Advanced Topics in Quantum Information Theory
Solution 3

FS 2012
Prof. M. Christandl
Prof. A. Imamoglu
Prof. R. Renner

Exercise 3.1 The Shor code and Stabilizers

We have seen in the previous exercise that the Shor code is useful for encoding a single qubit in 9 qubits. Now we will look at the Shor code in the stabilizer picture. The generators for stabilizer group for the Shor code has elements

$$
\begin{array}{c|c}
g_1 & Z_1Z_2 \\
g_2 & Z_2Z_3 \\
g_3 & Z_4Z_5 \\
g_4 & Z_5Z_6 \\
g_5 & Z_7Z_8 \\
g_6 & Z_8Z_9 \\
g_7 & X_1X_2X_3X_4X_5X_6 \\
g_8 & X_4X_5X_6X_7X_8X_9 \\
\bar{Z} & X^{\otimes 9} \\
\bar{X} & Z^{\otimes 9}
\end{array},
$$

where we also define two Pauli group elements (that are not generators) $\bar{Z}$ and $\bar{X}$.

a.) *Show that the generators stabilize the codewords*

$$|0_L\rangle = \frac{1}{2\sqrt{2}}\left(|000\rangle + |111\rangle\right) \otimes \left(|000\rangle + |111\rangle\right) \otimes \left(|000\rangle + |111\rangle\right)$$
$$|1_L\rangle = \frac{1}{2\sqrt{2}}\left(|000\rangle - |111\rangle\right) \otimes \left(|000\rangle - |111\rangle\right) \otimes \left(|000\rangle - |111\rangle\right).$$

To show that the generators stabilize the codewords, we want to show that $g_i|b_L\rangle = |b_L\rangle$ where $i \in \{1, \dots, 8\}$ and $b \in \{0, 1\}$. This is straightforward to show directly from the definitions of the logical bits and the generators.

b.) *Show that the operators $\bar{Z}$ and $\bar{X}$ act as logical Z and X operators on the logical bits $|0_L\rangle$ and $|1_L\rangle$. Show that $\bar{Z}$ and $\bar{X}$ are independent of and commute with the generators of the Shor code. Also show that $\bar{Z}$ and $\bar{X}$ anti-commute.*

$\bar{Z}$ flips all the $|0\rangle$'s into $|1\rangle$'s and vice-versa, so clearly $|0_L\rangle$ remains unchanged by the action of this operator. For $|1_L\rangle$ there are three minus signs from each of the three blocks (qubits 123, 456, and 789), so there is a global phase of -1. This means $\bar{Z}$ acts as a logical Z operator.

$\bar{X}$ leaves all $|0\rangle$'s alone, and applies a -1 phase to each $|1\rangle$. For $|0_L\rangle$ each block gets three -1 phases on the $|111\rangle$ terms, which results in a global state of $|1_L\rangle$. The same occurs with $|1_L\rangle$, and so the resulting state is $|0_L\rangle$. This means that $\bar{X}$ is a logical X operator.

$\bar{Z}$ is clearly independent of the generators, since only g_7 and g_8 could be combined to get X operators on individual qubits and g_7, g_8, and $g_7 g_8$ are independent of $\bar{Z}$. Similarly for $\bar{X}$ only $g_1, g_2, g_3, g_4, g_5, g_6$ can be combined to produce Z operators on each qubit. For the first block we would need $Z_1 \otimes Z_2 \otimes Z_3$. Only g_1 and g_2 affect this block, and none of g_1, g_2 or $g_1 g_2$ produce Z operators on all three qubits. Therefore $\bar{X}$ is independent of the generators of the group.

It is straightforward to show that $\bar{Z}$ and $\bar{X}$ commute with each generator. Due to symmetry, we only need to check that $[g_1, \bar{X}]$, $[g_1, \bar{Z}]$, $[g_7, \bar{X}]$, and $[g_7, \bar{Z}]$ are all zero.

$$\begin{aligned}
[g_1, \bar{X}] &= \mathbb{1}_1 \otimes \mathbb{1}_2 \otimes Z^{\otimes 7} - \mathbb{1}_1 \otimes \mathbb{1}_2 \otimes Z^{\otimes 7} = 0 \\
[g_1, \bar{Z}] &= -Y_1 \otimes Y_2 \otimes X^{\otimes 7} + Y_1 \otimes Y_2 \otimes X^{\otimes 7} = 0 \\
[g_7, \bar{X}] &= -Y^{\otimes 6} \otimes Z^{\otimes 3} + Y^{\otimes 6} \otimes Z^{\otimes 3} = 0 \\
[g_7, \bar{Z}] &= \mathbb{1}^{\otimes 6} \otimes Z^{\otimes 3} - \mathbb{1}^{\otimes 6} \otimes Z^{\otimes 3} = 0,
\end{aligned}$$

where we use the fact that $XZ \otimes XZ = ZX \otimes ZX = -Y \otimes Y$.

