Quantum Proofs, Semester A 2024

Homework # 5 Solutions **March 18th, 2024**

Please read the document and check your understanding of the answer. If you feel that your solution was correct, but I mistakenly did not award you all points, please talk to me. If my sketch is not detailed enough and you would like to see a full solution, please ask me as well.

Problem:

1. **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.)

The first inequality is easier. We have

$$\begin{aligned}\big|\langle\Gamma_n|\tilde{\omega}_n\rangle\big| &\geq \sum_{j=1}^n \omega_j \frac{1}{\sqrt{jC_n}}\\ &\geq \sum_{j=1}^n \omega_j^2\ ,\end{aligned}$$

by the previous question. For the second inequality, assume $m \leq n$ as otherwise the bound is trivial. Since $\sum_{j=1}^n \omega_j^2$ sums the n largest coefficients this sum is at least as large than the sum of *any* n squares of coefficients from ω_i. We choose $\omega_{ij} = \alpha_i/\sqrt{jC_n}$, for $i \in \{1,\dots,n\}$ and $j \in \{1,\dots,\lfloor n/m\rfloor\}$. This gives

$$\begin{aligned}\sum_{j=1}^n \omega_j^2 &\geq \sum_{i=1}^n \alpha_j^2 \sum_{j=1}^{n/m} \frac{1}{jC_n}\\ &= \frac{1}{C_n}\sum_{j=1}^{n/m}\frac{1}{j}\\ &\geq 1 - \frac{\log(m)}{\log(n)}\ ,\end{aligned}$$

where the second line uses that $|\varphi\rangle$ is normalized, and the last one is by standard comparison bounds for Harmonic series.

(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 $\mathcal{F}(|\psi_n\rangle\langle\psi_n|, |\varphi\rangle\langle\varphi| \otimes |\Gamma_n\rangle\langle\Gamma_n|) \geq 1-\varepsilon$.

For simplicity, let us make sure to choose n such that n/m is an integer. Order pairs (i,j) in decreasing order of weights $\alpha_i/\sqrt{j}$, i.e. the first pair has the largest $\alpha_i/\sqrt{j}$, etc. Locally, party A sends basis vector $|t\rangle$, for $t \in \{1,\dots,n\}$, to basis vector $|u_i\rangle|j\rangle$, where (i,j) is the t-th pair in the above ordering. (So, $|1\rangle$ is sent to $|u_i\rangle|j\rangle$ for (i,j) that has the largest $\alpha_i/\sqrt{j}$, etc.) Party B does the same, but with $|v_i\rangle$ instead of $|u_i\rangle$. Now, the reverse transformation is designed to exactly map $|\tilde{\omega}_n\rangle$ to $|\omega_n\rangle$. The conclusion then follows from part (c). Here, the fidelity is the squared overlap and so to get fidelity $1-\varepsilon$ it is enough to choose n such that $\log(n) \geq 2\log(m)/\varepsilon$, i.e. $n \geq m^{2/\varepsilon}$.

(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).

The coherent state exchange game is the game seen in class, where the players have to coherently exchange $|0\rangle|0\rangle$ for itself, and $|\phi\rangle = \frac{1}{\sqrt{2}}(|1\rangle|1\rangle + |2\rangle|2\rangle)$ for $|1\rangle|1\rangle$. To achieve this we can

i. Start with the state $|\Gamma_n\rangle$;

ii. Upon receiving a question, control on the question qubit to do the following: if the qubit is $|0\rangle$, do nothing. If it is not $|0\rangle$, then

   A. First apply the transformation from the previous question in reverse, to "erase" $|\phi\rangle$;

   B. Then apply the transformation in the forward direction, to make $|1\rangle|1\rangle$ "appear".

Using the previous question to estimate the fidelity with which the desired operation is implemented in steps ii.A and ii.B, the overall success probability will scale as $1-O(\log(m)/\log(n))$ where $n = d$ and $m = 2$, i.e. the success is $1-O(1/\log(d))$.

3. **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.]*

Let $D = 2^{\lceil d/2\rceil}$. We introduce the following matrices, for $i = 1, \ldots, \lceil d/2\rceil$, where X, Y, Z are the single-qubit Paulis:

$$\begin{aligned} C_1 &= X \otimes I \otimes \cdots \otimes I \\ C_2 &= Z \otimes I \otimes \cdots \otimes I \\ C_3 &= Y \otimes X \otimes I \otimes \cdots \otimes I \\ C_4 &= Y \otimes Z \otimes I \otimes \cdots \otimes I \\ &\vdots \qquad \vdots \\ C_{2i-1} &= Y \otimes \cdots \otimes Y \otimes X \otimes I \otimes \cdots \otimes I \\ C_{2i} &= Y \otimes \cdots \otimes Y \otimes Z \otimes I \otimes \cdots \otimes I \end{aligned}$$

Using the Pauli anti-commutation matrices, the C_j satisfy the desired constraints.

