Quantum Proofs, Semester A 2024

Homework # 5 **due: 5pm, March 4th, 2024**

Ground rules:

Homework is due through Moodle. If you are having issues with this, email the instructor (thomas.vidick@weizmann.ac.il) or drop your work in my mailbox at the top of the central stairs in Ziskind. Solutions can be latexed or handwritten. In the latter case, please make sure that your handwriting is legible. Special care should be taken in writing up a precise solution. If I am not able to follow the logic in your argument, if there is a small gap or an uncovered case, you will lose points.

You are encouraged to collaborate with your classmates on homework problems, but each person must write up the final solutions individually. You should note on your homework specifically which problems were a collaborative effort and with whom. You may not search online for solutions, but if you do use research papers or other sources in your solutions, you must cite them.

Late homework will not be accepted or graded.

The first two exercises depend on the lecture from February 20th, and the last two on the lecture from February 27th. The first problem asks you to show that a single family of states can act as embezzlers for any given state, provided that the given state is not too large. The second problem is an example of a three-player XOR game; we see that, in contrast to two-player XOR-games, with three players it is possible to have perfect quantum strategies when no perfect classical strategy exists. The third exercise asks you to show Tsirelson's theorem mentioned in class. The last exercise proves a connection between two-player XOR interactive proof systems and single-player two-message interactive proofs.

Any changes since the first posting will be marked in blue.

Problem:

1. (3 points) **Universal embezzlement**

   For any integer $n \geq 1$ let

   $$|\Gamma_n\rangle \;=\; \frac{1}{\sqrt{C_n}} \sum_{j=1}^{n} \frac{1}{\sqrt{j}} |j\rangle_A |j\rangle_B \;,$$

   where C_n is the appropriate normalization constant such that $\||\Gamma_n\rangle\| = 1$. Let $|\varphi\rangle = \sum_{i=1}^{m} \alpha_i |u_i\rangle_{A'} |v_i\rangle_{B'}$ be an arbitrary (normalized) state, where $\{|u_i\rangle\}$ and $\{|v_i\rangle\}$ are

orthonormal families. Finally, let

$$|\omega_n\rangle \;=\; \Big(\sum_{i=1}^{m} \alpha_i |i\rangle_{A'}|i\rangle_{B'}\Big) \otimes |\Gamma_n\rangle_{AB} \;\in\; \mathbb{C}^{nm\times nm}\;.$$

Let $\omega_1 \geq \cdots \geq \omega_{mn}$ be the Schmidt coefficients of $|\omega_n\rangle$, ordered in non-increasing order.

(a) For fixed i and t, let N_i^t be the number of Schmidt coefficients of $|\omega_n\rangle$ of the form $\alpha_i/\sqrt{jC_n}$ that are strictly greater than $1/\sqrt{tC_n}$. Show that $N_i^t < \alpha_i^2 t$. Deduce that $\sum_{i=1}^m N_i^t < t$.

(b) Show that the n largest Schmidt coefficients of $|\omega_n\rangle$ are smaller than the corresponding ones of $|\Gamma_n\rangle$, i.e. that $\omega_j \leq 1/\sqrt{jC_n}$ for all j.

(c) Let $|\tilde{\omega}_n\rangle \in \mathbb{C}^{nm\times nm}$ have the same Schmidt coefficients as $|\omega_n\rangle$, arranged in non-increasing order. So, $|\tilde{\omega}_n\rangle = \sum_{j=1}^{nm} \omega_j |j\rangle|j\rangle$. Further, write $|\Gamma_n\rangle$ for the same state as before, but embedded in $\mathbb{C}^{nm\times nm}$ (i.e., the Schmidt coefficients are zero on vectors $|j\rangle$ for $j > n$). Deduce from the previous question that

$$\big|\langle\Gamma_n|\tilde{\omega}_n\rangle\big| \;\geq\; \sum_{j=1}^{n} \omega_j^2 \;\geq\; 1 - \frac{\log(m)}{\log(n)}\;.$$

(Both inequalities need proof.)

(d) Let $\varepsilon > 0$. Describe a protocol that, given as input the state $|\Gamma_n\rangle$ (for some $n = n(\varepsilon)$ to be determined), performs local operations on A and B only and generates a state $|\psi_n\rangle$ such that $\mathcal{F}(|\psi_n\rangle\langle\psi_n|, |\varphi\rangle\langle\varphi| \otimes |\Gamma_n\rangle\langle\Gamma_n|) \geq 1 - \varepsilon$.

