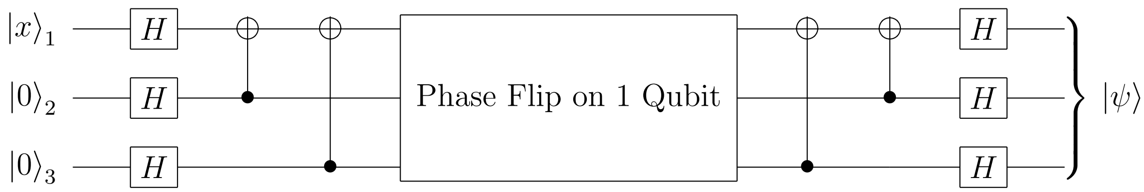
2.111J/18.435J Quantum Computation Problem Set 8 Solutions
(Due: Tuesday, December 6, 2005)

1) Verify that the following circuit is the appropriate encoder/decoder circuit for the 3 qubit phase flip code.



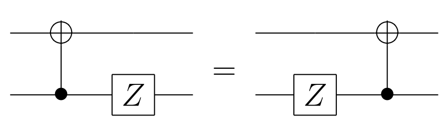
In other words, exhibit a measurement on the two ancillae in the circuit's output $|\psi\rangle$ that will detect whether a phase flip error occurred and locate the phase flip if it did occur. Then, exhibit an operation based on the above measurement that will correct the phase flip.

Solution:

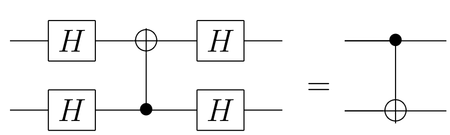
We shall demonstrate how to calculate this circuit's output without ever resorting long matrix multiplications. That is, we shall show how to calculate almost entirely by inspection the following table.

Phase Flip on	Circuit Output $\|\psi\rangle$
No qubits	$\|x\rangle_1 \otimes \|0\rangle_2 \otimes \|0\rangle_3$
3rd qubit	$\|x\rangle_1 \otimes \|0\rangle_2 \otimes \|1\rangle_3$
2nd qubit	$\|x\rangle_1 \otimes \|1\rangle_2 \otimes \|0\rangle_3$
1st qubit	$\|x \oplus 1\rangle_1 \otimes \|1\rangle_2 \otimes \|1\rangle_3$

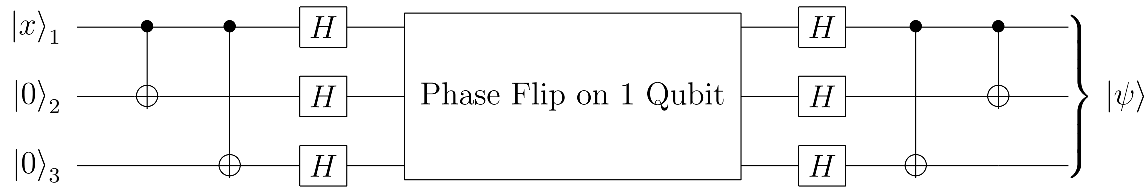
The key to this feat is to capitalize on the fact that the decoding circuit is the inverse of the encoding circuit. This fact by itself proves the first row of the above table. We can immediately prove the second and third rows of the above table by using the fact that phase flips (which are Pauli Z gates) commute with the control bits of CNOTs,



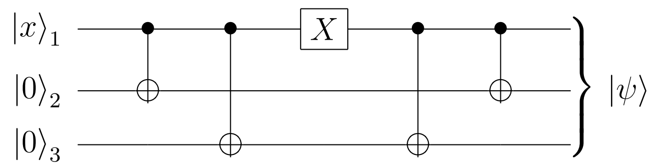
and the fact $HZH = X$. Finally, we prove the final row of the above table by using the circuit identity



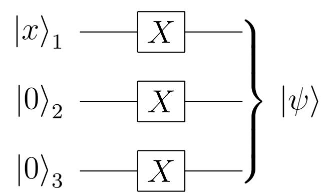
and the fact $H^2 = \mathbb{I}$ to rewrite the phase flip coder/decoder circuit as