To show that $\bar{X}$ and $\bar{Z}$ anti-commute:

$$\{\bar{X}, \bar{Z}\} = iY^{\otimes 9} - iY^{\otimes 9} = 0, \tag{1}$$

where we use the fact that $ZX = iY$ and $XZ = -iY$.

c.) *Prove that any error X_i, Z_i, and $X_i Z_i$ can be corrected by the Shor Code, where the position of the error, i, is arbitrary.*

To prove an error can be corrected, we just need to show that any combination of errors anti-commutes with at least one generator. The set of errors is $\{\mathbb{1}, X_i, Z_i, X_i Z_i\}$, and so the set of combinations is $\{X_i, Z_i, X_i Z_i, X_i Z_j, X_i X_j Z_j, Z_i X_j Z_j\}$ $(i \neq j)$. The list of combinations with the generators they anti-commute with are:

$$\begin{aligned}
X_1 : &\quad g_1 \\
X_2 : &\quad g_1, g_2 \\
X_3 : &\quad g_2 \\
X_4 : &\quad g_3 \\
X_5 : &\quad g_3, g_4 \\
X_6 : &\quad g_4 \\
X_7 : &\quad g_5 \\
X_8 : &\quad g_5, g_6 \\
X_9 : &\quad g_6 \\
Z_1, Z_2, Z_3 : &\quad g_7 \\
Z_4, Z_5, Z_6 : &\quad g_7, g_8 \\
Z_7, Z_8, Z_9 : &\quad g_8 \\
X_i Z_i : &\quad \text{combination of } X_i \text{ and } Z_i \text{ a-c generators} \\
X_i X_j Z_j : &\quad \text{at least a-c with same generators as } Z_j \\
Z_i X_j Z_j : &\quad \text{at least a-c with same generators as } X_j.
\end{aligned}$$

d.) *Prove that two qubit errors of the form X_iX_j can also be corrected, but Z_iZ_j errors cannot ($i \neq j$).*

Now the set of errors is $\{\mathbb{1}, X_i, Z_i, X_iZ_i, X_iX_j\}$ ($i \neq j$). Therefore the set of combinations of errors is $\{X_i, Z_i, X_iZ_i, X_iZ_j, X_iX_jZ_j, Z_iX_jZ_j, X_iX_jX_k\}$ ($i \neq j \neq k$). This is the same as in part (c), but now we have the combinations $X_iX_jX_k$. These terms anti-commute with $g_1, ..., g_6$ if i, j, k are in at least two different blocks. If they are all in the same block, then they commute with all generators. This means that the syndrome of X_i is the same as X_jX_k in this case. Note that the correction procedure for X_i is to apply a X_i operation. This means that if the error was instead X_jX_k then applying X_i does three X operations in a block, which results in a global phase, but the same initial state, so the error is corrected! This means that X_iX_j errors can also be corrected, even though not all error combinations anti-commute with at least one generator.

If we want to also correct Z_iZ_j errors then the set of errors is now $\{\mathbb{1}, X_i, Z_i, X_iZ_i, X_iX_j, Z_iZ_j\}$, and the set of combinations becomes

$$\{X_i, Z_i, X_iZ_i, X_iZ_j, X_iX_jZ_j, Z_iX_jZ_j, X_iX_jX_k,$$
$$Z_iZ_j, X_iZ_jZ_k, Z_iZ_jZ_k, X_iZ_iZ_jZ_k, X_iX_jZ_iZ_j, X_iX_jZ_jZ_k\} \quad (i \neq j \neq k).$$

If we consider the combination of errors $Z_1Z_4Z_7$, which can be the combination of the errors Z_1 and Z_4Z_7. This combination commutes with all the generators, so the syndromes for these errors are the same. The correction of Z_1 is to apply a $Z_1Z_2Z_3$ operation. This does not correct the Z_4Z_7 error, and so Z_iZ_j errors cannot be corrected.