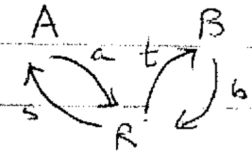
May 10, 2011
SDP in Quantum Information, Ashwin Nayak
XOR non-local games



$a \oplus b = f(s,t)$

Recall the CHSH-game: two parties A & B are asked a uniformly random pair of questions $s, t \in \{0,1\}$, respectively. Their goal is to respond with bits $a, b \in \{0,1\}$ such that

$$a \oplus b = s \wedge t.$$

It is well know that in a classical world, the maximum probability of succes $\leq 3/4$, whereas if the players A, B were allowed to share an EPR pair, they can succeed with probability $\cos^2 \frac{\pi}{8} \approx 0.853\ldots = \left(\frac{1+\sqrt{2}}{2\sqrt{2}}\right)$. In fact, the latter is optimal, even when arbitrary entanglement is allowed

This is an example of a XOR non-local game. In general, such a game has the following form:

1) A referee samples a pair of questions $(s,t) \in S \times T$ according to a probability distribution π over $S \times T$, and sends s to A, t to B.

2) The two parties respond, without communication with each other, with answers a, b, respectively.

3) The referee accepts iff $a \oplus b = f(s,t)$, where f is a specified Boolean function on $S \times T$.

So the game is determined by $S \times T$, π, f.
The two players may communicate arbitrarily before they receive the questions. So, in effect, they may begin with a shared

random string in the classical case, and a shared quantum state in the quantum case. They respond by computing their answer from their half of the shared state & the question.

<u>Question</u> suppose we play two games G_1, G_2 simultaneously. Is the best strategy to succeed in <u>both</u>, to play the two games independently? (think about performing two experiments simultaneously. what guarantees that the statistics generated are independent?)

If we play the CHSH game twice, classically, there is a strategy that beats playing the two games independently. What about quantum strategies? For a XOR-game G, let $\omega_q(G)$ denote the supremum over all strategies of the probability of success.

<u>Theorem</u> (Cleve, Slofstra, Unger, Upadhyay)
For any two XOR games G_1, G_2,
$$\omega_q(G_1 \wedge G_2) = \omega_q(G_1) \cdot \omega_q(G_2).$$

An important step in arriving at this result is a property of the "sum" of two games G_1, G_2. The sum $G_1 \oplus G_2$ is the game in which the referee generates, independently, questions (s_1, t_1), (s_2, t_2) from the two respective distributions π_1, π_2, and sends (s_1, s_2) to A, (t_1, t_2) to B. The players A, B respond with bits a, b, so as to achieve: $a \oplus b = f_1(s_1, t_1) \oplus f_2(s_2, t_2)$, where f_1 & f_2 are the functions in G_1, G_2, resp.

If the players play the two games independently, get answers (a_1, a_2) & (b_1, b_2), resp, and send $a = a_1 \oplus a_2$, $b = b_1 \oplus$

their probability of success is
$$\omega_q(G_1)\,\omega_q(G_2) + (1-\omega_q(G_1))(1-\omega_q(G_2)).$$

<u>Theorem</u> (CSUU) $\omega_q(G_1 \oplus G_2)$ <u>equals</u> the expression above.
("Additivity" property)

This is proven using SDPs, and follows by studying <u>symmetric</u> games.

Define the bias $\varepsilon_q(G)$ of a quantum game as

$$\varepsilon_q(G) = \omega_q(G) - (1-\omega_q(G)) = 2\omega_q(G) - 1$$
(Prob. of winning) − (Prob. of losing)

(We will drop the 'q' subscript, as we will only study quantum games henceforth.)

The theorem above is equivalent to: (Verify!)
$$\varepsilon(G_1 \oplus G_2) = \varepsilon(G_1)\cdot\varepsilon(G_2). \qquad (1)$$

We use a characterization of quantum strategies due to Tsirelson. A quantum strategy consists of a shared quantum state $|\psi\rangle \in \mathcal{H} \otimes \mathcal{K}$, and a set of measurements
$$\begin{cases} (\Pi^A_s,\ I-\Pi^A_s), & s \in S \\ (\Pi^B_t,\ I-\Pi^B_t), & t \in T \end{cases}$$
outcome 0, 1

on $\mathcal{H}$ & $\mathcal{K}$, respectively, that correspond to the computation of answers a, b, on questions s, t. It is more convenient to represent these measurements as observables
$$A_s = 2\Pi^A_s - I$$
$$B_t = 2\Pi^B_t - I.$$
(w.l.o.g Π^A_s, Π^B_t are orthogonal projections)

Then, the bias of the above strategy
$$= \sum_{s,t} \pi(s,t)\,(-1)^{f(s,t)} \langle\psi| A_s \otimes B_t |\psi\rangle \qquad (2)$$
(Verify!)