Thus, if the noise is Z_1, then the facts $H^2 = \mathbb{I}$ and $HZH = X$ simplify the circuit to



As having the bit flip X between the two sets of CNOTs merely ensures that either one set or the other will act, the circuit in the case of Z_1 noise finally simplifies to



which establishes the final row of the table. So, given the table

Phase Flip on	Circuit Output $\|\psi\rangle$
No qubits	$\|x\rangle_1 \otimes \|0\rangle_2 \otimes \|0\rangle_3$
3rd qubit	$\|x\rangle_1 \otimes \|0\rangle_2 \otimes \|1\rangle_3$
2nd qubit	$\|x\rangle_1 \otimes \|1\rangle_2 \otimes \|0\rangle_3$
1st qubit	$\|x \oplus 1\rangle_1 \otimes \|1\rangle_2 \otimes \|1\rangle_3$

we see an error detection procedure is to measure the two ancillae and an error correction procedure is to apply a bit flip to the first qubit if the ancillae are in the state $|1\rangle_2 \otimes |1\rangle_3$ and then, in all cases where a phase flip has occurred, throw out both ancillae and replace them with fresh ancillae initialized in the state $|0\rangle_2 \otimes |0\rangle_3$.

Pedagogical Endnote: While it's inituitively clear that Z gates commute with the control bits of CNOTs, here's how one explicitly proves this. Let G_i denote a single qubit gate G that acts on the ith qubit, and let $\mathrm{CNOT}_{i,j}$ denote a CNOT that uses the ith qubit as the control and the jth qubit as the target. Thus,

$$\begin{aligned}
Z_i \cdot \mathrm{CNOT}_{i,j} &= \Big(Z_i \otimes \mathbb{I}_j\Big)\Big(|0\rangle\langle 0|_i \otimes \mathbb{I}_j + |1\rangle\langle 1|_i \otimes X_j\Big) \\
&= \Big((|0\rangle\langle 0|_i - |1\rangle\langle 1|_i) \otimes \mathbb{I}_j\Big)\Big(|0\rangle\langle 0|_i \otimes \mathbb{I}_j + |1\rangle\langle 1|_i \otimes X_j\Big) \\
&= |0\rangle\langle 0|_i \otimes \mathbb{I}_j - |1\rangle\langle 1|_i \otimes X_j
\end{aligned}$$

since $(A_i \otimes B_j)(C_i \otimes D_j) = A_i C_i \otimes B_j D_j$ and since $|a\rangle\langle a| \cdot |a\rangle\langle a| = |a\rangle\langle a|$. With similar arithmetic, one shows $\mathrm{CNOT}_{i,j} \cdot Z_i$ is the same.

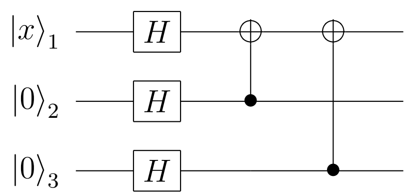
2) Construct an encoding circuit and a decoding circuit for the 9 qubit Shor code

$$|0\rangle \rightarrow \frac{1}{2\sqrt{2}}\big(|000\rangle + |111\rangle\big) \otimes \big(|000\rangle + |111\rangle\big) \otimes \big(|000\rangle + |111\rangle\big)$$

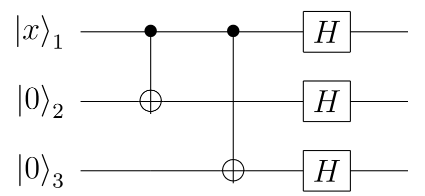
$$|1\rangle \rightarrow \frac{1}{2\sqrt{2}}\big(|000\rangle - |111\rangle\big) \otimes \big(|000\rangle - |111\rangle\big) \otimes \big(|000\rangle - |111\rangle\big).$$

Solution:

The Shor code can be viewed as the concatenation of the phase flip code with the bit flip code. We know the phase flip encoder from Problem 1, which can be written as either as



