QMATH summer school on the mathematics of entanglement via nonlocal games

Thomas Vidick

Vidick – Exercise Session 1

1.1 Warm-up

Exercise 1.1.

1. Show that any non-signaling strategy that is also deterministic is classical.
2. For $\mathcal{X} = \mathcal{Y} = \mathcal{A} = \mathcal{B} = \{0,1\}$, give an example of a strategy that is non-signaling but is not classical.

Exercise 1.2.

1. Show that there is a classical strategy which succeeds in the game $\mathcal{G}_{\mathrm{CHSH}}$ with probability $3/4$.
2. Show that there is a non-signaling strategy which succeeds in $\mathcal{G}_{\mathrm{CHSH}}$ with probability 1.
3. Show that $3/4$ is best achievable for classical strategies. *[Hint: first consider classical deterministic strategies. Such a strategy is represented by* 4 *bits only.]*

Exercise 1.3. What is the smallest possible size for the question and answer sets in a game whose non-signaling value is strictly larger than its classical value? And its quantum value?

Exercise 1.4. Say that a game is *nontrivial* if all pairs of questions with $\pi(x,y) > 0$ have at least one accepting answer to them. For a nontrivial XOR game $\mathcal{G}$, show that the non-signaling bias satisfies $\beta^{ns}(\mathcal{G}) = 1$.

Exercise 1.5. Prove Naimark's dilation theorem. State and prove a version of the theorem that simultaneously "dilates" multiple POVM $\{A_{xa}\}_{a\in\mathcal{A}}$ acting on the same Hilbert space $\mathcal{H}$.

Exercise 1.6 (Odd cycle game)**.** Let n be an odd integer. In the odd cycle game of order n, we take $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_n$ and $\mathcal{A} = \mathcal{B} = \{-1,1\}$. The distribution π is uniform on $\{(i,j) \in \mathbb{Z}_n \times \mathbb{Z}_n : i \in \{t-1,t\}\}$. The game predicate is $V(i,j,a,b) = 1$ if $j = i+1$ and $ab = -1$ or $j = i$ and $ab = 1$.

1. Verify that this is an XOR game and compute its classical value.
2. Design a quantum strategy that uses a single EPR pair and succeeds with probability $\cos^2(\pi/4n)$.
3. (Harder:) Show that this is optimal.

1.2 Tirelson's bound, and theorem

Exercise 1.7. Let A_0, A_1 and B_0, B_1 be observables on $\mathbb{C}^d$. Show that

$$\begin{aligned}(A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1)^2 &= ((A_0 + A_1) \otimes B_0 + (A_0 - A_1) \otimes B_1)^2 \\ &= 4\,\mathrm{Id} \otimes \mathrm{Id} + (A_1 A_0 - A_0 A_1) \otimes (B_0 B_1 - B_1 B_0)\,.\end{aligned} \tag{1.1}$$

Deduce a new proof of Tsirelson's upper bound on the quantum bias of the CHSH game.

Exercise 1.8.

1. For any $d \geq 1$, show that there exists Hermitian matrices $C_1, \ldots, C_d \in \mathbb{C}^{D \times D}$ where $D = 2^{\lfloor d/2 \rfloor}$ such that $C_i^2 = \mathrm{Id}$ for all i, and $\{C_i, C_j\} = C_i C_j + C_j C_i = 0$ for all $i \neq j$.
2. For $u, v \in \mathbb{R}^d$ let $U = \sum_i u_i C_i$ and $V = \sum_i v_i C_i$. Give simple expressions for U^2, C^2, and $\langle \phi_D | U \otimes V | \phi_D \rangle$, where $|\phi_D\rangle$ is the maximally entangled state in dimension D.
3. Show that given a vector solution to SDP($\mathcal{G}$) it is always possible to find a quantum strategy that achieves exactly the same value. (Be careful with complex numbers!)

Exercise 1.9. Grothendieck's inequality states that there exists a universal constant $K_G^{\mathbb{R}} \in \mathbb{R}$ such that for any integer n and any $M = (M_{ij}) \in \mathbb{R}^{n \times n}$,

$$\sup_{\substack{d,\, \vec{u}_i, \vec{v}_j \in \mathbb{C}^d \\ \|\vec{u}_i\|, \|\vec{v}_j\| \leq 1}} \Big| \sum_{i,j} M_{ij}\, \vec{u}_i \cdot \vec{v}_j \Big| \;\leq\; K_G \max_{x_i, y_j \in [-1,1]} \Big| \sum_{i,j} Mij\, x_i y_j \Big|\,.$$

The constant $K_G^{\mathbb{R}}$ is known to satisfy $K_G^{\mathbb{R}} \leq 1.782\ldots$. Furthermore, if $M = (M_{ij}) \in \mathbb{C}^{n \times n}$ and supremum on the right-hand side is taken over all complex $x_i, y_j \in \mathbb{C}$ such that $|x_i|, |y_j| \leq 1$ then the inequality holds with an improved constant $K_G^{\mathbb{C}} < K_G^{\mathbb{R}}$ such that $K_G^{\mathbb{C}} \leq 1.405\ldots$.

