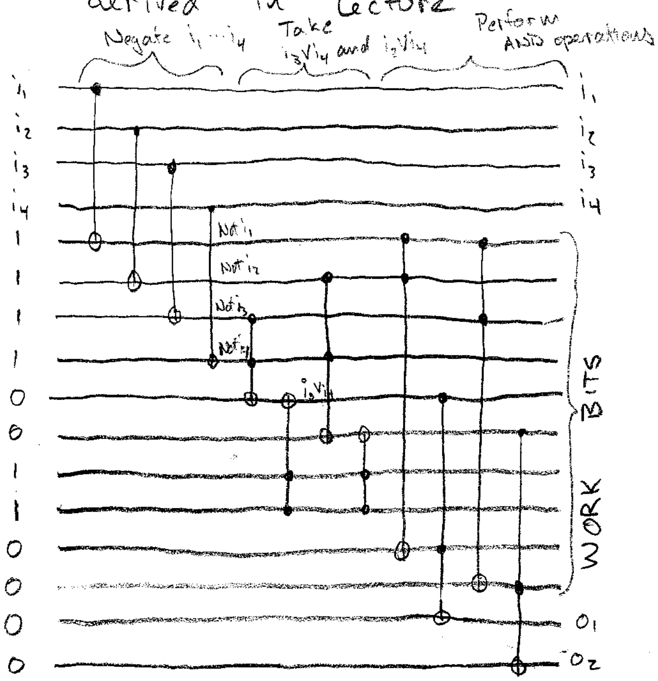
Problem 1

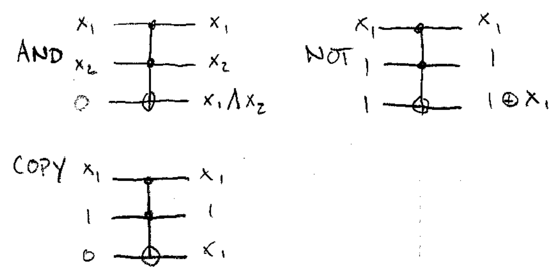
There are many ways to implement the desired circuit, and all that demonstrably meet the criteria will be acceptable. The circuit given here follows the logical progression used in class. It is undoubtedly inefficient in the number of Toffoli gates, but that is not important.

If we label our input bits as i_1, i_2, i_3, i_4 and the output bits as o_1, o_2 then we want the following logical operations

$$o_1 = (\text{Not } i_1) \text{ AND } (\text{Not } i_2) \text{ AND } (i_3 \text{ OR } i_4)$$
$$o_2 = (\text{Not } i_1) \text{ AND } (\text{Not } i_3) \text{ AND } (i_2 \text{ OR } i_4)$$

We can accomplish this with Toffoli gates using the equivalences derived in lecture





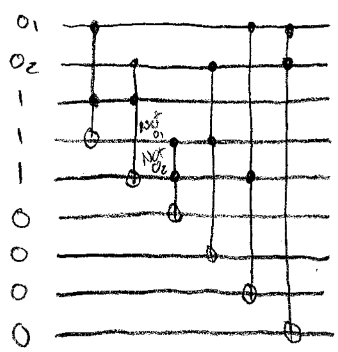
We can comput OR remembering

This circuit required 12 Toffoli gates, but we still have non-constant work bits and we have not erased our input bits.

To erase the work bits, we use the second theorem in class. We copy the output (using 2 more Toffoli gates) and then run the circuit in reverse. This leaves us the input, output, and constants and required 26 toffoli gates. Call this C_1.

What about getting rid of the input? We apply the third theorem and generate a reversible circuit that maps the output to the input (and taking the work bits to constants.)

This can be accomplished by



This took 6 Toffoli gates. To remove the work bits, we need four copies and then run the circuit in reverse. This piece takes 16 Toffoli gates. Call this C_2.

The overall circuit runs C_1 followed by $(C_2)^{-1}$ and requires $26+16=42$ gates.

Remember again that is is almost certainly not the most efficient circuit, either in number of gates or number of work bits.

Problem 2

We learned in class reversible gates of 1 and 2 bits can only create affine functions of the form

$$\underline{y} = M\underline{x} + \underline{a}$$

where $\underline{y}$, $\underline{x}$, and $\underline{a}$ are vector representations of our bit strings and M is a non-singular matrix of $\{0,1\}$ entries. (Addition is performed modulo 2). This is discussed in Preskill's notes section 6.1.3.

Now consider what happens with the circuit from problem 1. The affine relationship can be written as

$$\begin{bmatrix} y_i \\ k \end{bmatrix} = M \begin{bmatrix} x_i \\ k' \end{bmatrix} + \underline{a}$$

where x_i, y_i represent our input and output strings, and k and k' are the constant work bits.

What happens if we add up the four outputs (modulo 2)? We get 0, but as we'll see, this is a contradiction:

$$\underline{0} = \sum_i \begin{bmatrix} y_i \\ k \end{bmatrix} = M\left(\sum_i \begin{bmatrix} x_i \\ k' \end{bmatrix}\right) + \cancel{4}^{0}\underline{a} \qquad \text{But } \sum_i \begin{bmatrix} x_i \\ k' \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \text{ is not-zero.}$$

For this to be true M must be singular. Hence, a contradiction.

