Lecture 5

Nonlocal games and XOR games

In previous lectures, we discussed a few fairly direct connections between quantum information theoretic notions and semidefinite programs. For instance, the semidefinite program associated with an optimization over measurements is quite simple and direct, and if you are familiar with the Choi representation of channels the same can be said about our semidefinite program for optimizing over channels. Similarly, the semidefinite programs for the trace norm and fidelity are straightforward, once you know about the lemma from the previous lecture characterizing 2-by-2 positive semidefinite block operators.

In this lecture and the next, we will study an example of a semidefinite programming formulation of a quantum information theoretic notion where the relevance of semidefinite programming is not at all evident from the start—sometimes some work is required (and perhaps some luck as well) before a connection between a particular notion and semidefinite programming becomes apparent.

5.1 Nonlocal games

We will begin by introducing the nonlocal game model, in which two individuals, Alice and Bob, cooperatively play a game of incomplete information.

A specific instance $G$ of a nonlocal game specifies that four finite and nonempty sets, $X$, $Y$, $A$, and $B$, are to be fixed. The sets $X$ and $Y$ represent sets of questions, while $A$ and $B$ represent sets of answers. Alice will receive a question $x \in X$, to which she must respond with an answer $a \in A$, while Bob receives a question $y \in Y$, to which he must respond with an answer $b \in B$. The probability with which each pair of questions $(x, y) \in X \times Y$ is selected is determined by a probability distribution

$$
\pi : X \times Y \to [0, 1],
$$

(5.1)
and it is deemed that a pair of answers \((a, b) \in A \times B\) is correct for the question pair \((x, y)\) if and only if a fixed predicate
\[
V : A \times B \times X \times Y \rightarrow \{0, 1\}
\]
evaluates to 1. (We will write \(V(a, b|x, y)\) to denote the value of this predicate on the input \((a, b, x, y)\) to stress the interpretation that a pair \((a, b)\) is correct or incorrect given that the question pair is \((x, y)\).) The game \(G\) is fully specified by the pair \((\pi, V)\), and one should imagine that Alice and Bob have a complete description of these objects.

One may consider various classes of strategies Alice and Bob may use in a nonlocal game. For instance, a deterministic classical strategy prescribes that Alice always chooses her answer by evaluating a function \(f : X \rightarrow A\) on the question she receives, and similarly Bob chooses his answer by evaluating a function \(g : Y \rightarrow B\). For such a strategy, one finds that the probability that Alice and Bob win (meaning that they answer correctly) is equal to
\[
\sum_{(x, y) \in X \times Y} \pi(x, y) V(f(x), g(y)|x, y).
\]
The classical value of a nonlocal game \(G\), which is denoted \(\omega(G)\), is given by a maximization of this winning probability over all choices of the functions \(f\) and \(g\). When considering such strategies, it is implicit that Alice and Bob are not able to communicate with one another once they have received their respective questions. (It is natural to ask whether randomness could provide an advantage over a deterministic strategy in the classical setting, but it is not difficult to prove that randomness cannot provide an advantage.)

In this lecture and the next, we will mainly be concerned with quantum strategies, which are more general than deterministic strategies. When speaking of a quantum strategy, we imagine that Alice and Bob have decided that they will play a given nonlocal game \(G\) by first preparing a pair of registers \((U, V)\) in a joint state \(\rho \in \mathcal{D}(U \otimes V)\); Alice holds the register \(U\) and Bob holds \(V\). Upon receiving a question \(x \in X\), Alice measures the register \(U\) with respect to a measurement described by the collection of measurement operators
\[
\{P^x_a : a \in A\} \subset \text{Pos}(U),
\]
satisfying the usual constraint
\[
\sum_{a \in A} P^x_a = 1_U
\]
on the positive semidefinite operators describing a measurement. Similarly, Bob measures \(V\) with respect to a measurement described by operators
\[
\{Q^y_b : b \in B\} \subset \text{Pos}(V),
\]
Lecture 5

satisfying

\[ \sum_{b \in B} Q_{b}^{y} = 1. \quad (5.7) \]

The probability that Alice and Bob respond to a question pair \((x, y)\) with an answer pair \((a, b)\) is then given by

\[ \langle P_{a}^{x} \otimes Q_{b}^{y}, \rho \rangle, \quad (5.8) \]

so that the probability this strategy wins is equal to

\[ \sum_{(x, y) \in X \times Y} \pi(x, y) \sum_{(a, b) \in A \times B} V(a, b | x, y) \langle P_{a}^{x} \otimes Q_{b}^{y}, \rho \rangle. \quad (5.9) \]

The quantum value of a nonlocal game \(G\), which is denoted \(\omega^{*}(G)\), is defined as the supremum of the winning probabilities taken over all choices of quantum strategies. It is not known if this supremum winning probability is always achieved by some strategy—there could be nonlocal games in which Alice and Bob can only approach the quantum value in the limit, as the dimensions of the spaces \(U\) and \(V\) become large.