- What is the best constant K such that $\beta^*(\mathcal{G}) \leq K\beta(\mathcal{G})$, for any XOR game $\mathcal{G}$?

Exercise 1.10. Suppose that $\mathcal{G}$ is an XOR game such that $\beta^*(\mathcal{G}) = 1$. Show that $\beta(\mathcal{G}) = 1$.

1.3 Complexity aspects

Exercise 1.11. Show that exact computation of the classical bias of an XOR game is NP-hard. (Formally, this should be made in a decision problem — for example, show that there exists a real a such that deciding if $\beta(\mathcal{G}) \geq a$ or $\beta(\mathcal{G}) < a$ is NP-hard.)

Exercise 1.12. Relate the maximum success probability in the clause-vs-variable game to the largest number of clauses of φ that can be simultaneously satisfied by any assignment. Your relation need not be perfectly tight, but it should at least imply that the maximum success probability is 1 if and only if the formula is satisfiable.

1.4 Parallel repetition of XOR games

Exercise 1.13. Given two XOR games $\mathcal{G}_1 = (\mathcal{X}_1, \mathcal{Y}_1, \mathcal{A}_1, \mathcal{B}_1, \pi_1, V_1)$ and $\mathcal{G}_2 = (\mathcal{X}_2, \mathcal{Y}_2, \mathcal{A}_2, \mathcal{B}_2, \pi_2, V_2)$ define the AND game $\mathcal{G} = \mathcal{G}_1 \wedge \mathcal{G}_2$ by setting $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_2$, $\mathcal{Y} = \mathcal{Y}_1 \times \mathcal{Y}_2$, $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2$, $\mathcal{B} = \mathcal{B}_1 \times \mathcal{B}_2$,

$$\pi((x_1, x_2), (y_1, y_2)) \;=\; \pi_1(x_1, y_1)\pi_2(x_2, y_2) \tag{1.2}$$

and

$$V((x_1,x_2),(y_1,y_2),(a_1,a_2),(b_1,b_2)) \;=\; V_1(x_1,y_1,a_1,b_1)V_2(x_2,y_2,a_2,b_2)\;.$$

In words, the game $\mathcal{G}$ corresponds to playing $\mathcal{G}_1$ and $\mathcal{G}_2$ "in parallel" by sending one pair of questions for each game and accepting if and only if both pairs of questions are answered correctly. The goal of this exercise is to study how the bias of $\mathcal{G}$ relates to that of $\mathcal{G}_1$ and $\mathcal{G}_2$.

1. Consider the following nonlocal game $\mathcal{G}_F$. In this game we have $\mathcal{X} = \mathcal{Y} = \mathcal{A} = \mathcal{B} = \{0,1\}$, π is uniform over $\{(0,0),(0,1),(1,0)\}$ and we have $V(x,y,a,b) = 1$ if $(a \vee x) \neq (b \vee y)$ and 0 otherwise.

   (a) Is $\mathcal{G}_F$ an XOR game?

   (b) Compute $\omega(\mathcal{G}_F)$.

   (c) Show that $\omega(\mathcal{G}_F \wedge \mathcal{G}_F) = \omega(\mathcal{G}_F)$.

The previous question shows that there are nonlocal games whose value does not decrease under repetition. Moreover, it is possible (but harder) to show that the quantum value of $\mathcal{G}_F$ also does not decrease under repetition.

In the remainder of the exercise we show that this does not happen for the quantum value of an XOR game $\mathcal{G}$.

