Assignment 6

Due: 11:59pm, November 29, 2024

1. **A key result that's used in the construction of CSS codes [15 points].**
   Let $\mathcal{C}$ be any linear subspace of $\{0,1\}^m$ of dimension n (as a vector space over $\mathbb{Z}_2$). Define the *dual* of $\mathcal{C}$ as $\mathcal{C}^\perp = \{x \in \{0,1\}^m : \text{such that } x \cdot y = 0 \text{ for all } y \in \mathcal{C}\}$, where $x \cdot y = x_1 y_1 + \cdots + x_m y_m \bmod 2$. It is straightforward to prove that the dimension of $\mathcal{C}^\perp$ is $m - n$, and you can assume that here without proof.

   Prove that $H^{\otimes m}\Big(\frac{1}{\sqrt{2^n}} \sum_{x \in \mathcal{C}} |x\rangle\Big) = \frac{1}{\sqrt{2^{m-n}}} \sum_{y \in \mathcal{C}^\perp} |y\rangle.$

   Hint: This can be calculated directly by expanding the definition of $H^{\otimes m}$. If you are stuck then an alternative approach is to use the fact that there exists an $n \times m$ generator matrix G for $\mathcal{C}$ such that $\mathcal{C} = \{zG : z \in \{0,1\}^n\}$.

2. **Correcting errors at known positions [15 points].**
   Here we consider a method of encoding a 2-qubit state as a 4-qubit state that protects against a 1-qubit *erasure* error. An erasure error means that one qubit goes missing, and where we know *which* qubit goes missing. The code is based on these four logical states

$$
\begin{aligned}
|00\rangle_L &= \tfrac{1}{\sqrt{2}}|0000\rangle + \tfrac{1}{\sqrt{2}}|1111\rangle \\
|01\rangle_L &= \tfrac{1}{\sqrt{2}}|0101\rangle + \tfrac{1}{\sqrt{2}}|1010\rangle \\
|10\rangle_L &= \tfrac{1}{\sqrt{2}}|1001\rangle + \tfrac{1}{\sqrt{2}}|0110\rangle \\
|11\rangle_L &= \tfrac{1}{\sqrt{2}}|1100\rangle + \tfrac{1}{\sqrt{2}}|0011\rangle.
\end{aligned}
$$

   For any 2-qubit pure state $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, its encoding is the 4-qubit state $\alpha_{00}|00\rangle_L + \alpha_{01}|01\rangle_L + \alpha_{10}|10\rangle_L + \alpha_{11}|11\rangle_L$.

   The claim is that if any one of the four qubits of the encoding goes missing—and we know which qubit is missing—then the 2-qubit data can be recovered from the three remaining qubits. Here we consider the special case where the *last* qubit is missing.

   Draw a 4-qubit quantum circuit *with gates acting only on the first three qubits* that maps any encoding $\alpha_{00}|00\rangle_L + \alpha_{01}|01\rangle_L + \alpha_{10}|10\rangle_L + \alpha_{11}|11\rangle_L$ to the state

$$
\big(\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle\big) \otimes \big(\tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|11\rangle\big).
$$

   This can be done with only four CNOT gates (and no other gates); please only use CNOT gates. The existence of such a circuit implies that the 2-qubit data can be recovered from only the first three qubits of the encoding.

   (What about then other three cases, where a different qubit goes missing? By the symmetries of the encoding, those cases are very similar to the case above, and you are not asked to show the circuits for those cases.)

3. **GHZ game with different initial state [15 points; 5 each].**
Recall the GHZ game (section 9.2 of the lecture notes on *Quantum information theory* and video lecture 20). In that game, three physically separated players, Alice, Bob, and Carol, receive inputs bits r, s, t (respectively) such that $r \oplus s \oplus t = 0$. From this—and without communicating—they must produce output bits a, b, c (respectively) such that $a \oplus b \oplus c = r \vee s \vee t$. We saw that this was possible if they possess qubits whose joint state is of the form $\frac{1}{2}|000\rangle - \frac{1}{2}|011\rangle - \frac{1}{2}|101\rangle - \frac{1}{2}|110\rangle$.

   (a) What if the joint state is changed to $\frac{1}{2}|000\rangle + \frac{1}{2}|011\rangle + \frac{1}{2}|101\rangle + \frac{1}{2}|110\rangle$? Either show how they can succeed at the GHZ game using this state, or explain why they cannot.

   (b) What if the joint state is changed to $\frac{1}{2}|000\rangle + \frac{1}{2}|001\rangle + \frac{1}{2}|010\rangle + \frac{1}{2}|011\rangle$? Either show how they can succeed at the GHZ game using this state, or explain why they cannot.

   (c) What if the joint state is changed to $\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$? Either show how they can succeed at the GHZ game using this state, or explain why they cannot.

4. **A nonlocal game [15 points].**
Consider the nonlocal game where Alice and Bob are physically separated and their goal is to produce outputs that satisfy the winning conditions explained below. Alice receives a trit $s \in \{0, 1, 2\}$ (randomly sampled by the uniform distribution), and Bob receives a trit $t \in \{s, s + 1 \bmod 3\}$ (randomly sampled according to the uniform distribution on $\{s, s + 1 \bmod 3\}$). They each output a bit, a for Alice and b for Bob.

   The winning condition is: $a \oplus b = 1$, in the case where $(s, t) = (2, 0)$; and $a \oplus b =\ 0$ in the other five cases.

   To summarize the game, there are six possible instances of the inputs (s, t), which each arise with probability 1/6. They are listed in the following table, along with the corresponding winning condition.

$s\ t$	$a \oplus b$
0 0	0
0 1	0
1 1	0
1 2	0
2 2	0
2 0	1

   (a) [5 points] Show that any classical strategy for this game succeeds with probability $\leq 5/6 \approx 0.833$. (You can just show it for classical *deterministic* strategies, even though the same bound also applies to classical probabilistic strategies.)

   (b) [10] Show that there is a quantum strategy (using entanglement) that succeeds with probability $\cos^2(\pi/12) \approx 0.933$.

   Hint: Recall that the entangled strategy for the CHSH game can be expressed as starting with the state $\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$ and Alice and Bob each perform a rotation depending on their respective inputs s and t. Consider a variant of this with different rotation angles.