5.2 XOR games

XOR games are a restricted type of nonlocal game in which both players answer binary values, so that \(A = B = \{0, 1\}\), and for which the predicate \(V\) takes the form

\[ V(a, b | x, y) = \begin{cases} 1 & \text{if } a \oplus b = f(x, y) \\ 0 & \text{if } a \oplus b \neq f(x, y) \end{cases} \quad (5.10) \]

for some choice of a function \(f : X \times Y \rightarrow \{0, 1\}\) (and where \(a \oplus b\) denotes the exclusive OR of \(a\) and \(b\)). Intuitively speaking, the function \(f\) specifies whether \(a\) and \(b\) should agree or disagree in order to be correct answers for a given question pair.

Two examples of nonlocal games follow, the first of which is an XOR game and the second of which is not.

Example 5.1 (CHSH game). The CHSH game (named after Clauser, Horn, Shimony, and Holt) is the nonlocal game in which the questions and answers correspond to binary values, \(X = Y = A = B = \{0, 1\}\), the probability \(\pi\) over question pairs is uniform,

\[ \pi(0, 0) = \pi(0, 1) = \pi(1, 0) = \pi(1, 1) = \frac{1}{4}, \quad (5.11) \]
and the predicate indicating correctness is defined as

$$V(a, b|x, y) = \begin{cases} 1 & \text{if } a \oplus b = x \land y \\ 0 & \text{if } a \oplus b \neq x \land y \end{cases}$$

(5.12)

(where $x \land y$ denotes the AND of $x$ and $y$). The CHSH game is evidently an XOR game, corresponding to the function $f(x, y) = x \land y$.

If we let $G$ denote the CHSH game, then we have that its classical value is $\omega(G) = 3/4$ and its quantum value is $\omega^*(G) = \cos^2(\pi/8) \approx 0.85$. It is easy enough to determine that the classical value is $3/4$ by simply considering each of the 16 possible deterministic classical strategies. The fact that the quantum value is $\cos^2(\pi/8)$ is not quite so simple—it can be proved in different ways, one of which will emerge at the end of the lecture following this one.

Example 5.2 (FFL game). The FFL game (named after Fortnow, Feige, and Lovász) is the nonlocal game in which the questions and answers correspond to binary values, $X = Y = A = B = \{0, 1\}$, the probability $\pi$ over question pairs is given by

$$\pi(0, 0) = \pi(0, 1) = \pi(1, 0) = \frac{1}{3}, \quad \pi(1, 1) = 0,$$

(5.13)

and the predicate indicating correctness is defined as

$$V(a, b|x, y) = \begin{cases} 1 & \text{if } a \lor x \neq b \lor y \\ 0 & \text{if } a \lor x = b \lor y \end{cases}$$

(5.14)

(where $a \lor x$ denotes the OR of $a$ and $x$, and similar for $b \lor y$). The FFL game is not an XOR game, which is clear from an inspection of $V$.

If we let $G$ denote the FFL game, then we have that its classical value and quantum value agree: $\omega(G) = \omega^*(G) = 2/3$. The fact that $\omega(G) = 2/3$ is easily established by testing all deterministic classical strategies. We will not prove the upper bound $\omega^*(G) \leq 2/3$, but it is not too difficult to do this. (One way to do this is to prove that even the so-called no-signaling value, which upper-bounds the quantum value, of the FFL game is $2/3$. The no-signaling value can be computed through linear programming.)

There is no particular reason why the quantum value $\omega^*(G)$ of a given nonlocal game $G$ should correspond to the optimal value of a semidefinite program derived in a simple way from $G$. Straightforward attempts to find a semidefinite program for the value $\omega^*(G)$ fail because the winning probability (5.9) is nonlinear in the direct sum of the collection of operators $\{P_a^x\}, \{Q_b^y\}$, and $\rho$ that describe a quantum strategy. We will see, however, that the quantum value of an XOR game can be
expressed by a semidefinite program, due to a theorem of Tsirelson that will be proved shortly.