(e) Deduce a lower bound, depending on $d \geq 1$, on the success probability that one can achieve in the coherent state exchange game by using an entangled state of dimension d (for each player, so d^2 in total).

2. (2 points) **Mermin's game**

"Mermin's game" is the following. Consider three space-like separated players: Alice, Bob, and Charlie. Alice receives input bit x, Bob receives input bit y, and Charlie receives input bit z. The input satisfies the promise that $x \oplus y \oplus z = 0$. The goal of the players is to output bits a, b, c, respectively, such that $a \oplus b \oplus c = OR(x, y, z)$. In other words, the outputs should sum to $0 (\mathrm{mod} 2)$ if $x = y = z = 0$, and should sum to $1 (\mathrm{mod} 2)$ if $x + y + z = 2$.

(a) Show that every classical randomized strategy has success probability at most $3/4$ under the uniform distribution on the four allowed inputs x, y, z.

(b) Suppose the players share the following entangled 3-qubit state:

$$\frac{1}{2}\big(|000\rangle - |011\rangle - |101\rangle - |110\rangle\big)\;.$$

Suppose each player does the following: if his/her input bit is 1, apply H to his/her qubit, otherwise do nothing. Describe the resulting 3-qubit superposition.

(c) Give a quantum strategy that wins the above game with probability 1 on every input that satisfies the promise.

3. (4 points) **Tsirelson's theorem**

The goal of this exercise is to show that given an XOR game G and a vector solution to $\mathsf{SDP}(G)$ it is always possible to find a quantum strategy that achieves exactly the same value. We start with some warm-ups.

(a) For $D \geq 1$ let $|\phi_D\rangle = D^{-1/2} \sum_{i=1}^{D} |i\rangle|i\rangle$. For any $D \times D$ matrices A, B, compute $\langle\phi_D|A \otimes B|\phi_D\rangle$.

(b) Suppose that A and $B^\dagger$ anticommute, i.e. $AB^\dagger = -B^\dagger A$. Show that $\mathrm{Tr} AB^\dagger = 0$.

(c) Show that for any integer $d \geq 1$ there exists a D and Hermitian matrices $C_1, \ldots, C_d \in \mathbb{C}^{D\times D}$ that square to identity and pairwise anti-commute. *[Hint: use tensor products of Pauli matrices.]*

(d) For any vector $u \in \mathbb{R}^d$, consider $u \mapsto C(u) := \sum_i u_i C_i$. What can you say about $C(u)$? Compute $\langle\phi_D|C(u) \otimes C(v)|\phi_D\rangle$.

Recall that to an XOR game G with question distribution π on $\{1, \ldots, n\} \times \{1, \ldots, m\}$ and decision predicate $V(a, b|s, t) = a \oplus b \oplus c_{st}$ we associate the semidefinite program

$$\begin{aligned} \mathsf{SDP}(G) \;=\; \sup \quad & \sum_{s,t} \pi(s,t)(-1)^{c_{st}} x_s \cdot y_t \\ s.t. \quad & x_s, y_t \in \mathbb{R}^{n+m} \;, \quad \forall\; s, t \\ & \|x_s\| \leq 1 \;, \quad \forall\; s = 1, \ldots, n \\ & \|y_t\| \leq 1 \;, \quad \forall\; t = 1, \ldots, m \;. \end{aligned}$$

(e) Show that there is a quantum strategy for G whose success bias is $\beta^*(G) = \mathsf{SDP}(G)$.

4. (4 points) **An upper bound on XOR games**

Show that for any c, s such that $0 \leq s < c \leq 1$, $\oplus\mathsf{MIP}^*_{c,s}(2) \subseteq \mathsf{QIP}_{c,s}(2)$.

[Hint: Consider the following first step for the verifier: sample $(s, t) \sim \pi$ and prepare the state $|\Phi\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle|s\rangle + |1\rangle|1\rangle|t\rangle$. Send the last two registers to the prover and ask them to write their answer as a phase.
Complete this protocol and show that it achieves the desired completeness and soundness guarantees.]

Since $\mathsf{QIP}(2) \subseteq \mathsf{QIP}(3) \subseteq \mathsf{PSPACE} \subseteq \mathsf{EXP}$, this refines the inclusion $\oplus\mathsf{MIP}^*(2) \subseteq \mathsf{EXP}$ seen in class.