2.111J/18.435J Quantum Computation Problem Set 1 Solutions
(Problem Set 1 Due Date: Tuesday, September 20, 2005)

1) Draw how to implement the NAND gate using a combination of capacitors, pFETs, and/or nFETs.

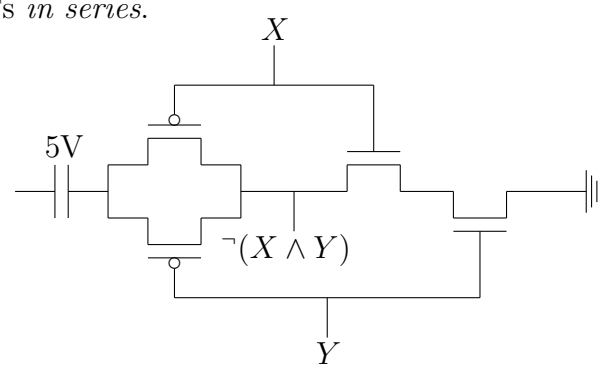
Notes: NAND is the Boolean logic gate which takes two binary inputs X and Y and outputs 0 if $X = Y = 1$ and otherwise outputs 1. Capacitors store bit values: 0 volts = "0" and +5 volts = "1". A pFET is a transistor switch which allows current to pass through it if there's 0 volts on its gate and does not allow current to pass through it if there is +5 volts on its gate. Conversely, a nFET is a transistor switch which allows current to pass through it if there is +5 volts on its gate and doesn't allow current to pass through it if there is 0 volts on its gate.

Solution: While the circuit is simple enough to be drawn just by trial and error, the guiding principle is this. *When the output capacitor is supposed to be charged at 5V and encoding a logical 1, it must be connected to the 5V voltage source and isolated from ground. Conversely, when it is supposed to be at 0V and encoding a logical 0, it must be connected to ground and isolated from the 5V voltage source.*

So let us now look at the truth table we want to implement:

NAND Truth Table		
X	Y	X NAND Y
0	0	1
0	1	1
1	0	1
1	1	0

Thus, so long as X and Y are not both 1, the output should be connected to the voltage source and isolated from ground. Conversely, only when $X = Y = 1$ should the output point be connected to ground and isolated from the voltage source. This suggests the output point should be connected to the voltage source by a two pFETs *in parallel* and connected to ground by two nFETs *in series*.



2) Verify that AND is a nonlinear gate.

Notes: In other words, verify that if we denote the inputs to AND by the letters X and Y,

then there does not exist any function of the form $aX + bY + c$ (a, b, c are constants) that reproduces the truth table of X AND Y.

Solution: Consider the following truth table

X AND Y versus $aX + bY + c$			
X	Y	X AND Y	$aX + bY + c$
0	0	0	c
0	1	0	$b + c$
1	0	0	$a + c$
1	1	1	$a + b + c$

Row 1 of the above table implies $c = 0$. Combined with row 2, this implies $b = 0$ as well. Combined with row 3, we have $a = 0$ too. This leads to a contradiction with row 4, as we now have $a + b + c = 0$ when we needed $a + b + c = 1$. Therefore, AND is not a linear gate.

---

3) Prove that all reversible gates with 2 inputs and 2 outputs are linear.

Notes: In other words, prove that any 2 input / 2 output gate that is reversible and has inputs X and Y must have outputs that are expressible in the form $aX + bY + c$ and $a'X + b'Y + c'$ where a, a', b, b', c, c' are constants.

Solution: For a 2 input / 2 output gate to be reversible it must be a bijective function (*i.e.*, 1-to-1 and onto) $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ where $\mathbb{Z}_2$ is the of bit strings of length 2, $\{(0,0), (0,1), (1,0), (1,1)\}$ to itself.

Now realize that a 2 input / 2 output gate with a linear input-output relation

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} a & b \\ a' & b' \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} c \\ c' \end{pmatrix}$$

will be reversible only if its matrix $\begin{pmatrix} a & b \\ a' & b' \end{pmatrix}$ is *invertible*.

