0,a_1} A_{a_0,a_1} \otimes B_{a_y}^y |\psi\rangle}_{|\psi_y\rangle} = 1.$$

This is the inner product of $|\psi\rangle$ with a vector $|\psi_y\rangle$ whose norm is at most one; if the inner product is 1, then the two vectors must be equal.

(c) Deduce that

$$A_{a_0,a_1} \otimes I |\psi\rangle = A_{a_0,a_1} \otimes B_{a_0}^0 |\psi\rangle = \sum_{a_0'} A_{a_0',a_1} \otimes B_{a_0}^0 |\psi\rangle$$

$$A_{a_0,a_1} \otimes I |\psi\rangle = A_{a_0,a_1} \otimes B_{a_1}^1 |\psi\rangle = \sum_{a_1'} A_{a_0,a_1'} \otimes B_{a_1}^1 |\psi\rangle$$

Hint: use the previous part together with orthogonality between elements corresponding to different outcomes (e.g. the fact that $A_{a_0,a_1} A_{a_0',a_1} = 0$ for $a_0 \neq a_0'$). *We shall show this for $y = 0$; the calculations for $y = 1$ are completely analogous. By the fact that the A operators form a projective measurement, we know that $A_{a_0,a_1} A_{a_0',a_1'}$ is equal to A_{a_0,a_1} if $a_0 = a_0'$ and $a_1 = a_1'$, and 0 otherwise. Hence, applying the result of the previous part*

$$\begin{aligned} A_{a_0,a_1} \otimes I |\psi\rangle &= A_{a_0,a_1} \otimes I \Big(\sum_{a_0',a_1'} A_{a_0',a_1'} \otimes B_{a_0}^0 |\psi\rangle \Big) \\ &= A_{a_0,a_1} \otimes B_{a_0}^0 |\psi\rangle . \end{aligned}$$

Now, we will deduce the second equality, by using similar ideas together with the fact that the B measurement is projective (so $B^y_a B^y_{a'} = B^y_a$ if $a = a'$ and 0 otherwise).

$$\begin{aligned}\sum_{a'_0} A_{a'_0,a_1} \otimes B^0_{a_0} |\psi\rangle &= \sum_{a'_0} A_{a'_0,a_1} \otimes B^0_{a_0} (\sum_{a''_0,a'_1} A_{a''_0,a'_1} \otimes B^0_{a''_0} |\psi\rangle) \\ &= \sum_{a'_0} \sum_{a'_1} (A_{a_0,a_1} A_{a''_0,a'_1}) \otimes B^0_{a_0} |\psi\rangle \\ &= A_{a_0,a_1} \otimes B^0_{a_0} |\psi\rangle ,\end{aligned}$$

where we used the projectivity of the B measurement to set $a''_0 = a_0$ in the sum.

(d) Using the previous two parts, prove that

$$A_{a_0,a_1} \otimes I |\psi\rangle = I \otimes B^0_{a_0} B^1_{a_1} |\psi\rangle = I \otimes B^1_{a_1} B^0_{a_0} |\psi\rangle .$$

We use the second equality from each line of the previous part.

$$\begin{aligned}A_{a_0,a_1} \otimes I |\psi\rangle &= \sum_{a'_0} A_{a'_0,a_1} \otimes B^0_{a_0} |\psi\rangle \\ &= (I \otimes B^0_{a_0})(\sum_{a'_0} A_{a'_0,a_1} \otimes I) |\psi\rangle \\ &= (I \otimes B^0_{a_0})(\sum_{a'_0,a'_1} A_{a'_0,a'_1} \otimes B^1_{a_1}) |\psi\rangle \\ &= I \otimes B^0_{a_0} B^1_{a_1},\end{aligned}$$

where we used completeness of the A measurement to write $\sum_{a'_0,a'_1} A_{a'_0,a'_1} = I$. The same steps with 0 and 1 interchanged give us the Bs in the opposite order.