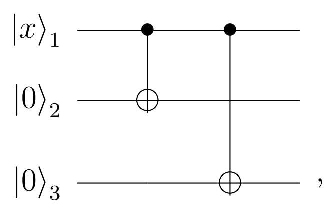
or



Either circuit maps

$$\begin{aligned} |000\rangle \longrightarrow |+++\rangle &= \frac{1}{2\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle + |1\rangle\big), \\ |111\rangle \longrightarrow |---\rangle &= \frac{1}{2\sqrt{2}}\big(|0\rangle - |1\rangle\big) \otimes \big(|0\rangle - |1\rangle\big) \otimes \big(|0\rangle - |1\rangle\big). \end{aligned}$$

The bit flip encoder is



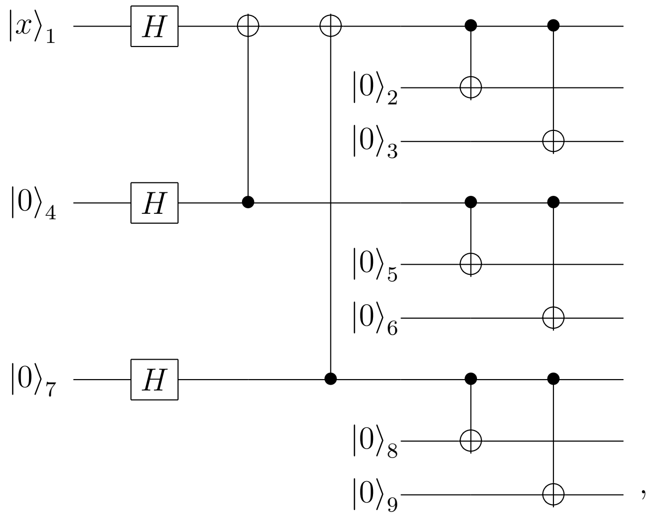
and it maps

$$|000\rangle \longrightarrow |000\rangle; \quad |100\rangle \longrightarrow |111\rangle,$$

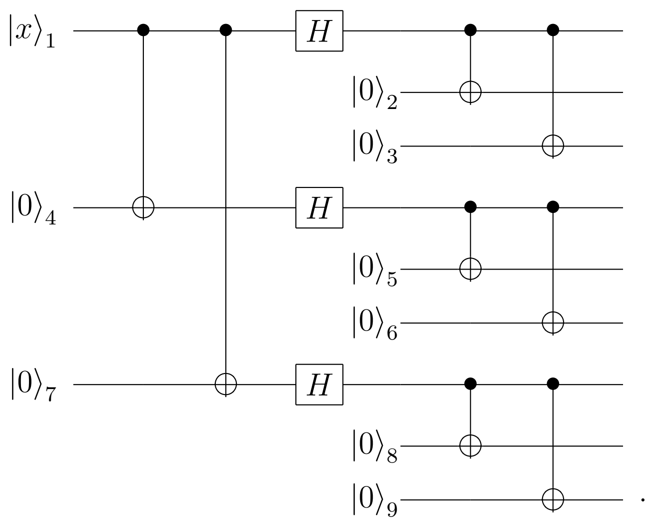
and thus, more to the point, it maps

$$\begin{aligned} |+00\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |00\rangle = \frac{1}{\sqrt{2}}\big(|000\rangle + |100\rangle\big) &\longrightarrow \frac{1}{\sqrt{2}}\big(|000\rangle + |111\rangle\big), \\ |-00\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) \otimes |00\rangle = \frac{1}{\sqrt{2}}\big(|000\rangle - |100\rangle\big) &\longrightarrow \frac{1}{\sqrt{2}}\big(|000\rangle - |111\rangle\big). \end{aligned}$$

Therefore, the encoder for the Shor code can be written as



or if you prefer,



As usual, the decoder is simply the encoder run backward.

Pedagogical Endnote: Just as quantum operations in general do not commute, the order of concatenation is in general important. In the case above, if we were instead to use the bit flip encoder and then phase flip encoder we would not get Shor's 9-qubit entangled code states that can correct any error on 1 qubit, but rather the tensor product states $|{+}{+}{+}{+}{+}{+}{+}{+}{+}\rangle$ and $|{-}{-}{-}{-}{-}{-}{-}{-}{-}\rangle$, which would only be good for correcting phase flips.

