18.435/2.111 Homework # 2 Solutions

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.

Solution: It is easy to check that the only one-bit conservative classical gate is the identity. The two- bit conservative classical gates must take 00 to 00, must take 11 to 11, and must take 01 and 10 to a state with exactly 1 one. This leaves four possibilities,

IN	OUT
00	00
01	01
10	10
11	11

IN	OUT
00	00
01	10
10	01
11	11

IN	OUT
00	00
01	01
10	01
11	11

IN	OUT
00	00
01	10
10	10
11	11

The first of these gates is the identity and the second is the SWAP gate. Suppose you want to implement a 1-1 function whose output bits are not a fixed permutation of the input bits. The last two of these gates cannot be used as they map the inputs 01 and 10 to the same outputs, and so can not be used for the computation of a 1-1 function, as these would lead to fewer than 2^n possible outputs. The identity and the SWAP gates merely change the order the bits. Thus, these four gates cannot compute (say) a Fredkin gate, which is a 1-1 conservative functions that is not a permutation of the inputs.

The above proof does not allow for the use of extra workbits that can be initialized in the states 0 or 1, but it is easy to check that these don't help, as if a constant bit is one of the inputs to any of the above four gates, it behaves the same as either the identity gate or the SWAP gate.

My attempt to build a Fredkin gate in problems 2–5 failed because of a sign error in Problem 4.

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.

Solution: The most general two-qubit conservative gate cannot mix the three subspaces containing no $|1\rangle$'s, containing one $|1\rangle$, and containing two $|1\rangle$'s, and thus is composed of two arbitary 1×1 unitary matrices and an arbitrary 2×2 unitar matrix. This can be expressed, for example, as

$$\begin{pmatrix} e^{i\theta_0} & 0 & 0 & 0 \\ 0 & a & b & 0 \\ 0 & e^{i\theta_1} b^* & -e^{i\theta_1} a^* & 0 \\ 0 & 0 & 0 & e^{i\theta_2} \end{pmatrix}$$

where the θ_i are real numbers, and a and b are complex numbers satisfying $|a|^2+|b|^2 = 1$.

The SWAP gate is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

If you take its eigenvectors and eigenvalues, you find that $|\,00\rangle$, $|\,11\rangle$, and $\frac{1}{\sqrt{2}}(|\,01\rangle + |\,10\rangle)$ are eigenvectors with eigenvalue 1, while $\frac{1}{\sqrt{2}}(|\,01\rangle - |\,10\rangle)$ is an eigenvectors with eigenvalue -1. If these eigenvectors are λ_i and $|\,v_i\rangle$, the square root can be found by taking

$$\sum_i \sqrt{\lambda_i}\,|\,v_i\rangle\,\langle v_i\,|,$$

which for one choice of square roots is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1+i) & \frac{1}{2}(1-i) & 0 \\ 0 & \frac{1}{2}(1-i) & \frac{1}{2}(1+i) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

3. **Part 1:** 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.

Solution: Let

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix};$$

this is σ_z applied to qubit 1 tensored with the identity on qubit 2. Let Q be the square root of SWAP gate found in the solutions to problem 2. Then it is easy to check that

$$PQPQ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Now, let Q_{12} be Q (on qubits 1 and 2) tensored with the identity on qubit 3, and $P_{3\to 1}$ be the controlled gate which applies σ_z to the first qubit when the third qubit is a $|\,0\rangle$, and the identity to the first qubit when the third qubit is a $|\,1\rangle$.

Then, $P_{3\to 1}Q_{12}P_{3\to 1}Q_{12}$ applies $PQPQ$ to the first two qubits when the third qubit is a $|\,0\rangle$, and SWAP to these two qubits when the third qubit is a $|\,1\rangle$. This is a Fredkin gate, albeit with the incorrect phase of i applied to the states $|\,010\rangle$ and $|\,100\rangle$.

3. **Part 2:** Show that there is an $8 \otimes 8$ diagonal unitary matrix which you can multipy by $\tilde{F}$ to produce a Fredkin gate.

Solution: No matter which states have incorrect phases, you can multiply the matrix by a diagonal matrix which changes the phase on the incorrect states. For example, in the solution above, we need to fix the phases on $|\,010\rangle$ and $|\,100\rangle$. the diagonal matrix with entries $1, 1, -i, 1, -i, 1, 1, 1$ does this.

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.

Solution: Let $\lambda_{b_1 b_2 b_3}$ be the diagonal entry corresponding to the bit string $b_1 b_2 b_3$ We will show that we can achieve any diagonal matrix that satisfies

$$\lambda_{000}\lambda_{011}\lambda_{101}\lambda_{110} = \lambda_{001}\lambda_{010}\lambda_{100}\lambda_{111}; \qquad (1)$$

that is, the product of the eigenvalues for even parity bit strings is equal to the product of the eigenvalues for odd parity bit strings.

