Assignment 5
Due date: 11:59pm, December 6, 2022

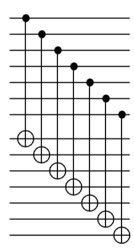
1. **Operations that are transversal for the Steane code [15 points; 5 each].** This question is about properties of the 7-qubit Steane code (which is the example code that is explained in section 3.3 of the notes *Quantum Information Theory, part II*).

   The Steane code has a nice property: that certain gates are *transversal* for it. To understand what transversal means, suppose that we have a 7-qubit state of the form $\alpha_0|0\rangle_L + \alpha_1|1\rangle_L$ (which is the encoding of the qubit state $\alpha_0|0\rangle + \alpha_1|1\rangle$). Now suppose that we want to convert this into an encoding of the qubit state $H(\alpha_0|0\rangle + \alpha_1|1\rangle)$, where H is the Hadamard transform. The most obvious way of doing this is to: first decode the 7-qubit encoding to recover the data $\alpha_0|0\rangle + \alpha_1|1\rangle$; then modify the qubit by applying H to it; and then encode the modified qubit back into a 7-qubit codeword. For the Steane code, we can bypass all this and simply apply $H^{\otimes 7}$ directly to the encoding; the net result is the same.

   The following are the main steps in the proofs that H and some other gates are transversal for the Steane code.

   (a) Prove that, for all $a \in \{0,1\}$, it holds that $H^{\otimes 7}|a\rangle_L = \frac{1}{\sqrt{2}}|0\rangle_L + (-1)^a \frac{1}{\sqrt{2}}|1\rangle_L$. (This implies that H is transversal for the Steane code.)

   (b) Prove that, for all $a, b \in \{0,1\}$, it holds that $\text{CNOT}^{\otimes 7}|a\rangle_L|b\rangle_L = |a\rangle_L|b \oplus a\rangle_L$, where by $\text{CNOT}^{\otimes 7}$ we mean apply a CNOT to the k-th bits of the respective encodings, for $k = 1,2,3,4,5,6,7$, as illustrated by the following circuit diagram.



   (This implies that CNOT is transversal for the Steane code.)

   (c) Let $S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$. Prove that, for all $a \in \{0,1\}$, it holds that $(S^*)^{\otimes 7}|a\rangle_L = i^a|a\rangle_L$. (This implies that S is essentially transversal for the Steane code.)

2. **Optimality of the CHSH inequality violation [15 points].** We saw that, for the CHSH game, there is an entangled strategy that succeeds with probability $(1 + \frac{1}{\sqrt{2}})/2 \approx 0.853$, whereas any classical strategy succeeds with probability at most $3/4$. The entangled strategy uses one Bell state. Is there another strategy for the CHSH game (possibly using more entanglement than one Bell state) that achieves a higher success probability than $(1 + \frac{1}{\sqrt{2}})/2$? The answer is no, and we will prove this here.

   CONTINUED ON NEXT PAGE

Consider a strategy that employs the entangled pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A$ and $\mathcal{H}_B$ are Alice and Bob's local Hilbert spaces. Let A_0, A_1 be Alice's binary observables for her two respective inputs, and let B_0, B_1 be Bob's binary observables for his respective inputs. (Recall that binary observables are Hermitian matrices with eigenvalues in $\{+1, -1\}$.) If the inputs $s, t \in \{0, 1\}$ to Alice and Bob are chosen uniformly then the expected value of the outcome of observable $(-1)^{st} A_s B_t$ is given by

$$\langle\psi|\big(\tfrac{1}{4}A_0 \otimes B_0 + \tfrac{1}{4}A_0 \otimes B_1 + \tfrac{1}{4}A_1 \otimes B_0 - \tfrac{1}{4}A_1 \otimes B_1\big)|\psi\rangle. \quad (1)$$

We will show that the quantity in Eq. (1) is $\leq \frac{1}{\sqrt{2}}$ (which implies the success probability is $\leq (1 + \frac{1}{\sqrt{2}})/2$). It's straightforward to show that the quantity in Eq. (1) is bounded above by $\frac{1}{4}$ times the largest eigenvalue of $M = A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1$.

(a) [10 points] Prove that, for any binary observables A_0, A_1, B_0, B_1, the largest eigenvalue of M^2 is ≤ 8. (Hint: for binary observables, $A_0^2 = A_1^2 = B_0^2 = B_1^2 = I$.)

(b) [5] Explain why the result in part (a) implies that $\frac{1}{4}$ times the largest eigenvalue of M is upper bounded by $\frac{1}{\sqrt{2}}$.

3. **Searching when the fraction of marked items is** $1/4$ **[15 points].** Suppose that $f : \{0,1\}^n \to \{0,1\}$ has the property that, for exactly $\frac{1}{4}2^n$ of the values of $x \in \{0,1\}^n$, $f(x) = 1$. Let the goal be to find such an $x \in \{0,1\}^n$ such $f(x) = 1$. Note that there's a simple classical algorithm that finds such an x with high probability with few queries (because a random query succeeds with probability $1/4$). What if we want to solve this problem *exactly* (i.e., with error probability 0)?

   (a) [5 points] Show that, for any classical algorithm, the number of f-queries required to solve this problem exactly is exponential in n.

   (b) [10] Show that there is a quantum algorithm that makes one single f-query and is guaranteed to find an $x \in \{0,1\}^n$ such $f(x) = 1$. (Hint: consider what a single iteration of Grover's algorithm does.)

4. **A distinguishing problem for BB84 states [15 points].** Suppose that a uniformly random $b \in \{0,1\}$ is "encrypted" as the mixed state

$$\begin{cases} |b\rangle & \text{with probability } \frac{1}{2} \\ H|b\rangle & \text{with probability } \frac{1}{2} \end{cases} \quad (2)$$

and you receive the encrypted state (but no other information). Your goal is to guess what b is with the highest possible success probability. Give an optimal distinguishing procedure, including a statement of its success probability, and a proof that it is optimal.

5. **(This is an optional question for bonus credit)**
Searching when the fraction of marked items is $1/2$**? [6 points].** This is the same as question 3, part (b), but with the assumption that f has the property that, for exactly $\frac{1}{2}2^n$ of the values of $x \in \{0,1\}^n$, $f(x) = 1$. Can the x still be found exactly with one f-query? Either give a quantum algorithm that solves this problem with a single f-query or prove that none exists.