3) Verify that the 9 qubit Shor code corrects a bit and/or phase flip on any 1 of the 9 qubits.

Solution:

Unlike the phase flip code of Problem 1 or the LMPZ code of the next problem, Shor's code does *not* achieve its full error correcting potential if we use the procedure

$$[\text{encode}] \rightarrow [\text{noise}] \rightarrow [\text{decode}] \rightarrow [\text{detect error}] \rightarrow [\text{correct error}].$$

Instead, to fulfill Shor's code potential of being able to correct a bit and/or phase flip on any 1 of the 9 qubits, we must follow the procedure

$$[\text{encode}] \rightarrow [\text{noise}] \rightarrow [\text{detect error}] \rightarrow [\text{correct error}] \rightarrow [\text{decode}].$$

The reason lies in how Shor's code concatenates a phase flip and a bit flip code. Thus, for example, if we follow the first procedure and a phase flip error occurs on any of the ancillae that enter only at bit flip encoding stage and then exit at the bit flip decoding stage (i.e., qubits 2, 3, 5, 6, 8, or 9), then we will not be able to correct the phase flip. In contrast, if we follow the second procedure and perform error detection and correction on the codewords themselves, then not only can we correct such a phase flip, but also we can quite conveniently derive the appropriate detection and correction procedures simply by concatenating the detection and correction operations for the codewords of the constituent phase flip and bit flip codes.

So what are valid detection and correction procedures to apply to the codewords themselves of the phase flip and bit flip codes? The answer is quite easy to intuit since both the phase flip and bit flip codes are merely the quantum analogues of 3-bit majority vote codes. Thus, we seek the quantum analogue of comparing the first bit to the second and the second to the third to locate a single error. These analogues are not hard to intuit, namely Z_iZ_j to compare the Z states of qubits i and j to determine whether a bit flip has occurred to either (thus making their Z values disagree and multiply to -1 rather than 1) and X_iX_j to compare the X states of qubits i and j to determine whether a phase flip has occurred to either (thus making the X values disagree and multiply to -1 rather than 1). However, one might worry that such measurements ruin the encoded data.

The worry turns out to be unfounded because measuring Z_iZ_j does *not* discriminate between the bit flip codewords $\{|000\rangle, |111\rangle\}$ or corruptions thereof by a single bit flip and/or phase flip. We see this from the fact

$$\langle 000|M_k Z_i Z_j M_k|000\rangle = \langle 111|M_k Z_i Z_j M_k|111\rangle$$

for all $i, j, k \in \{1, 2, 3\}$ and for all $M \in \{\mathbb{I}, X, Y, Z\}$. (In words, the expectation value of Z_iZ_j is the same on both the state $M_k|000\rangle$ and the state $M_k|111\rangle$. Hence, even if we had access to an arbitrarily large ensemble of identically prepared systems in these two states and could gather statistics by repeatedly measuring Z_iZ_j, we could not discriminate between these two states.)

Similarly, measuring X_iX_j does not discriminate between the phase flip codewords $|+{+}+\rangle$ and $|-{-}-\rangle$ or corruptions thereof by a single bit flip and/or phase flip as

$$\langle +{+}+|M_k X_i X_j M_k|+{+}+\rangle = \langle -{-}-|M_k X_i X_j M_k|-{-}-\rangle.$$

Concatenating the bit flip and phase flip codes into Shor's code, the analogous statements are that neither measuring $X_{3m-2}X_{3m-1}X_{3m}X_{3n-2}X_{3n-1}X_{3n}$ (where $m, n \in \{1, 2, 3\}$) nor measuring Z_iZ_j (where $i, j \in \{1, \ldots, 9\}$) discriminates between the Shor codewords

$$|0\rangle_{\text{Shor}} = \frac{1}{2\sqrt{2}}\big(|000\rangle + |111\rangle\big) \otimes \big(|000\rangle + |111\rangle\big) \otimes \big(|000\rangle + |111\rangle\big)$$