<u>Theorem</u> (Tsirelson) $\exists$ unit vectors $x_s, y_t \in \mathbb{R}^{2n^2}$, where $n = \dim(\mathcal{H}) = \dim$ such that

$$\langle\psi| A_s \otimes B_t |\psi\rangle = x_s^T \cdot y_t \qquad \text{——— (3)}$$

for all $(s,t) \in S \times T$. Conversely, given unit vectors $(x_s), (y_t) \in \mathbb{R}^N$, $\exists$ observables A_s, B_t with ± 1-eigenvalues, & $|\psi\rangle$ on $\mathcal{H} \otimes \mathcal{K}$, $\dim(\mathcal{H})$ (or $\mathcal{K}$) $= 2^{\lceil N/2 \rceil}$ s.t. (3) holds.

<u>Note</u>: The matrix $(x_s^T \cdot y_t)$ may be thought of as a submatrix of a Gram matrix, so that the problem of maximizing $\varepsilon(G)$, or equivalently $\omega(G)$, may be expressed as an SDP.

$(x_s^T y_t)$ is a submatrix of $W^T W$, where

$$W = \begin{array}{c} \begin{bmatrix} \uparrow & \uparrow \\ x_s & y_t \\ \downarrow & \downarrow \end{bmatrix} \\ \begin{array}{cc} \underbrace{\quad}_{S} & \underbrace{\quad}_{T} \end{array} \end{array}$$

Since x_s & y_t are unit vectors, the diagonal entries of $W^T W$ are all 1. Moreover $W^T W \geq 0$. Conversely, given a matrix $X \geq 0$, real, with diagonal $= \bar{1}$, its polar decomposition $X = W^T W$ gives us the unit vectors x_s, y_t. (of dim $\leq |S| + |T|$.)

Define the matrix $P = \left(\pi(s,t)(-1)^{f(s,t)}\right)_{s,t}$, and the matrix $Q = \begin{bmatrix} 0 & \frac{1}{2}P \\ \frac{1}{2}P^T & 0 \end{bmatrix}$, as the "cost matrix" of G.

Then from (2), we have that the bias of a strategy given by $(A_s), (B_t), |\psi\rangle$ is $\mathrm{Tr}(Q^T X)$, and the opt strategy by:

$$\sup \ \mathrm{Tr}(Q^T X)$$

subject to $\qquad\qquad (P_{XOR}) \equiv (P_Q)$

$$\mathrm{diag}(X) = \bar{1}$$

$$X \geq 0$$

(X is real, of dim $(|S|+|T|) \times (|S|+|T|)$)

Its dual is given by

$$\inf \quad (u,v)^T \cdot \mathbf{1} \qquad (D_Q)$$

subject to

$$\Delta(u,v) \geq Q$$

where $u \in \mathbb{R}^{|S|}$, $v \in \mathbb{R}^{|T|}$, and $\Delta^{(u,v)}$ is the matrix with u & v on its diagonal & 0 elsewhere:

$$\Delta(u,v) = \left[\begin{array}{c|c} \begin{matrix} \ddots & 0 \\ 0 & \ddots \end{matrix}\ u & 0 \\ \hline 0 & \begin{matrix} \ddots & 0 \\ 0 & \ddots \end{matrix}\ v \end{array}\right] \qquad \mathrm{diag}(\Delta(u,v)) = (u,v).$$

<u>Proposition</u>: Both P_Q & D_Q have Slater points, so strong duality holds, & both achieve their optima. Moreover P_Q may be modified without changing its optimum so that its feasible region is well-bounded with parameters (R, r) with $R = |S| + |T|$, & $r = 1$. (Similarly with D_Q.) So the optimum of P_Q & D_Q can be approximated efficiently.
(HW)

<u>Corollary</u>: $\oplus \mathrm{MIP}^* \subseteq \mathrm{EXP}$.

<u>Proof of the additivity property</u>:

$$\varepsilon(G_1 \oplus G_2) = \varepsilon(G_1) \cdot \varepsilon(G_2).$$

Playing the two games independently gives us

$$\varepsilon(G_1 \oplus G_2) \geq \varepsilon(G_1) \cdot \varepsilon(G_2) \qquad \text{(Verify!)} \quad \text{—— (4)}$$

So we need only prove

$$\varepsilon(G_1 \oplus G_2) \leq \varepsilon(G_1) \cdot \varepsilon(G_2). \quad \text{—— (5)}$$

If the cost matrix of G_i is

$$Q_i = \begin{bmatrix} & \frac{1}{2} P_i \\ \frac{1}{2} P_i^T & \end{bmatrix} \qquad (i = 1, 2)$$

then the cost matrix of $G_1 \oplus G_2$ is

$$Q = \begin{bmatrix} & \frac{1}{2} P_1 \otimes P_2 \\ \frac{1}{2} P_1^T \otimes P_2^T & \end{bmatrix}$$

Given an optimal feasible solution to each the dual for G_1 & G_2, we'll construct a feasible solution for the dual of $G_1 \oplus G_2$, such that the objective function value is $\le$ product of the two optima. This proves (5).

