Hw 2.

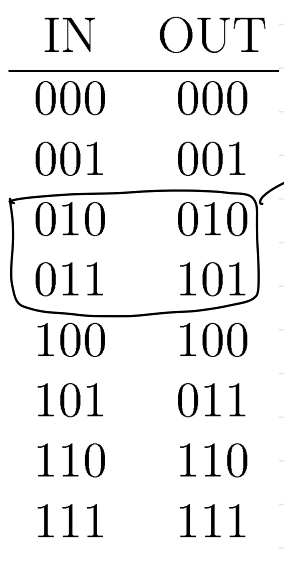
1. What are the one- and two-bit conservative classical gates? Show that these are not sufficient to do universal classical computation, and thus cannot be used to make a Fredkin gate.

one-bit conservative classical gates : Identity $1 \to 1$, $0 \to 0$

two-bit conservative classical gates : Identity $\begin{matrix}1\\1\end{matrix} \Rightarrow \begin{matrix}1\\1\end{matrix}$, $\begin{matrix}0\\0\end{matrix} \Rightarrow \begin{matrix}0\\0\end{matrix}$

swap gate $\begin{matrix}1\\0\end{matrix} \Rightarrow \begin{matrix}0\\1\end{matrix}$, $\begin{matrix}0\\1\end{matrix} \Rightarrow \begin{matrix}1\\0\end{matrix}$

truth table for Fredkin gate :



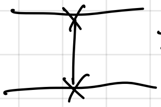
IN	OUT
000	000
001	001
010	010
011	101
100	100
101	011
110	110
111	111

It is impossible to implement these in the same one and two-bit conservative classical gate.

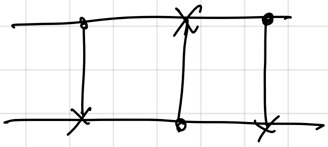
They can't make a Fredkin gate.

2. Find some conservative two-bit quantum gates. Gates which just change phase (diagonal unitary matrices) are conservative, as is the SWAP gate. Find a larger class of such gates. Find a square root of SWAP.

SWAP gate =



=



$$= \begin{bmatrix} 1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0 \end{bmatrix}$$

$$= \begin{bmatrix} 1&0&0&0\\0&0&0&1\\0&1&0&0\\0&0&1&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0 \end{bmatrix}$$

$$= \begin{bmatrix} 1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1 \end{bmatrix}$$

with changing phase

$$i \quad \begin{bmatrix} e^{i\theta}&0&0&0\\0&a&b&0\\0&b^*&c&0\\0&0&0&e^{i\theta'} \end{bmatrix}$$

$$\left| \begin{bmatrix} 1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1 \end{bmatrix} - \lambda I \right| = 0$$

$$\Rightarrow \lambda = \pm 1$$

$\lambda = 1$: eigenvectors: $|00\rangle, |11\rangle, \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

$\lambda = -1$: eigenvectors: $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

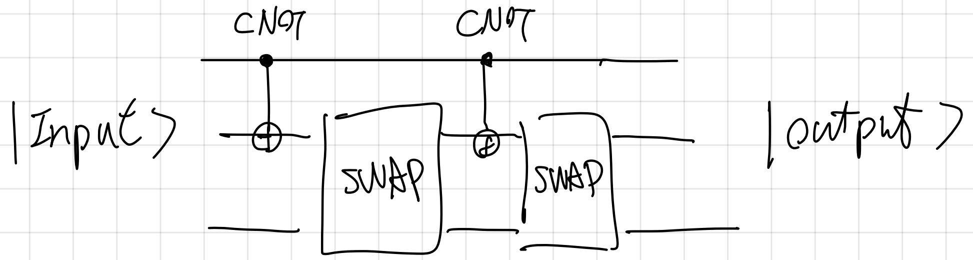
SWAP gate can be diagonalized as $\sum_i \lambda_i |x_i\rangle\langle x_i|$

We can take square root : $\sum_i \sqrt{\lambda_i} |x_i\rangle\langle x_i|$

$$\sqrt{SWAP} = \begin{bmatrix} 1&0&0&0\\0&\frac{1}{\sqrt{2}}&\frac{1}{\sqrt{2}}&0\\0&\frac{1}{\sqrt{2}}&-\frac{1}{\sqrt{2}}&0\\0&0&0&1 \end{bmatrix} \begin{bmatrix} \sqrt{1}&0&0&0\\0&\sqrt{1}&0&0\\0&0&\sqrt{-1}&0\\0&0&0&\sqrt{1} \end{bmatrix} \begin{bmatrix} 1&0&0&0\\0&\frac{1}{\sqrt{2}}&\frac{1}{\sqrt{2}}&0\\0&\frac{1}{\sqrt{2}}&-\frac{1}{\sqrt{2}}&0\\0&0&0&1 \end{bmatrix}$$

$$= \begin{bmatrix} 1&0&0&0\\0&\frac{1}{\sqrt{2}}&\frac{1}{\sqrt{2}}&0\\0&\frac{1}{\sqrt{2}}&-\frac{1}{\sqrt{2}}&0\\0&0&0&1 \end{bmatrix} \begin{bmatrix} 1&0&0&0\\0&\frac{1}{\sqrt{2}}&\frac{1}{\sqrt{2}}&0\\0&\frac{i}{\sqrt{2}}&-\frac{i}{\sqrt{2}}&0\\0&0&0&1 \end{bmatrix} = \begin{bmatrix} 1&0&0&0\\0&\frac{1}{2}(1+i)&\frac{1}{2}(1-i)&0\\0&\frac{1}{2}(1-i)&\frac{1}{2}(1+i)&0\\0&0&0&1 \end{bmatrix}$$