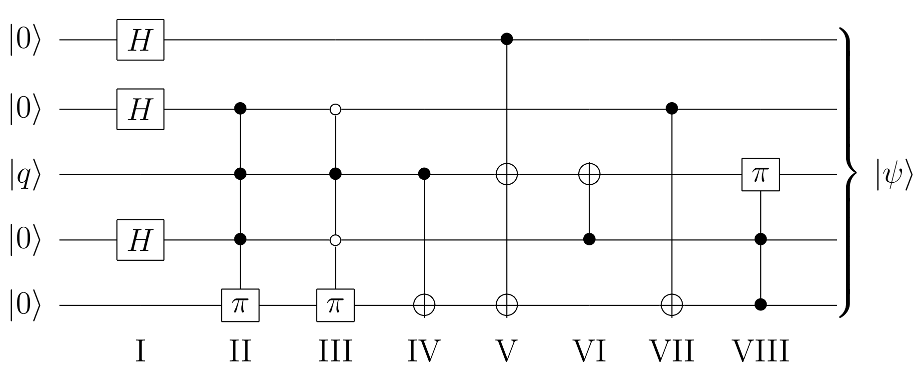
$$|1\rangle_{\text{Shor}} = \frac{1}{2\sqrt{2}}\big(|000\rangle - |111\rangle\big) \otimes \big(|000\rangle - |111\rangle\big) \otimes \big(|000\rangle - |111\rangle\big).$$

or corruptions thereof by a single bit and/or phase flip.

Therefore, to detect a bit flip in the Shor code, we perform measurements of Z_1Z_2, Z_2Z_3, $\ldots$, Z_7Z_8 on the encoded qubits. To correct the bit flip, we perform an X gate on the qubit where the bit flip occurred. To detect a phase flip, we measure $X_1X_2X_3X_4X_5X_6$ and $X_4X_5X_6X_7X_8X_9$ on the encoded qubits. Granted, this cannot detect exactly which qubit was affected by the phase flip, only which trio of qubits (123), (456), or (789) was affected. However, this suffices and we perform a Z gate on any qubit of the affected triplet in order to correct the phase flip (or, if you prefer aesthetically to keep with the theme of concatenation, we perform ZZZ on the affected trio).

---

4) What is the output $|\psi\rangle$ of the following circuit, which is the encoder for the Laflamme-Miquel-Paz-Zurek perfect 5 qubit code?



Solution: This is just some bit of semi-tedious arithmetic and there's no great cleverness to be had other than choosing good, concise notation that allows one to minimize the opportunity for typos and the desire to cry out, "Why am I writing out this problem in full?! How much credit really would be deducted if I stopped now?!"

To that end, we do not explicitly write out all the component kets in the computer's quantum state until the end. Note that in the following $\delta_{(xyz),(x'y'z')}$ denotes the Kronecker delta function that equals 1 only if $x = x'$, $y = y'$, and $z = z'$, and otherwise equals 0. Also, as usual, $\oplus$ denotes addition mod 2.