Thus, the key question becomes: how many distinct reversible linear 2 input / 2 output gates are there? If this number equals the total number of reversible 2 input / 2 output gates of any type, then all reversible 2 input / 2 output gates are in fact linear.

Remembering that all our addition is integer addition mod 2, there's clearly 4 distinct possibilities for the vector $\begin{pmatrix} c \\ c' \end{pmatrix}$, namely

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

As for the matrix, invertibility demands a nonzero determinant: $ab' - a'b \neq 0$. This leaves 6 distinct possibilities, namely

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

Thus, we conclude there are 24 distinct, reversible linear 2 input / 2 output gates.

In comparison, the total number of 2 input / 2 output reversible gates of any type is simply the number of distinct permutations possible on a set of 4 elements as a function $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ must be a permutation of $\mathbb{Z}_2$ if it is to be bijective. This number is $4! = 24$.

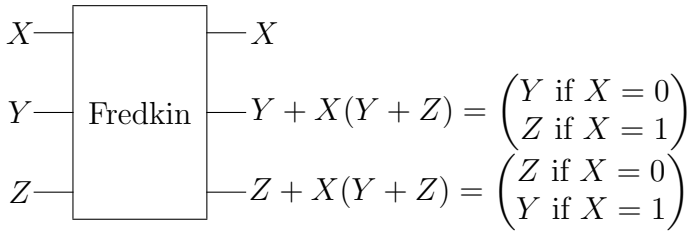
Therefore, the number of distinct, reversible linear 2 input / 2 output gates equals the number of distinct, reversible 2 input / 2 output gates of any type. All reversible 2 input / 2 output gates are linear.

---

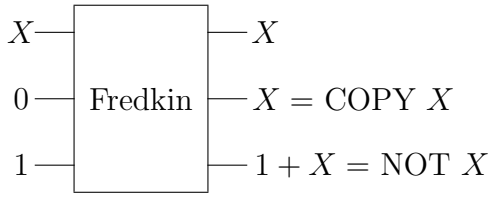
4) Prove that the Fredkin (controlled-SWAP) gate is universal by explicitly showing how to make AND, OR, NOT, and COPY gates out of one or more Fredkin gates.

Notes: The Fredkin (controlled-SWAP) gate is a gate that takes three inputs X, Y, and Z and produces three outputs X', Y', and Z' according to the rule that if $X = 0$ then it does nothing (*i.e.,* $X' = X, Y' = Y, Z' = Z$) and if $X = 1$ then it swaps Y and Z (*i.e.,* $X' = X, Y' = Z, Z' = Y$). In making AND, OR, NOT, and COPY, you are free to specify some gate inputs to be fixed values.

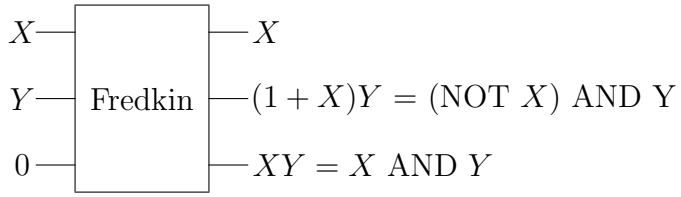
Solution: As it turns out that AND, OR, NOT, and COPY can all be made out of just one Fredkin gate, it is possible to find the answer simply by trial and error. However, it is illuminating, especially for more complicated problems, to write down explicit Boolean algebra formulas for the Fredkin gate. (NB: As usual, all addition is mod 2.)



Thus, setting $Y = 0$ and $Z = 1$ on the Fredkin gate will enact a COPY X at its middle output and a NOT X at its bottom output.



Setting $Z = 0$ on the Fredkin gate enacts X AND Y at its bottom output.



Finally, setting $Y = 1$ on the Fredkin gate enacts X OR Z at its bottom output.