Rather than working with the quantum value of XOR games, given by the supremum of the winning probability over all quantum strategies, we will consider the quantum bias of XOR games. For a given XOR game $G$, the quantum bias is denoted $\varepsilon^*(G)$, and is defined as the supremum of the probability of winning minus the probability of losing, ranging over all possible quantum strategies. As the probability of winning plus the probability of losing is always equal to 1, for any strategy, we have that the quantum bias $\varepsilon^*(G)$ and the quantum value $\omega^*(G)$ of any XOR game $G$ are related by the equation

$$\varepsilon^*(G) = 2\omega^*(G) - 1,$$

which is equivalent to

$$\omega^*(G) = \frac{1}{2} + \frac{\varepsilon^*(G)}{2}. \tag{5.16}$$

Of course, if we have a semidefinite program whose optimal value is $\varepsilon^*(G)$, we can trivially modify it to obtain a semidefinite program for $\omega^*(G)$—but we won’t bother doing that, and it will turn out to be more convenient to work with semidefinite programs for the quantum bias than for the quantum value anyway.

Suppose that an XOR game $G$, defined by a distribution $\pi : X \times Y \to [0, 1]$ and a function $f : X \times Y \to \{0, 1\}$, is given. For a quantum strategy represented by operators $\{P_x^0\}, \{Q_y^0\},$ and $\rho$, we have that the probability of winning minus the probability of losing is given by the following expression:

$$\sum_{x,y \in X \times Y} \pi(x,y)(-1)^{f(x,y)} \langle (P_x^0 - P_x^1) \otimes (Q_y^0 - Q_y^1), \rho \rangle. \tag{5.17}$$

By setting $A_x = P_x^0 - P_x^1$ for each $x \in X$ and $B_y = Q_y^0 - Q_y^1$ for each $y \in Y$, we may express this quantity as

$$\sum_{x,y \in X \times Y} \pi(x,y)(-1)^{f(x,y)} \langle A_x \otimes B_y, \rho \rangle. \tag{5.18}$$

Notice that as we range over all possible binary-valued measurements $\{R_0, R_1\}$, the operator $R_0 - R_1$ ranges over all Hermitian operators $H$ such that $\|H\| \leq 1$, and therefore the bias of $G$ is given by the supremum value of the expression (5.18) over all choices of operators

$$\{A_x : x \in X\} \subset \text{Herm}(\mathcal{U}),$$
$$\{B_y : y \in Y\} \subset \text{Herm}(\mathcal{V}), \tag{5.19}$$

and

$$\rho \in \text{D}(\mathcal{U} \otimes \mathcal{V}) \tag{5.20}$$

satisfying $\|A_x\| \leq 1$ and $\|B_y\| \leq 1$ for every $x \in X$ and $y \in Y$. 

5
5.3 A theorem of Tsirelson

Now we will prove the theorem of Tsirelson mentioned previously. The connection it makes between the bias of an XOR game and semidefinite programming will likely be apparent, but we will go through it in detail in the next lecture.

**Theorem 5.3** (Tsirelson’s theorem). Let $M \in \mathbb{R}^{n \times m}$ be a matrix. The following statements are equivalent:

1. There exist complex Euclidean spaces $\mathcal{U}$ and $\mathcal{V}$, a density operator $\rho \in \mathcal{D}(\mathcal{U} \otimes \mathcal{V})$, and two collections $\{A_1, \ldots, A_n\} \subset \text{Herm}(\mathcal{U})$ and $\{B_1, \ldots, B_m\} \subset \text{Herm}(\mathcal{V})$ of operators such that $\|A_j\| \leq 1$, $\|B_k\| \leq 1$, and

$$M(j, k) = \langle A_j \otimes B_k, \rho \rangle \quad (5.21)$$

for all $j \in \{1, \ldots, n\}$ and $k \in \{1, \ldots, m\}$.

2. There exist positive semidefinite operators $R \in \text{Pos}(\mathbb{C}^n)$ and $S \in \text{Pos}(\mathbb{C}^m)$, with $R(j, j) = 1$ and $S(k, k) = 1$ for all $j \in \{1, \ldots, n\}$ and $k \in \{1, \ldots, m\}$, such that

$$\begin{pmatrix} R & M \\ M^* & S \end{pmatrix} \succeq 0. \quad (5.22)$$

The proof of this theorem will make use of a collection of unitary and Hermitian operators known as Weyl–Brauer operators.