$$
\begin{aligned}
|\mathrm{I}\rangle &= \frac{1}{2\sqrt{2}} \sum_{z_1=0}^{1} \sum_{z_2=0}^{1} \sum_{z_4=0}^{1} |z_1\, z_2\, q\, z_4\, 0\rangle \\
|\mathrm{II}\rangle &= \frac{1}{2\sqrt{2}} \sum_{z_1=0}^{1} \sum_{z_2=0}^{1} \sum_{z_4=0}^{1} (-1)^{\delta_{(z_2\, q\, z_4),(111)}} |z_1\, z_2\, q\, z_4\, 0\rangle \\
|\mathrm{III}\rangle &= \frac{1}{2\sqrt{2}} \sum_{z_1=0}^{1} \sum_{z_2=0}^{1} \sum_{z_4=0}^{1} (-1)^{\delta_{(z_2\, q\, z_4),(010 \text{ or } 111)}} |z_1\, z_2\, q\, z_4\, 0\rangle \\
|\mathrm{IV}\rangle &= \frac{1}{2\sqrt{2}} \sum_{z_1=0}^{1} \sum_{z_2=0}^{1} \sum_{z_4=0}^{1} (-1)^{\delta_{(z_2\, q\, z_4),(010 \text{ or } 111)}} |z_1\, z_2\, q\, z_4\, q\rangle \\
|\mathrm{V}\rangle &= \frac{1}{2\sqrt{2}} \sum_{z_1=0}^{1} \sum_{z_2=0}^{1} \sum_{z_4=0}^{1} (-1)^{\delta_{(z_2\, q\, z_4),(010 \text{ or } 111)}} |z_1\, z_2\, (q \oplus z_1)\, z_4\, (q \oplus z_1)\rangle \\
|\mathrm{VI}\rangle &= \frac{1}{2\sqrt{2}} \sum_{z_1=0}^{1} \sum_{z_2=0}^{1} \sum_{z_4=0}^{1} (-1)^{\delta_{(z_2\, q\, z_4),(010 \text{ or } 111)}} |z_1\, z_2\, (q \oplus z_1 \oplus z_4)\, z_4\, (q \oplus z_1)\rangle \\
|\mathrm{VII}\rangle &= \frac{1}{2\sqrt{2}} \sum_{z_1=0}^{1} \sum_{z_2=0}^{1} \sum_{z_4=0}^{1} (-1)^{\delta_{(z_2\, q\, z_4),(010 \text{ or } 111)}} |z_1\, z_2\, (q \oplus z_1 \oplus z_4)\, z_4\, (q \oplus z_1 \oplus z_2)\rangle \\
|\mathrm{VIII}\rangle &= \frac{1}{2\sqrt{2}} \sum_{z_1=0}^{1} \sum_{z_2=0}^{1} \sum_{z_4=0}^{1} (-1)^{\delta_{[z_4 (q \oplus z_1 \oplus z_2)],(11)}} (-1)^{\delta_{(z_2\, q\, z_4),(010 \text{ or } 111)}} |z_1\, z_2\, (q \oplus z_1 \oplus z_4)\, z_4\, (q \oplus z_1 \oplus z_2)\rangle
\end{aligned}
$$

Now we finally write out the component kets in full. First, the $q = 0$ case

$$
|00000\rangle \longrightarrow |0\rangle_{\mathrm{LMPZ}} = \frac{1}{2\sqrt{2}} \left(\begin{array}{c} |00000\rangle + |00110\rangle + |01001\rangle - |01111\rangle \\ +|10101\rangle - |10011\rangle + |11100\rangle + |11010\rangle \end{array} \right),
$$

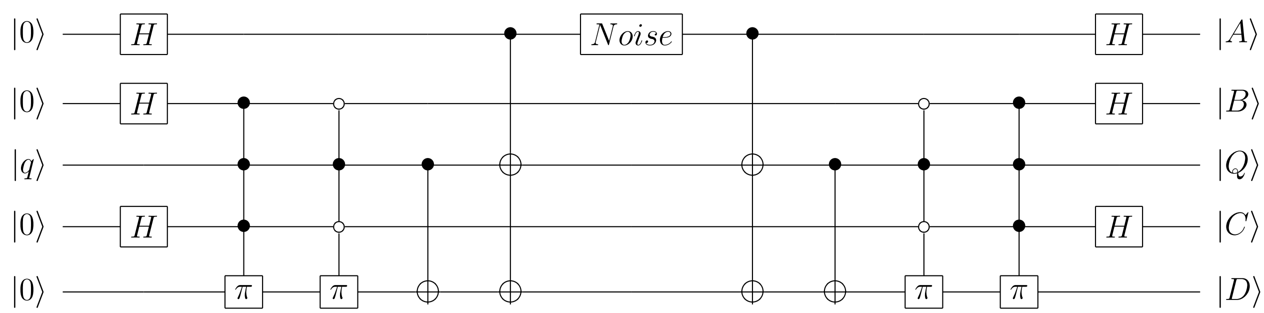
and then the $q = 1$ case

$$
|00100\rangle \longrightarrow |1\rangle_{\mathrm{LMPZ}} = \frac{1}{2\sqrt{2}} \left(\begin{array}{c} -|00101\rangle - |00011\rangle + |01100\rangle - |01010\rangle \\ -|10000\rangle + |10110\rangle + |11001\rangle + |11111\rangle \end{array} \right).
$$

5) Verify that the decoder of the above circuit allows one to correct a bit and/or phase flip on any 1 of the 5 qubits.

