Quantum Information Processing Assignment 9

Name: Nate Stemen (20906566)
Email: nate.stemen@uwaterloo.ca

Due: Thurs, Nov 26, 2020 11:59 PM
Course: QIC 710

I worked with Chelsea Komlo and Wilson Wu on this assignment.

Problem 1

An error-correcting encoding of a qubit into three qutrits.

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

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

$$\left(\alpha_0 |0\rangle + \frac{\alpha_1}{\sqrt{2}}(|1\rangle + |2\rangle)\right) \otimes \frac{1}{\sqrt{3}}(|00\rangle + |12\rangle + |21\rangle)$$

(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.

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

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

Solution. (a) In order to show that M is unitary, we want to show that $MM^\dagger = \mathbb{1}$. We can do this by taking two arbitrary vectors $|a, b\rangle$ and $|c, d\rangle$, applying M to them, and taking their inner product. *If* we can show this equals the inner product of the two vectors themselves, then we've shown M is unitary. First recall $\langle a, b|c, d\rangle = \delta_{ac}\delta_{bd}$. Thus when we write

$$\langle a, b| M^\dagger M |c, d\rangle = \langle 2a + b \mod 3, a + b \mod 3|2c + d \mod 3, c + d \mod 3\rangle$$

we can see this will only be 1 when $2a + b = 2c + d \pmod 3$ *and* $a + b = c + d$ (again, mod 3). Subtracting the second equation from the first we see then that $a = c$, which then implies $b = d$. In all other cases the expression will be 0, and hence equivalent to $\delta_{ac}\delta_{bd}$. Thus we've shown $\langle a, b| M^\dagger M |c, d\rangle = \langle a, b|c, d\rangle$, and hence M is unitary.

(b) Here we will apply $M \otimes \mathbb{1}$ onto the encoded state and then do some algebra.

$$\begin{aligned}
M \otimes \mathbb{1} \Bigg[& \frac{\alpha_0}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle) \\
& + \frac{\alpha_1}{\sqrt{6}}(|012\rangle + |021\rangle + |102\rangle + |120\rangle + |201\rangle + |210\rangle)\Bigg] \\
= & \frac{\alpha_0}{\sqrt{3}}(|000\rangle + |021\rangle + |012\rangle) \\
& + \frac{\alpha_1}{\sqrt{6}}(|112\rangle + |221\rangle + |212\rangle + |100\rangle + |121\rangle + |200\rangle) \\
= & \frac{\alpha_0}{\sqrt{3}}|0\rangle \otimes [|00\rangle + |21\rangle + |12\rangle] \\
& + \frac{\alpha_1}{\sqrt{6}}|1\rangle \otimes [|12\rangle + |00\rangle + |21\rangle] \\
& + \frac{\alpha_1}{\sqrt{6}}|2\rangle \otimes [|21\rangle + |12\rangle + |00\rangle] \\
= & \left(\alpha_0|0\rangle + \frac{\alpha_1}{\sqrt{2}}(|1\rangle + |2\rangle)\right) \otimes \frac{1}{\sqrt{3}}(|00\rangle + |12\rangle + |21\rangle)
\end{aligned}$$

(c) To begin, apply M as defined above to the first two qutrits, and throw away the second qubit. Then apply a transformation that does the following basis change on the first qubit:

$$\begin{aligned}
|0\rangle &\longmapsto |0\rangle \\
\frac{1}{\sqrt{2}}(|1\rangle + |2\rangle) &\longmapsto |1\rangle \\
\frac{1}{\sqrt{2}}(|1\rangle - |2\rangle) &\longmapsto |2\rangle
\end{aligned}$$

This can be seen to be a unitary operation by a previous homework exercise we showed changes of bases are indeed unitary operations. This unitary will take our first qubit to $\alpha_0|0\rangle + \alpha_1|1\rangle$ as desired.

(d) Here we use the fact that the encoded state is invariant under permutations of the qutrits. That is when swapping any two qutrits, the encoded state remains the same. So, if the first qutrit goes missing, we can permute it to the last qutrits position and run through the procedure we outlined above.

(e) What I would like to do here is "simply" trace out the second two qutrits for the above encoded state, and I would expect that to yield a qutrit that is a uniform superposition of $|0\rangle$, $|1\rangle$ and $|2\rangle$, or something similar, but I don't know how to do this. ☹

Problem 2

A key result that's used in the construction of CSS codes.

Solution. We'll first show part (a) for good measure. We'll make use of the fact that the n-fold tensor product of the Hadamard gate on an arbitrary state $|a\rangle$ where $a \in \{0,1\}^n =: \mathbb{B}^n$ is given by

$$H^{\otimes n}|a\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{B}^n} (-1)^{a \cdot x} |x\rangle .$$

Let's now apply this to our equally weighted superposition over C.

$$\begin{aligned}
H^{\otimes n}\left(\frac{1}{\sqrt{|C|}} \sum_{x \in C} |x\rangle\right) &= \frac{1}{\sqrt{|C|}} \sum_{x \in C} \frac{1}{\sqrt{2^n}} \sum_{y \in \mathbb{B}^n} (-1)^{x \cdot y} |y\rangle \\
&= \frac{1}{\sqrt{2^n |C|}} \sum_{\substack{x \in C \\ y \in \mathbb{B}^n}} (-1)^{x \cdot y} |y\rangle \\
&= \frac{1}{\sqrt{2^n |C|}} \left[|C| \sum_{y \in C^\perp} |y\rangle + \sum_{\substack{x \in C \\ y \notin C^\perp}} (-1)^{x \cdot y} |y\rangle \right] \\
&= \sqrt{\frac{|C|}{2^n}} \sum_{y \in C^\perp} |y\rangle \qquad \text{(using } \textstyle\sum_{x \in C} (-1)^{x \cdot y} = 0 \text{ if } y \notin C^\perp\text{)} \\
&= \frac{1}{\sqrt{|C^\perp|}} \sum_{y \in C^\perp} |y\rangle
\end{aligned}$$

Where in the last line we've used the fact that $|C||C^\perp| = 2^n$. Now to do part (b) we will replace most instances of x with $x + w$. Let's go through it again (leaving out a few steps though).

$$\begin{aligned}
H^{\otimes n}\left(\frac{1}{\sqrt{|C|}} \sum_{x \in C} |x + w\rangle\right) &= \frac{1}{\sqrt{2^n |C|}} \sum_{\substack{x \in C \\ y \in \mathbb{B}^n}} (-1)^{x \cdot y} (-1)^{w \cdot y} |y\rangle \\
&= \frac{1}{\sqrt{2^n |C|}} \left[|C| \sum_{y \in C^\perp} (-1)^{w \cdot y} |y\rangle + \sum_{\substack{x \in C \\ y \notin C^\perp}} (-1)^{(x+w) \cdot y} |y\rangle \right] \\
&= \sqrt{\frac{|C|}{2^n}} \sum_{y \in C^\perp} (-1)^{w \cdot y} |y\rangle \\
&= \frac{1}{\sqrt{|C^\perp|}} \sum_{y \in C^\perp} (-1)^{w \cdot y} |y\rangle
\end{aligned}$$

Where again the second term drops out for the same reason as above. To make this a little clearer, split the exponent $(-1)^{(x+w)\cdot y} = (-1)^{x \cdot y}(-1)^{w \cdot y}$ and notice for each x, the second term is constant, and hence still goes to zero when $y \notin C$.