Assignment 9

Due date: 11:59pm, November 26 (Thursday), 2020

1. **An error-correcting encoding of a qubit into three qutrits [15 points; 3 each].** Consider the following encoding of a qubit into three qu*trits* (where the computational basis states for a qutrit are $|0\rangle$, $|1\rangle$, $|2\rangle$). The data qubit in state $\alpha_0|0\rangle + \alpha_1|1\rangle$ is mapped to the three qutrit *encoded state*

$$\frac{\alpha_0}{\sqrt{3}}\big(|000\rangle + |111\rangle + |222\rangle\big) + \frac{\alpha_1}{\sqrt{6}}\big(|012\rangle + |021\rangle + |102\rangle + |120\rangle + |201\rangle + |210\rangle\big). \quad (1)$$

We will show that this code can handle the following type of calamity: one of the three qutrits goes missing (where we do not know which one) *and* the remaining two qutrits are given to us in an arbitrary order. So what we're left with is two qutrits, but we have no idea whether they're the first two, the last two, or the first and the last (and they may be out of order). The following steps will help guide you to a method for decoding:

(a) Consider the following linear operator M acting on two-qutrit states. For all $a, b \in \{0,1,2\}$, $M|a,b\rangle = |2a+b \bmod 3, a+b \bmod 3\rangle$. Show that this M is unitary.

(b) Show that, if M is applied to the first two qutrits of the above encoded state (Eq. (1)) then it is transformed to the state

$$\big(\alpha_0|0\rangle + \tfrac{1}{\sqrt{2}}\alpha_1(|1\rangle + |2\rangle)\big) \otimes \tfrac{1}{\sqrt{3}}(|00\rangle + |12\rangle + |21\rangle). \quad (2)$$

(c) Assume the results in part (a) and (b) are true, and show how to recover the data qubit from just the first two qutrits of the encoded state (in Eq. (1)).

(d) Assume a solution to part (c) and show how to recover the qubit from the state of *any* two of the qutrits in a manner that does not require us to know which two qutrits they are (or in what order they are given). (Hint: symmetry!)

(e) Now, suppose that you are in possession of only the first qutrit of the encoding in Eq. (1). Prove that absolutely no information about the original qubit can be deduced from this.

2. **A key result that's used in the construction of CSS codes [15 points].** Let C be any linear subspace of $\{0,1\}^n$ (as a vector space over $\mathbb{Z}_2$). Define the dual of C as $C^\perp = \{x \in \{0,1\}^n : \text{such that } x \cdot y = 0 \text{ for all } y \in C\}$, where $x \cdot y = x_1y_1 + \cdots + x_ny_n \bmod 2$.

(a) Prove that $H^{\otimes n}\left(\dfrac{1}{\sqrt{|C|}}\displaystyle\sum_{x\in C}|x\rangle\right) = \dfrac{1}{\sqrt{|C^\perp|}}\displaystyle\sum_{y\in C^\perp}|y\rangle.$

(b) Prove that, for any $w \in \{0,1\}^n$, $H^{\otimes n}\left(\dfrac{1}{\sqrt{|C|}}\displaystyle\sum_{x\in C}|x+w\rangle\right) = \dfrac{1}{\sqrt{|C^\perp|}}\displaystyle\sum_{y\in C^\perp}(-1)^{y\cdot w}|y\rangle.$

Since part (b) subsumes part (a), a correct solution to (b) alone is worth 15 points. The purpose of part (a) is as a warm-up to part (b). (Just doing part (a) is worth 8 points.)