3. Multiply some of the gates found in (2) to build a quantum gate $\tilde{F}$ which manipulates the bits in the same way as the Fredkin gate when operating on states in the canonical basis, but in which some phases might be different. (So that the 8×8 matrix representing $\tilde{F}$ is the same as for the Fredkin gate, except that some of the $+1$ entries have been replaced by other unit complex numbers.) Show that there is an 8×8 diagonal unitary matrix which you can multiply by $\tilde{F}$ to produce a Fredkin gate. (If you directly build a Fredkin gate with all the phases correct, you may skip this last step.)



4. By combining two-qubit unitary diagonal matrices (these represent gates that just manipulate phases), which three-qubit diagonal matrices can you obtain? Show that if you augment these gates with the gates represented by diagonal matrices with entries $1, 1, e^{-i\theta}, 1, e^{i\theta}, 1, 1, 1$ on the diagonal you can obtain all of the 3-qubit diagonal gates.

WARNING: I made a mistake in this homework problem. Both exponentials should be $e^{i\theta}$. This means that problem 5 no longer works, so you don't have to do it. I don't know whether it's possible to build a Fredkin gate from conservative 2-qubit gates or not.

5. Use the gate $\tilde{F}$ produced in (3) in combination with 2-qubit phase gates to produce diagonal gates which (like the ones in Problem 4) will produce all three-qubit diagonal matrices in combination with two-qubit diagonal gates,

X It is impossible to onstructe Fredkin gate by two-qubit conservative gates.

7. Suppose that you can build an efficient quantum circuit that performs a quantum Fourier transform for each of two large primes p and q. Show that you use these two circuits to build an efficient quantum circuit for the quantum Fourier transform over pq.

Clarification: the circuit performing the Fourier transform for prime p acts on states $|\, a\rangle$ as follows:

$$|\, a\rangle \to \frac{1}{\sqrt{p}} \sum_{0}^{p-1} e^{2\pi i ab/p} \,|\, b\rangle$$

where a, b are numbers $a, b < p$ represented in binary. The circuit's actions on $|\, a\rangle$ with $a \geq p$ is not known (it does have to give some output for these states, but it doesn't matter what it is for this problem).

Hint: Use the Chinese remainder theorem (p. 629 of Nielsen & Chuang).

We have $|a_1\rangle \to \frac{1}{\sqrt{p}} \sum_{0}^{p-1} e^{2\pi i a_1 b_1/p} |b_1\rangle$

$|a_2\rangle \to \frac{1}{\sqrt{q}} \sum_{0}^{q-1} e^{2\pi i a_2 b_1/q} |b_2\rangle$

We want ~~to~~ implement

$$|a'\rangle \to \frac{1}{\sqrt{pq}} \sum_{0}^{pq-1} e^{2\pi i a' b'/pq} |b'\rangle$$

From Chinese remainder theorem

We can reform the performence :

$|x \bmod p\rangle \to \frac{1}{\sqrt{p}} \sum_{0}^{p-1} e^{2\pi i xy/p} |y \bmod p\rangle$

$|x \bmod q\rangle \to \frac{1}{\sqrt{q}} \sum_{0}^{q-1} e^{2\pi i xy/q} |y \bmod q\rangle$

$|x \bmod pq\rangle \to \frac{1}{\sqrt{pq}} \sum_{0}^{pq-1} e^{2\pi i xy/pq} |y \bmod pq\rangle$

From Chinese remainder theorem (equal modulo)

$|x \bmod pq\rangle \to |x \bmod p\rangle |x \bmod q\rangle$

Combine 2 circuits

$$|x \bmod p\rangle|x \bmod q\rangle \to \frac{1}{\sqrt{pq}}\sum_{0}^{p-1}\sum_{0}^{q-1} e^{2\pi i x y_1/p} e^{2\pi i x y_2/q}|y_1 \bmod p\rangle|y_2 \bmod q\rangle$$

$$\to \frac{1}{\sqrt{pq}}\sum_{0}^{p-1}\sum_{0}^{q-1} e^{2\pi i x (y_1 q + y_2 p)/pq}\underbrace{|y_1 \bmod p\rangle|y_2 \bmod q\rangle}$$

$$|y_1 \bmod p\rangle|y_2 \bmod q\rangle = |y_1 q \bmod p\rangle|y_2 p \bmod q\rangle$$

by Chinese remainder theorem

$$\Rightarrow |y_1 q \bmod p\rangle|y_2 p \bmod q\rangle = |y_1 q + y_2 p \bmod pq\rangle$$

define $y_1 q + y_2 p = y$

$$\to \frac{1}{\sqrt{pq}}\sum_{0}^{pq-1} e^{2\pi i x y/pq}|y \bmod pq\rangle$$

So hard ...