Let (u_1, v_1) & (u_2, v_2) be optimal feasible solutions to D_{Q_1} & D_{Q_2}, resp. Then

$$R_1 = \begin{pmatrix} \Delta(u_1) & -\frac{1}{2} P_1 \\ -\frac{1}{2} P_1^T & \Delta(v_1) \end{pmatrix} \succeq 0 \quad \& \; R_2 = \begin{pmatrix} \Delta(u_2) & -\frac{1}{2} P_2 \\ -\frac{1}{2} P_2^T & \Delta(v_2) \end{pmatrix} \succeq 0 .$$

Consider $2(u_1 \otimes u_2, v_1 \otimes v_2)$. We claim that it is feasible for D_Q, i.e.,

$$\begin{pmatrix} 2 \cdot \Delta(u_1 \otimes u_2) & -\frac{1}{2} P_1 \otimes P_2 \\ -\frac{1}{2} P_1^T \otimes P_2^T & 2 \Delta(v_1 \otimes v_2) \end{pmatrix} \succeq 0$$

Note: $\Delta(u_1 \otimes u_2) = \Delta(u_1) \otimes \Delta(u_2)$

Indeed, this is (two times) a principal submatrix of $R_1' \otimes R_2$, where

$$R_1' = \begin{pmatrix} \Delta(u_1) & \frac{1}{2} P_1^T \\ \frac{1}{2} P_1^T & \Delta(v_1) \end{pmatrix} = \begin{pmatrix} I & \\ & -I \end{pmatrix} R_1 \begin{pmatrix} I & \\ & -I \end{pmatrix} \succeq 0$$

So that

$$R_1' \otimes R_2 = \begin{pmatrix} \Delta(u_1) \otimes \Delta(u_2) & & -\frac{1}{4} P_1 \otimes P_2 \\ & \cdot & \\ -\frac{1}{4} P_1^T \otimes P_2^T & & \Delta(v_1) \otimes \Delta(v_2) \end{pmatrix} \succeq 0 .$$

where we have omitted the unimportant blocks of $R_1' \otimes R_2$.

Consider the objective function value of this soln :

$$2\,(u_1 \otimes u_2\,,\ v_1 \otimes v_2)^T \cdot \bar{1}$$
$$= 2\left[(u_1 \otimes u_2)^T \cdot \bar{1} \ + \ (v_1 \otimes v_2)^T \cdot \bar{1}\right]$$
$$= 2\left[(u_1^T \cdot \bar{1})(u_2^T \cdot \bar{1}) \ + \ (v_1^T \cdot \bar{1})(v_2^T \cdot \bar{1})\right], \qquad (6)$$

where the dual optima for D_{Q_1}, D_{Q_2} are

$$(u_i, v_i)^T \cdot \bar{1} \ = \ (u_i^T \cdot 1) \ + \ (v_i^T \cdot 1)\ , \qquad i = 1, 2 \,.$$

<u>Claim</u>: We may choose (u_i, v_i) s.t. $u_i^T \cdot 1 = v_i^T \cdot 1$.

<u>Proof</u>: If they are unequal, scale (u_i, v_i) as $(u_i', v_i') = (\lambda u_i, \frac{1}{\lambda} v_i)$ s.t. $\lambda u_i^T \cdot 1 = \frac{1}{\lambda} v_i^T \cdot 1$

(Note: since $P_i \neq 0$, $u_i, v_i \neq 0$. Further, they are both non-negative $\because$ of the dual constraint.)

This gives obj. fn. value

$$= 2\sqrt{(u_i^T \cdot \bar{1})(v_i^T \cdot \bar{1})} \ \leq \ (u_i^T \cdot \bar{1}) + (v_i^T \cdot \bar{1}).$$

(u_i', v_i') is feasible as

$$\begin{pmatrix} \Delta(u_i') & -\frac{1}{2} P_i \\ -\frac{1}{2} P_i^T & \Delta(v_i') \end{pmatrix} = \begin{pmatrix} \sqrt{\lambda} & \\ & \frac{1}{\sqrt{\lambda}} \end{pmatrix} \begin{pmatrix} \Delta(u_i) & -\frac{1}{2} P_i \\ -\frac{1}{2} P_i^T & \Delta(v_i) \end{pmatrix} \begin{pmatrix} \sqrt{\lambda} & \\ & \frac{1}{\sqrt{\lambda}} \end{pmatrix}$$

$$\succcurlyeq 0 \,. \quad \boxed{\text{S}}$$

This implies that the expression in (6) equals $\mathrm{opt}(D_{Q_1}) \cdot \mathrm{opt}(D_{Q_2})$.
This proves that $\varepsilon(G_1 \oplus G_2) \ \leq \ \varepsilon(G_1) \cdot \varepsilon(G_2)$, so that they are equal ("additivity" holds).

– The use of dual feasible solutions to bound primal optima occurs in several other works. Notably, this was used by Mochon to show bounds on the bias of weak coin flipping protocols, leading to protocols with arbitrarily small bias.