18.435/2.111 Homework # 2

Due Thursday, October 2

The Fredkin gate is a 3-bit gate that implements a controlled SWAP: if the third bit is a 1, the first and second bits are swapped, and if the third bit is a 0, all three bits are unchanged. [NOTE: The Fredkin gate is commonly defined with the first bit being the control bit; I am using the third bit here to be consistent with the discussion in Nielsen & Chuang, pp. 156–161, although they also define it with the first bit being the control bit in a discussion later in the text.]
The truth table is:

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

The Fredkin gate has the property that it is conservative, meaning that it preserves the number of 1's. This means that, for example, it can be used to show that an idealized "billiard ball computer" (see Nielsen & Chuang, pp. 155-156) is a universal classical computer. The "billiard ball computer" does computation using idealized frictionless billiard balls, which act according to Newton's laws of motion. Since the number of billiard balls is conserved, and since in a frictionless environment, Newton's laws of motion are reversible, any gates a "billiard ball computer" uses must be conservative and reversible. It is shown that the Fredkin gate is universal on p. 157 of the textbook.

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.

In problems 2–5, you will build a Fredkin gate from one- and two-bit conservative quantum gates. (A conservative quantum gate is one that preserves the number of qubits in the $|1\rangle$ state, i.e., it commutes with the observable that measures the number of $|1\rangle$'s.) There is more than one way of building a Fredkin gate, even if the steps outlined below are followed.

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.

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the 8×8 matrix representing $\tilde{F}$ is the same as for the Fredkin gate, except that some of the $+1$ entries have been replaced by other unit complex numbers.)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.)

Hint: The square root of SWAP gate (or alternatively, the square root of the product D SWAP for some unitary diagonal matrix D) can be useful here. Can you combine two square root of SWAP gates with other two-qubit gates so that the SWAP is performed if the third qubit is 1 and a diagonal matrix is performed if the third qubit is 0?

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,

6. **Extra Credit.** How few two-qubit conservative gates are sufficient to build a Fredkin gate? I don't know the answer to this one. Anyone finding reasonably small constructions will get extra credit.

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).