(e) Optional bonus: what about the case where Alice and Bob win with probability $1 - \epsilon$? Can you make a quantitative version of the preceding arguments work? *Essentially you have to do the previous parts keeping track of the Euclidean distance between the LHS and RHS of the vector equations.*

4. **Non-signalling correlations:** The NPA hierarchy gives us a collection of outer approximations to the set $\mathcal{C}_{qc}$ of quantum commuting correlations. A much cruder outer approximation is the set of *non-signalling correlations* $\mathcal{C}_{ns}$. A correlation $p(a, b|x, y)$ is non-signalling if for every a, x, y, y'

$$p(a|x, y) = p(a|x, y'),$$

and likewise for every b, x, x', y

$$p(b|x, y) = p(b|x', y).$$

That is, Alice's outcome probabilities for a given question should be the same regardless of Bob's question, and vice versa.

(a) Prove that $\mathcal{C}_{qc} \subseteq \mathcal{C}_{ns}$. Recall that a correlation is in $\mathcal{C}_{qc}$ if it can be written as

$$p(a, b|x, y) = \langle\psi| A^x_a B^y_b |\psi\rangle ,$$

for some state $|\psi\rangle$ and Hermitian operators A_a^x, B_b^y satisfying the conditions

$$\forall x, (A_a^x)^2 = A_a^x \quad \text{and} \quad \sum_a A_a^x = I$$
$$\forall y, (B_b^y)^2 = B_b^y \quad \text{and} \quad \sum_b B_b^y = I$$
$$\forall x, y, a, b, \ [A_a^x, B_b^y] = 0.$$

We have to show that every element of $\mathcal{C}_{qc}$ is also contained in $\mathcal{C}_{ns}$. We can do this by explicitly checking the nonsignalling conditions given in the problem statement. Given $p \in \mathcal{C}_{qc}$, choose any a, x, y, y':

$$\begin{aligned} p(a|x,y) &= \sum_b p(a,b|x,y) \\ &= \sum_b \langle\psi| A_a^x B_b^y |\psi\rangle \\ &= \langle\psi| A_a^x (\sum_b B_b^y) |\psi\rangle \\ &= \langle\psi| A_a^x (I) |\psi\rangle \\ &= \langle\psi| A_a^x (\sum_b B_b^{y'}) |\psi\rangle \\ &= p(a|x,y'). \end{aligned}$$

This shows that Bob cannot signal to Alice. To show the reverse is a totally analogous calculation. Choose any b, x, x', y:

$$\begin{aligned} p(b|x,y) &= \sum_a p(a,b|x,y) \\ &= \sum_a \langle\psi| A_a^x B_b^y |\psi\rangle \\ &= \langle\psi| (\sum_a A_a^x) B_b^y |\psi\rangle \\ &= \langle\psi| (I) B_b^y |\psi\rangle \\ &= \langle\psi| (\sum_a A_a^{x'}) B_b^y |\psi\rangle \\ &= p(b|x',y). \end{aligned}$$

(b) Show that there is a non-signalling correlation that wins the CHSH game with certainty.

The correlation is the one that for every pair of questions x, y returns one of the two winning pairs of answers a, b with probabilitly $1/2$ each. The nonzero probabilities in p are given by

$$p(0,0|0,0) = 1/2, p(1,1|0,0) = 1/2$$
$$p(0,0|0,1) = 1/2, p(1,1|0,1) = 1/2$$
$$p(0,0|1,0) = 1/2, p(1,1|1,0) = 1/2$$
$$p(0,1|1,1) = 1/2, p(1,0|1,1) = 1/2.$$

By construction, this wins CHSH with probability 1*, because it is only supported on winning pairs of answers. To see that it is nonsignalling, observe that for all* x, y*,* $p(a|x, y)$ *and* $p(b|x, y)$ *are both the uniform distribution over* $\{0, 1\}$*, so the conditions in the problem statement hold. (In words, if you imagine Alice and Bob have access to a magic pair of boxes that implement this correlation, Alice will always observe what looks to her like a totally uniform random bit, uncorrelated with anything else, so she cannot learn anything about Bob's question from the outcome of her box.)*