Problem 3

This is closely related to the solution for Problem 2. We have now removed the contradiction. We can see this by noting that the inputs are linearly independendent, as are the outputs. We can therefore create a linear relation between the two and can thus use CNOT gates to build the circuit. (You could do this through a methodology similar to problem 1.

Problem 4

We derived in class that a rotation by θ about an axis $\hat{n} = (n_x, n_y, n_z)$ is given by

$$R_{\hat{n}}(\theta) \equiv \exp(-i\theta\, \hat{n} \cdot \vec{\sigma}/2) = \cos\frac{\theta}{2}\, I - i \sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z)$$

(This is Nielsen and Chuang equation 4.8).

Applying this for $\hat{n} = (1/\sqrt{3}, 1/\sqrt{3}, 1/\sqrt{3})$ we get

$$\cos\frac{\pi}{3}\, I - i \sin\frac{\pi}{3}\left(\frac{1}{\sqrt{3}} X + \frac{1}{\sqrt{3}} Y + \frac{1}{\sqrt{3}} Z\right)$$

$$= \cancel{\begin{bmatrix} \frac{\sqrt{3}}{2} - \frac{i}{2\sqrt{3}} & \frac{-1-i}{2\sqrt{3}} \\ \frac{1-i}{2\sqrt{3}} & \frac{\sqrt{3}}{2} + \frac{i}{2\sqrt{3}} \end{bmatrix}} \qquad \frac{1}{2}\begin{bmatrix} 1-i & -1-i \\ 1-i & 1+i \end{bmatrix}$$

Problem 5

~~Assume a U that fixes $|z+\rangle$ and $|z-\rangle$ ($|0\rangle$ and $|1\rangle$)~~

~~So $U|0\rangle = |0\rangle$ and $U|1\rangle = |1\rangle$.~~

~~From this, we already know how it affects $|y\pm\rangle$:~~

$$|y+\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \qquad |y-\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$$

$$U|y+\rangle = \frac{U|0\rangle + iU|1\rangle}{\sqrt{2}} \qquad U|y-\rangle = \frac{U|0\rangle - iU|1\rangle}{\sqrt{2}}$$

$$= |y+\rangle \qquad\qquad = |y-\rangle$$

~~Thus we cannot have a unitary that fixes the x and z directions, but flips the y.~~

See correction on the next page.

Correct Solution to Problem 5

5. $|z+\rangle := |0\rangle$, $|z-\rangle = |1\rangle$ $\quad |x\pm\rangle = \frac{1}{\sqrt{2}}(|z+\rangle \pm |z-\rangle)$ $\quad |y\pm\rangle = \frac{1}{\sqrt{2}}(|z+\rangle \pm i|z-\rangle)$

Also note
$$|y+\rangle = \frac{1+i}{2}|x+\rangle + \frac{(1-i)}{2}|x-\rangle$$
$$|y-\rangle = \frac{1-i}{2}|x+\rangle + \frac{(1+i)}{2}|x-\rangle$$

A unitary operator that fixes $|x\pm\rangle$ and $|z\pm\rangle$ implies that
$$U|z+\rangle = e^{i\theta_1}|z+\rangle,\ U|z-\rangle = e^{i\theta_2}|z-\rangle,\ U|x+\rangle = e^{i\theta_3}|x+\rangle,\ U|x-\rangle = e^{i\theta_4}|x-\rangle$$

Using the relations between $|x\pm\rangle$ and $|z\pm\rangle$ we can show that $\theta_1 = \theta_2 = \theta_3 = \theta_4$

$$e^{i\theta_3}|x+\rangle = U|x+\rangle = \frac{1}{\sqrt{2}}\left(U|z+\rangle + U|z-\rangle\right) = \frac{e^{i\theta_1}|z+\rangle + e^{i\theta_2}|z-\rangle}{\sqrt{2}}$$
$$= e^{i\theta_1}\left(\frac{|z+\rangle + e^{i(\theta_2-\theta_1)}|z-\rangle}{\sqrt{2}}\right)$$

We see that these are only equal if $\theta_3 = \theta_1 = \theta_2$ (mod 2π of course)
A similar argument with $|x-\rangle$ shows that $\theta_4 = \theta_1 = \theta_2$.

We can now see that the further requirement that $U|y+\rangle = e^{i\theta_5}|y-\rangle$, $U|y-\rangle = e^{i\theta_6}|y+\rangle$ leads to a contradiction.

$$U|y+\rangle = \frac{1}{\sqrt{2}}\left(U|z+\rangle + iU|z-\rangle\right) = \frac{e^{i\theta_1}}{\sqrt{2}}\left(|z+\rangle + i|z-\rangle\right) = e^{i\theta_1}|y+\rangle$$

similarly
$$U|y-\rangle = e^{i\theta_1}|y-\rangle$$

Notice that this follows only after showing that $\theta_1 = \theta_2$.