2. Show that the quantum bias $\beta^*(\mathcal{G})$ can be expressed as the optimum of the following semidefinite program

$$\begin{aligned}
\beta^*(\mathcal{G}) \;=\; \max\; & \sum_{i,j} G_{ij} M_{ij} \\
s.t.\quad & X = \begin{pmatrix} R & M \\ M^\dagger & S \end{pmatrix} \geq 0 \\
& \forall i\,, R_{ii} = 1 \\
& \forall j\,, S_{jj} = 1\;.
\end{aligned}$$

3. Verify that the dual program can be expressed as

$$\begin{aligned}
\beta^*(\mathcal{G}) \;=\; \min\; & \frac{1}{2}\sum_i u_i + \frac{1}{2}\sum_j v_j \\
s.t.\quad & \begin{pmatrix} \mathrm{Diag}(u) & -G \\ -G^\dagger & \mathrm{Diag}(v) \end{pmatrix} \geq 0 \\
& u \in \mathbb{R}^n,\; v \in \mathbb{R}^m\;.
\end{aligned} \tag{1.3}$$

4. Show that for any optimal solution (u,v) to the dual, $\sum_i u_i = \sum_j v_j$.

5. For the special case of $\mathcal{G} = \mathcal{G}_{\mathrm{CHSH}}$, exhibit a dual solution that certifies $\beta^*(\mathcal{G}_{\mathrm{CHSH}}) \leq \cos^2 \pi/8$, thus providing a third proof of Tsirelson's bound.

Before analyzing the parallel repetition of two XOR games, it is convenient to study their "XOR repetition". The XOR of two XOR games $\mathcal{G}_1$ and $\mathcal{G}_2$ is the XOR game $\mathcal{G} = \mathcal{G}_1 \oplus \mathcal{G}_2$ with $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_2$, $\mathcal{Y} = \mathcal{Y}_1 \times \mathcal{Y}_2$, and if $G^{(1)}$ and $G^{(2)}$ are the game matrices of $\mathcal{G}_1$ and $\mathcal{G}_2$ respectively then the game matric of $\mathcal{G}$ is

$$G_{(x_1,y_1),(x_2,y_2)} \;=\; G^{(1)}_{x_1,y_1} G^{(2)}_{x_2,y_2}\;.$$

In other words, the game matrix for $\mathcal{G}$ is obtained by taking the tensor product of the game matrices for $\mathcal{G}_1$ and $\mathcal{G}_2$. (Make sure that you understand the difference between this definition and the definition of $\mathcal{G}_1 \wedge \mathcal{G}_2$. In particular, recall that the game predicate V is $\{0,1\}$-valued, whereas the game matrix G is real-valued.)

6. Verify that $\beta^*(\mathcal{G}_1 \oplus \mathcal{G}_1) \geq \beta^*(\mathcal{G}_1)\beta^*(\mathcal{G}_2)$.
7. We now prove the opposite inequality.
   (a) Given dual feasible solutions (u_1, v_1) and (u_2, v_2) to the dual program (1.3) for $\mathcal{G}_1$ and $\mathcal{G}_2$ respectively, show that $(u, v) = (u_1 \otimes u_2, v_1 \otimes v_2)$ is a feasible dual solution to the dual program for $\mathcal{G}$.
   (b) Deduce that $\beta^*(\mathcal{G}_1 \oplus \mathcal{G}_1) \leq \beta^*(\mathcal{G}_1)\beta^*(\mathcal{G}_2)$.
8. Show that for any XOR games $\mathcal{G}_1$ and $\mathcal{G}_2$, it holds that $\omega^*(\mathcal{G}_1 \wedge \mathcal{G}_2) = \omega^*(\mathcal{G}_1) \wedge \omega^*(\mathcal{G}_2)$.
9. Generalize this equality to the case of n XOR games.

Vidick – Exercise Session 2

Exercise 2.1. Let $Y_1, \ldots, Y_9$ be an operator solution to the Magic Square system. Show that there is an orthonormal basis with respect to which

$$\begin{array}{ccc} Y_1 = (I_2 \otimes \sigma_Z) \otimes \mathrm{Id} & Y_2 = (\sigma_Z \otimes I_2) \otimes \mathrm{Id} & Y_3 = (\sigma_Z \otimes \sigma_Z) \otimes \mathrm{Id} \\ Y_3 = (\sigma_X \otimes I_2) \otimes \mathrm{Id} & Y_4 = (I_2 \otimes \sigma_X) \otimes \mathrm{Id} & Y_5 = (\sigma_X \otimes \sigma_X) \otimes \mathrm{Id} \, , \\ Y_7 = (\sigma_X \otimes \sigma_Z) \otimes \mathrm{Id} & Y_8 = (\sigma_Z \otimes \sigma_X) \otimes \mathrm{Id} & Y_9 = (\sigma_Y \otimes \sigma_Y) \otimes \mathrm{Id} \end{array}$$

where I_2 denotes the identity on $\mathbb{C}^2$ and Id is the identity on $\mathbb{C}^d$ for some d.