Solution: This is just more semi-tedious arithmetic, which if you calculate out the entire syndrome for all 15 possible 1-qubit errors, becomes very tedious. However, as in Problem 1, there is some pedagogical value in seeing how to manipulate commutation relations and other circuit identities so as to avoid any long matrix multiplication. But even this gets old fast. So, we'll content ourselves with verifying that the code corrects a bit and/or phase flip on the first qubit.

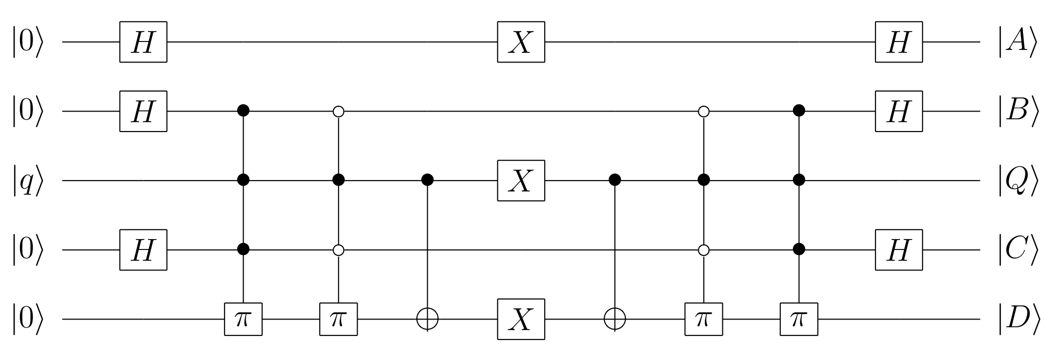
We choose the first qubit since it will allow us to take the greatest possible advantage from the fact the decoder is the inverse of the encoder. If the error is definitely on the first qubit, then the relevant part of the encoder-decoder circuit is



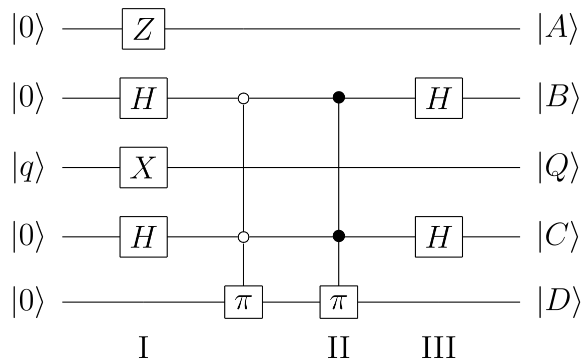
If the noise is a Pauli Z gate (a phase flip), then since Z's commute with the control bits of CNOTs (see solution to Problem 1) and since $HZH = X$, we immediately conclude that the output of the encoder-decoder circuit in the case of a phase flip on the first qubit is $|ABQCD\rangle = |10Q00\rangle$.

Thus, the ancillae syndrome for a phase flip error on the first qubit is $(A, B, C, D) = (1, 0, 0, 0)$*, and an appropriate correction operation is to apply a bit flip to the first qubit or simply to discard it and replace it with a fresh ancilla in the state* $|0\rangle$*.*

If the noise is Pauli X gate (a bit flip), then we know that only one of the C-NOT-NOTs controlled by the first qubit will act. So, the circuit simplifies to



But this circuit can be simplified even further since the X-gate affecting the third qubit means that only one of the CNOTs targeting the fifth qubit will act. Thus, those CNOTs just turn into another X-gate on the fifth qubit. However, this extra X-gate cancels out the X-gate already there. Moreover, the X-gate affecting the third qubit means that only one of the two pairs of triply-controlled-π gates will act. This reduces the two pairs of triply-controlled-π gates into just one pair of doubly-controlled-π gates. Finally, we note $HXH = Z$. Hence, the encoder-decoder circuit in the case of bit flip noise on the first qubit simplifies to just