We first show this equation must be satified. This is true because it is satisfied for all 2-qubit diagonal matrices. For example, suppose we have a diagonal matrix D which is a two-qubit gate for the first two qubits. Then

$$\begin{aligned} \lambda_{000} &= \lambda_{001}, & \lambda_{010} &= \lambda_{011}, \\ \lambda_{100} &= \lambda_{101}, & \lambda_{110} &= \lambda_{111}. \end{aligned}$$

so the equation above must be satisfied. Similar arguments apply to two-qubit gates which operate on the first and third qubits, and on the second and third qubits.

We now show that we can achieve a diagonal matrix with arbitrary values in the first seven diagonal places. Consider the product

$$\begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & b & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & c & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & d & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & b & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & c & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & e & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & f & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & e & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & f \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & g & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & g \end{pmatrix}$$

By choosing the appropriate values for a, b, c, d, e, f, g (for example, we need $e = \lambda_{100} a^{-1}$ and $g = \lambda_{110} e^{-1} c^{-1}$, we can produce arbitrary values for all of the first seven entries on the diagonal. The λ_{111} entry is determined by Eq. (1) above.

5. (Paraphrased.) Build a Fredkin gate using the gates from 3 and 4.

This problem was cancelled, as a sign error I made rendered it impossible. If you just have three qubits to work with, it is impossible to build a Fredkin gate out of two-qubit conservative quantum gates. The proof works as follows. Consider the following matrix.

$$\begin{pmatrix} E & & & & & & & \\ & O & O & & O & & & \\ & O & O & & O & & & \\ & & & E & & E & E & \\ & O & O & & O & & & \\ & & & E & & E & E & \\ & & & E & & E & E & \\ & & & & & & & O \end{pmatrix}$$

The indicated entries are the only ones allowed to be non-zero in a three-qubit conservative gate. I have divided them into E's and O's depending on the parity of the number of 1's in the states they act on. Consider the two 4×4 matrices M_E and M_O that contain the E entries and the O entries. For example, M_E contains the first, fourth, sixth and seventh rows and columns (corresponding to 000, 011, 101 and 110, respectively). For any three-qubit gate built out of two-qubit conservative gates, we must have that the determinants of M_E and M_O are equal. To prove this, we just need to show that this is true for any two-qubit conservative gate, as multiplying tow matrices multiplies their determinants as well. But one can check that for a two-qubit conservative gate, M_O can be obtained from M_E by applying the same permutation to the rows and columns, and this operation preserves the determinant.

A Fredkin gate has $\det M_O = 1$ and $\det M_E = -1$, and thus cannot be constructed from two-qubit conservative gates.

6. To build a Fredkin gate, one can use the construction in Problem 3 and the phase gates in problem 4 to produce a Fredkin gate that has the incorrect phase on any given entry and a $+1$ phase on the rest of them. These can then be used with a constant value of $|\,0\rangle$ or $|\,1\rangle$ in one of the three input qubits to produce AND, OR and NOT gates (which also produce junk outputs) which have phases of all $+1$. These can then be put together to produce a Fredkin gate. The junk generated by the AND, OR and NOT qubits can be eliminated by using the construction for classical reversible computation that gets rid of all the junk.

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:

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

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).

Solution: We want to implement the unitary transformation

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

Let's start by using the Chinese remainder theorem to take

$$|\,x \bmod pq\rangle \rightarrow |\,x \bmod p\rangle\,|\,x \bmod q\rangle\,.$$

The Chinese remainder theorem states that there is a 1-1 map between the left and right sides of the transformation above, and this transformation can be done reversibly and efficiently, since there is a classical algorithm both for this function and its inverse. We can now apply the Fourier transform to each of the registers, since we assume we have a Fourier transform circuit for both p and q

$$\begin{aligned} |\,x \bmod p\rangle\,|\,x \bmod q\rangle &\rightarrow \frac{1}{\sqrt{pq}} \sum_{y_1=0}^{p-1} \sum_{y_2=0}^{q-1} e^{2\pi i x y_1/p} e^{2\pi i x y_2/q}\,|\,y_1 \bmod p\rangle\,|\,y_2 \bmod q\rangle \\ &= \frac{1}{\sqrt{pq}} \sum_{y_1=0}^{p-1} \sum_{y_2=0}^{q-1} e^{2\pi i x (y_1 q + y_2 p)/pq}\,|\,y_1 \bmod p\rangle\,|\,y_2 \bmod q\rangle\,. \end{aligned}$$

Now, all we need to do is show that we can go reversibly from $|\,y_1 \bmod p\rangle\,|\,y_2 \bmod q\rangle$ to $|\,y_1 q + y_2 p \bmod pq\rangle$. This will let us obtain the state

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

since $|\,y_1 q + y_2 p \bmod pq\rangle$ ranges over all residues $y \bmod pq$. This can be done by first multiplying the first register by $q \bmod p$ and the second register by $p \bmod q$ to obtain $|\,y_1 q \bmod p\rangle\,|\,y_2 p \bmod q\rangle$. This can then be taken by the Chinese remainder theorem to $|\,y_1 q + y_2 p \bmod pq\rangle$.