**Definition 5.4.** Let $N$ be a positive integer and let $\mathbb{Z} = \mathbb{C}^2$. The Weyl–Brauer operators of order $N$ are the operators $V_1, \ldots, V_{2N+1} \in \text{L}(\mathbb{Z}^\otimes N)$ defined as

$$V_{2k-1} = \sigma_z \otimes (k-1) \otimes \sigma_x \otimes 1 \otimes (N-k),$$

$$V_{2k} = \sigma_z \otimes (k-1) \otimes \sigma_y \otimes 1 \otimes (N-k), \quad (5.23)$$

for all $k \in \{1, \ldots, N\}$, as well as

$$V_{2N+1} = \sigma_z \otimes N, \quad (5.24)$$

where $1$, $\sigma_x$, $\sigma_y$, and $\sigma_z$ denote the Pauli operators:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (5.25)$$
Example 5.5. In the case $N = 3$, the Weyl–Brauer operators $V_1, \ldots, V_7$ are

\begin{align*}
V_1 &= \sigma_x \otimes 1 \otimes 1 \\
V_2 &= \sigma_y \otimes 1 \otimes 1 \\
V_3 &= \sigma_z \otimes \sigma_x \otimes 1 \\
V_4 &= \sigma_z \otimes \sigma_y \otimes 1 \\
V_5 &= \sigma_z \otimes \sigma_z \otimes \sigma_x \\
V_6 &= \sigma_z \otimes \sigma_z \otimes \sigma_y \\
V_7 &= \sigma_z \otimes \sigma_z \otimes \sigma_z.
\end{align*}

(5.26)

A proposition summarizing the properties of the Weyl–Brauer operators that are relevant to the proof of Tsirelson’s theorem follows.

Proposition 5.6. Let $N$ be a positive integer, let $V_1, \ldots, V_{2N+1}$ denote the Weyl–Brauer operators of order $N$. For every unit vector $u \in \mathbb{R}^{2N+1}$, the operator

\[ \sum_{k=1}^{2N+1} u(k)V_k \]  

is both unitary and Hermitian, and for any two vectors $u, v \in \mathbb{R}^{2N+1}$, it holds that

\[ \frac{1}{2N} \left\langle \sum_{j=1}^{2N+1} u(j)V_j, \sum_{k=1}^{2N+1} v(k)V_k \right\rangle = \langle u, v \rangle. \]  

(5.28)

Proof. Each operator $V_k$ is Hermitian, and therefore the operator (5.27) is Hermitian as well.

The Pauli operators anti-commute in pairs:

\[ \sigma_x \sigma_y = -\sigma_y \sigma_x, \quad \sigma_x \sigma_z = -\sigma_z \sigma_x, \quad \text{and} \quad \sigma_y \sigma_z = -\sigma_z \sigma_y. \]  

(5.29)

By an inspection of the definition of the Weyl–Brauer operators, it follows that $V_1, \ldots, V_{2N+1}$ also anti-commute in pairs:

\[ V_j V_k = -V_k V_j \]  

(5.30)

for distinct choices of $j, k \in \{1, \ldots, 2N + 1\}$. Moreover, each $V_k$ is unitary (as well as being Hermitian), and therefore $V_k^2 = 1^{\otimes N}$. It follows that

\[ \left( \sum_{k=1}^{2N+1} u(k)V_k \right)^2 = \sum_{k=1}^{2N+1} u(k)^2 V_k^2 + \sum_{1 \leq j < k \leq 2N+1} u(j)u(k)(V_j V_k + V_k V_j) \]

\[ = \sum_{k=1}^{2N+1} u(k)^2 1^{\otimes N} = 1^{\otimes N}, \]  

(5.31)
and therefore (5.27) is unitary.

Next, observe that
\[
\langle V_j, V_k \rangle = \begin{cases} 
2^N & \text{if } j = k \\
0 & \text{if } j \neq k.
\end{cases}
\] (5.32)

Therefore, one has
\[
\frac{1}{2^N} \left( \sum_{j=1}^{2^N} u(j) V_j, \sum_{k=1}^{2^N} v(k) V_k \right) = \sum_{k=1}^{2^N+1} u(k) v(k) = \langle u, v \rangle,
\] (5.33)
as required.

**Proof of Theorem 5.3.** Assume that statement 1 holds, and define an operator
\[
K = \begin{pmatrix}
\text{vec}((A_1 \otimes 1)\sqrt{\rho})^* \\
\vdots \\
\text{vec}((A_n \otimes 1)\sqrt{\rho})^* \\
\text{vec}((1 \otimes B_1)\sqrt{\rho})^* \\
\vdots \\
\text{vec}((1 \otimes B_m)\sqrt{\rho})^*
\end{pmatrix} \in L(\mathcal{U} \otimes \mathcal{V} \otimes \mathcal{U} \otimes \mathcal{V}, \mathbb{C}^{n+m}).
\] (5.34)