(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 $\langle\phi_D|C(u) \otimes C(v)|\phi_D\rangle$.

A simple calculation reveals that this equals $u \cdot v$, *if* $C(u) = C(u)^T$. This is not the case for the construction above. To avoid this issue can either use more dimensions to construct C_j's that do not use the Pauli Y, or replace $\langle\phi_D|C(u) \otimes C(v)|\phi_D\rangle$ in the question with $\langle\phi_D|C(u) \otimes C(v)^T|\phi_D\rangle$.

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

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

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

Everyone solved this last question correctly, by combining the previous questions and work done in class.

4. An upper bound on XOR games

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

This exercise was a little harder. First we follow the hint, which specifies the first step for the verifier. Next we need to specify the prover's actions. Let $|\psi\rangle_{AB}$ be a bipartite entangled state, and A_s and B_t observables, that constitute a strategy for the players in the original XOR game. The prover in the QIP(2) game applies the transformation[1]

$$\begin{aligned} |0\rangle|s\rangle|\psi\rangle &\mapsto |0\rangle|s\rangle A_s\otimes\mathbb{I}_B|\psi\rangle\;, \\ |0\rangle|t\rangle|\psi\rangle &\mapsto |0\rangle|s\rangle\mathbb{I}_A\otimes B_t|\psi\rangle\;. \end{aligned}$$

One can verify that this is unitary. At the last step, the verifier measures in a basis that contains the vector $|\gamma_{st}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|s\rangle + (-1)^{c_{st}}|1\rangle|1\rangle|t\rangle)$, where c_{st} is the correct parity for the answers, and accepts if and only if $|\gamma_{st}\rangle$ is obtained as outcome.

We first verify completeness, i.e. that the strategy for the prover described above has the same success probability as the two-prover strategy in the XOR game. Let

$$|\psi_{st}\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle|s\rangle(A_s\otimes\mathbb{I}_B)|\psi\rangle + |1\rangle|1\rangle|t\rangle(\mathbb{I}_A\otimes B_t)|\psi\rangle\;.$$

Then the player's success probability, conditioned on questions s,t having been sent, is

$$\begin{aligned} \langle\psi_{st}|\big(|\gamma_{st}\rangle\langle\gamma_{st}|\otimes\mathbb{I}\big)|\psi_{st}\rangle &= \frac{1}{4}\Big\|(A_s\otimes\mathbb{I}_B)|\psi\rangle + (\mathbb{I}_A\otimes B_t)|\psi\rangle\Big\|^2 \\ &= \frac{1}{2}+\frac{1}{2}\langle\psi|A_s\otimes B_t|\psi\rangle\;, \end{aligned}$$

[1] For intuition, consider that in the case of a classical strategy, the entangled state is $|\psi\rangle = (1)$ (i.e. the state is 1-dimensional, and the observables are $A_s = (-1)^{a(s)}$ and $B_t = (-1)^{b(t)}$, where $a(s), b(t)\in\{0,1\}$ are the answers that the classical prover would have sent back to question s,t respectively.

which is exactly the two players' success probability in the XOR game, conditioned on questions s, t having been sent.

We now give the idea for showing soundness. For this, we need to model the actions of an arbitrary prover in the QIP(2) protocol. Such a prover starts in an ancilla state $|0\rangle_{anc}$ and applies a unitary U on the 2-qubit question register & the ancilla register. Let $|x_s\rangle = (\langle 0|\langle s| \otimes \mathbb{I})U(|0\rangle|s\rangle|0\rangle_{anc})$. Note that $|x_s\rangle$ is a sub-normalized quantum state, of dimension the dimension of the ancilla register. Similarly, let $|y_t\rangle = (\langle 1|\langle t| \otimes \mathbb{I})U(|0\rangle|s\rangle|0\rangle_{anc})$. Let

$$|\psi'_{st}\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle|s\rangle + |1\rangle|1\rangle|t\rangle\big)|0\rangle_{anc} \ .$$

Then, the prover's success probability is

$$\begin{aligned}\langle\psi|U^\dagger\big(|\gamma_{st}\rangle\langle\gamma_{st}| \otimes \mathbb{I}\big)U|\psi\rangle &= \frac{1}{4}\big\||x_s\rangle + |y_t\rangle\big\|^2 \\ &\leq \frac{1}{2} + \frac{1}{2}\Re\big(\langle x_s|y_t\rangle\big) \ .\end{aligned}$$

Here, the first equality requires a bit of spelling things out, and we omitted details. The last line is an inequality because $\||x_s\rangle\|, \||y_t\rangle\| \leq 1$. Using the preceding calculation, it is then straightforward to show that the provers' maximum success probability cannot exceed the SDP value of the XOR game. As shown in the previous exercise, the SDP value is the same as the quantum value; which concludes the soundness proof.