Exercise 2.2. Show that the conclusion of Lemma **??** holds under the following weaker assumption: $|\psi\rangle_{\mathsf{ABE}} \in (\mathbb{C}^2)_{\mathsf{A}}^{\otimes n} \otimes \mathcal{H}_{\mathsf{B}}^{\otimes n} \otimes \mathcal{H}_{\mathsf{E}}$ with $\mathcal{H}_{\mathsf{B}}$ arbitrary, and for every $i \in \{1, \ldots, n\}$,

$$\left(\sigma_{X,i}\right)_{\mathsf{A}} \otimes \left(X_i\right)_{\mathsf{B}} |\psi\rangle_{\mathsf{ABE}} \;=\; \left(\sigma_{Z,i}\right)_{\mathsf{A}} \otimes \left(Z_i\right)_{\mathsf{B}} |\psi\rangle_{\mathsf{ABE}} \;=\; |\psi\rangle_{\mathsf{ABE}} \, ,$$

with X_i and Z_i arbitrary binary observables on $\mathcal{H}_{\mathsf{B}}$. *[Hint: Make a careful use of Claim* **??***]*

Exercise 2.3. A game is called *symmetric* if $\mathcal{X} = \mathcal{Y}$ and $\mathcal{A} = \mathcal{B}$, the distribution on questions π is invariant under permutation of the two questions, $\pi(x, y) = \pi(y, x)$ for all (x, y), and the verification predicate is symmetric as well, i.e. $V(x, y, a, b) = V(y, x, b, a)$ for all (x, y, a, b). Define a strategy $(|\psi\rangle, \{A_{xa}\}, \{B_{yb}\})$ to be *symmetric* if $\mathcal{H}_{\mathsf{A}} = \mathcal{H}_{\mathsf{B}}$, $|\psi\rangle$ is invariant under exchange of the two subsystems, and $A_{xa} = B_{xa}$ for all x, a.

Show that whenever a game $\mathcal{G}$ is symmetric then for any strategy $(|\psi\rangle, \{A_{xa}\}, \{B_{yb}\})$ that succeeds with some probability p in the game there is a symmetric strategy $(|\tilde{\psi}\rangle, \{\tilde{A}_{xa}\})$ that succeeds with the same probability.

Exercise 2.4. The *BLR linearity game* is a nonlocal game which can be described as follows:

- The referee selects $a, a' \in \mathbb{Z}_2^n$ uniformly at random. She sends (a, a') to one player and a, a', or $a + a'$ to the other player.
- The first player replies with two bits $e_1, e_2 \in \{\pm 1\}$, and the second with a single bit $f \in \{\pm 1\}$. The referee accepts if and only if the player's answers satisfy the natural relation, e.g. if the third player received $a + a'$ then it should be that $f = e_1 e_2$.

1. A classical deterministic strategy in the game can be modeled in the obvious way by three functions $f_{A,1}, f_{A,2} : (\mathbb{Z}_2^n)^2 \to \{\pm 1\}$, representing Alice's two answer bits, and $f_B : \mathbb{Z}_2^n \to \{\pm 1\}$, representing Bob's single answer bit. Show that if $(f_{A,1}, f_{A,2}, f_B)$ succeeds with probability $1 - \varepsilon$ in the game then

$$\mathrm{E}_{a,a' \in \mathbb{Z}_2^n} \left[f_B(a) f_B(a') f_B(a + a') \right] \;\geq\; 1 - O(\varepsilon) \, .$$

2. Using the Fourier expansion $f_B(a) = \sum_{S\subseteq\{1,\dots,n\}} \widehat{f_B}(S)\chi_S(a)$, where $\chi_S(a) = \prod_{i\in S} a_i$, deduce from the previous question that for any near-optimal strategy f_B must have one "large" (to be quantified as a function of ε in your answer) Fourier coefficient.

3. Conclude that successful strategies in the BLR linearity game must be close to "linear."

4. Extend the previous reasoning to quantum strategies. In particular, give a clear formulation for the statement that the BLR linearity game, as described above, is "sound against quantum strategies." *[Hint: you may find it easier to first only consider strategies that use a maximally entangled state, i.e. $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^d$ and $|\psi\rangle = |\phi_d\rangle$. For this case, extend the previous proof to "matrix-valued" functions defined from the strategy and use Fourier analysis directly at the matrix level. What is the quantum analogue of having a large Fourier coefficient? The general case is similar, but a little more technical]*