The operator \(KK^* \in \text{Pos}(\mathbb{C}^{n+m})\) may be written in a block form as
\[
KK^* = \begin{pmatrix}
P & M \\
M^* & Q
\end{pmatrix}
\] (5.35)
for \(P \in \text{Pos}(\mathbb{C}^n)\) and \(Q \in \text{Pos}(\mathbb{C}^m)\); the fact that the off-diagonal blocks are as claimed follows from the calculation
\[
\langle (A_j \otimes 1)\sqrt{\rho}, (1 \otimes B_k)\sqrt{\rho} \rangle = \langle A_j \otimes B_k, \rho \rangle = M(j, k).
\] (5.36)

For each \(j \in \{1, \ldots, n\}\) one has
\[
P(j,j) = \langle (A_j \otimes 1)\sqrt{\rho}, (A_j \otimes 1)\sqrt{\rho} \rangle = \langle A_j^2 \otimes 1, \rho \rangle,
\] (5.37)
which is necessarily a nonnegative real number in the interval \([0, 1]\); and through a similar calculation, one finds that \(Q(k,k)\) is also a nonnegative integer in the interval \([0, 1]\) for each \(k \in \{1, \ldots, m\}\). A nonnegative real number may be added to each diagonal entry of this operator to yield another positive semidefinite operator, so one has that statement 2 holds.
Next, assume statement 2 holds, and observe that

$$\frac{1}{2} \begin{pmatrix} R & M \\ M^* & S \end{pmatrix} + \frac{1}{2} \begin{pmatrix} R & M^T \\ M^* & S \end{pmatrix} = \begin{pmatrix} \frac{R + R}{2} & M \\ \frac{M^* + S}{2} & \frac{S + S}{2} \end{pmatrix}$$  \hspace{1cm} (5.38)$$

is a positive semidefinite operator having real number entries, and all of its diagonal entries are equal to 1. It follows that statement 2 holds for \( R \) and \( S \) being positive semidefinite operators whose entries are all real.

A matrix with real number entries is positive semidefinite if and only if it is the Gram matrix of a collection of real vectors, and therefore there must exist real vectors \( \{u_1, \ldots, u_n, v_1, \ldots, v_m\} \) such that

$$\langle u_j, v_k \rangle = M(j, k)$$  \hspace{1cm} (5.39)$$

for all \( j \in \{1, \ldots, n\} \) and \( k \in \{1, \ldots, m\} \), as well as

$$\langle u_{j_0}, u_{j_1} \rangle = R(j_0, j_1) \quad \text{and} \quad \langle v_{k_0}, v_{k_1} \rangle = S(k_0, k_1)$$  \hspace{1cm} (5.40)$$

for all \( j_0, j_1 \in \{1, \ldots, n\} \) and \( k_0, k_1 \in \{1, \ldots, m\} \). There are \( n + m \) of these vectors, and therefore they span a real vector space of dimension at most \( n + m \), so there is no loss of generality in assuming \( u_1, \ldots, u_n, v_1, \ldots, v_m \in \mathbb{R}^{n+m} \). Observe that these vectors are all unit vectors, as the diagonal entries of \( R \) and \( S \) represent their norm squared.

Now choose \( N \) so that \( 2N + 1 \geq n + m \) and let \( Z = \mathbb{C}^2 \). Define operators \( A_1, \ldots, A_n, B_1, \ldots, B_m \in L(Z^{\otimes N}) \) as

$$A_j = \sum_{i=1}^{n+m} u_j(i) V_i \quad \text{and} \quad B_k = \sum_{i=1}^{n+m} v_k(i) V_i^T$$  \hspace{1cm} (5.41)$$

for each \( j \in \{1, \ldots, n\} \) and \( k \in \{1, \ldots, m\} \), where \( V_1, \ldots, V_{n+m} \) are the first \( n + m \) Weyl–Brauer operators of order \( N \). By Proposition 5.6, each of these operators is both unitary and Hermitian, and therefore each of these operators has spectral norm equal to 1. Finally, define \( \rho = \mathbf{w} \mathbf{w}^* \) for

$$w = \frac{1}{\sqrt{2^N}} \text{vec}(1^{\otimes N}) \in Z^{\otimes N} \otimes Z^{\otimes N}. \hspace{1cm} (5.42)$$

Applying Proposition 5.6 again gives

$$\langle A_j \otimes B_k, \rho \rangle = \frac{1}{2N} \langle A_j, B_k^T \rangle = \langle u_j, v_k \rangle = M(j, k)$$  \hspace{1cm} (5.43)$$

for each \( j \in \{1, \ldots, n\} \) and \( k \in \{1, \ldots, m\} \). We have proved that statement 2 implies statement 1 (where we have implicitly chosen \( U = Z^{\otimes N} \) and \( V = Z^{\otimes N} \)), and so the proof is complete. \( \Box \)