Alas, we now have to do (a little) arithmetic

$$
\begin{aligned}
|\mathrm{I}\rangle &= \frac{1}{2}\sum_{z_2=0}^{1}\sum_{z_4=0}^{1} |0\, z_2\, (q\oplus 1)\, z_4\, 0\rangle \\
|\mathrm{II}\rangle &= \frac{1}{2}\sum_{z_2=0}^{1}\sum_{z_4=0}^{1} (-1)^{\delta_{(z_2\, z_4),(00 \text{ or } 11)}} |0\, z_2\, (q\oplus 1)\, z_4\, 0\rangle \\
&= |0_1\, (q\oplus 1)_3\, 0_5\rangle \otimes \frac{1}{2}\Big(-|0_2 0_4\rangle + |0_2 1_4\rangle + |1_2 0_4\rangle - |1_2 1_4\rangle \Big) \\
|\mathrm{III}\rangle &= |0_1\, (q\oplus 1)_3\, 0_5\rangle \otimes \frac{1}{2}\Big(H_2 \otimes H_4 \Big)\Big(|0_2 0_4\rangle - |0_2 1_4\rangle - |1_2 0_4\rangle + |1_2 1_4\rangle \Big) \\
&= |0_1\, (q\oplus 1)_3\, 0_5\rangle \otimes \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} -1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \\
&= |0_1\, (q\oplus 1)_3\, 0_5\rangle \otimes \frac{1}{4}\begin{pmatrix} 0 \\ 0 \\ 0 \\ -1 \end{pmatrix} \\
&= -|0\, 1\, (q\oplus 1)\, 1\, 0\rangle
\end{aligned}
$$

Thus, the ancillae syndrome for a bit flip error on the first qubit is $(A, B, C, D) = (0, 1, 1, 0)$, *and an appropriate correction operation is to apply* $X_2\pi_3 X_3 X_4$ *or simply to apply* $\pi_3 X_3$ *and discard the ancillae and replace them with fresh ones in the state* $|0\rangle$.

Finally, when it comes to a combined bit flip and phase flip error XZ, it turns out we can trivially combine the above results. The only change from the reduced circuit depicted above for the bit flip alone case is that the effective gate for the first qubit is $iY = HXZH$ instead of $Z = HXH$. Hence, the output of the encoder-decoder circuit is $|ABQCD\rangle = -|1\,1\,(q \oplus 1)\,1\,0\rangle$.

Thus, the ancillae syndrome for a ZX error on the first qubit is $(A, B, C, D) = (1, 1, 1, 0)$, and an appropriate correction operation is to apply $X_1 X_2 \pi_3 X_3 X_4$ or simply to apply $\pi_3 X_3$ and replace the ancillae with fresh ones in the state $|0\rangle$.

---

6) Consider the code $|0\rangle_{en} = \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big)$; $|1\rangle_{en} = \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big)$. Show that an arbitrary superposition of encoded states $\alpha|0\rangle_{en} + \beta|1\rangle_{en}$ is robust against errors of the form $e^{-i\theta\sigma_z/2} \otimes e^{-i\theta\sigma_z/2}$.

Solution:

This code is robust against errors of the form $e^{-i\theta\sigma_z/2} \otimes e^{-i\theta\sigma_z/2}$ since both $|01\rangle$ and $|10\rangle$ are invariant under such unitary operations.

To make this explicit, note that $e^{-i\theta\sigma_z/2} = \exp\left[\frac{-i\theta}{2}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\right] = \begin{pmatrix}e^{-i\theta/2} & 0\\ 0 & e^{i\theta/2}\end{pmatrix}$. It is then trivial to verify that

$$e^{-i\theta\sigma_z/2} \otimes e^{-i\theta\sigma_z/2}|01\rangle = e^{-i\theta/2}|0\rangle \otimes e^{i\theta/2}|1\rangle = |01\rangle,$$

$$e^{-i\theta\sigma_z/2} \otimes e^{-i\theta\sigma_z/2}|10\rangle = e^{i\theta/2}|1\rangle \otimes e^{-i\theta/2}|0\rangle = |10\rangle.$$

(Thus, from the standpoint of being immune to errors of the form $e^{-i\theta\sigma_z/2} \otimes e^{-i\theta\sigma_z/2}$, any 2 orthogonal states in the space spanned by $|01\rangle$ and $|10\rangle$ would work.)