Chapter 10 – Solutions

10.1 (a) Suppose $|\psi\rangle = (a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle)$. Equivalently, $|\psi\rangle = a_0 \cdot b_0|00\rangle + a_0 \cdot b_1|01\rangle + a_1 \cdot b_0|10\rangle + a_1 \cdot b_1|11\rangle$.
From this we conclude : $a_0 \cdot b_0 = \frac{1}{\sqrt{2}}$, $a_0 \cdot b_1 = a_1 \cdot b_0 = 0$, $a_1 \cdot b_1 = \frac{1}{\sqrt{2}}$
which implies that one of $a_0, b_1 = 0$ and also one of $a_1, b_0 = 0$ but then $a_0 \cdot b_0 = 0$ or $a_1 \cdot b_1 = 0$, which is a contradiction.

(b) $|0\rangle$ with probability 1/2 and $|1\rangle$ with probability 1/2.

(c) After measuring the first qubit, the second qubit will have the same value as the first one.

10.2 Denote by C the total unitary operation that the circuit preforms. Then

$$C|00\rangle = CNOT(H|0\rangle \otimes |0\rangle) = CNOT\left(\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes |0\rangle\right) = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

as required. Similarly, we get

$$C|10\rangle = CNOT(H|1\rangle \otimes |0\rangle) = CNOT\left(\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \otimes |0\rangle\right) = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

$$C|01\rangle = CNOT(H|0\rangle \otimes |1\rangle) = CNOT\left(\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes |1\rangle\right) = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

$$C|11\rangle = CNOT(H|1\rangle \otimes |1\rangle) = CNOT\left(\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \otimes |1\rangle\right) = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

10.3 By definition of the (classical) Fourier Transform, it is easy to see that $QFT\left(\frac{1}{\sqrt{M}}\sum_{j=0}^{M-1}|j\rangle\right) = |0\rangle$.

10.4 $QFT(|j\rangle) = \frac{1}{\sqrt{M}}\sum_{x=1}^{M}\omega^{x\cdot j}|x\rangle$, where $\omega = e^{\frac{2\pi i}{M}}$.

10.5 By the previous problem,

$$|\beta\rangle = QFT(|\alpha\rangle) = \sum_j \alpha_j \sum_x \omega^{x\cdot j}|x\rangle = \sum_x \left(\sum_j \alpha_j \omega^{x\cdot j}\right)|x\rangle$$

Also,

$$|\beta\rangle' = QFT(|\alpha\rangle') = \sum_j \alpha_j \sum_x \omega^{x\cdot(j+l)}|x\rangle = \sum_x \omega^{x\cdot l}\left(\sum_j \alpha_j \omega^{x\cdot j}\right)|x\rangle = \sum_x \omega^{l\cdot j}\beta_j|x\rangle$$

The rest follows since we know that the Fourier transform of the periodic vector $\sum_{j=0}^{M/k-1}\sqrt{\frac{k}{M}}|jk\rangle$ is $\sum_{j=0}^{k-1}\frac{1}{\sqrt{k}}|jM/k\rangle$.

10.6 Let C be the left circuit. We will examine what state does C produce for inputs the computational states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. We will do the calculations just for one of them, say $|01\rangle$. The rest follow similarly.
We first apply Hadamard gates to both qubits and get the state: $(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes (\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle) = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$. Then, we apply CNOT gate to get $\frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|11\rangle - \frac{1}{2}|10\rangle = (\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle) \otimes (\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle)$.
Finally, we apply Hadamard gates again to both qubits, and the final state is: $|11\rangle$. Observe that if we switch the control and target qubits of the CNOT gate (call that gate C'), we have $C'|01\rangle = |11\rangle$, as claimed.Similarly, we obtain $C'|00\rangle = C|00\rangle = |0\rangle 0, C'|10\rangle = C|10\rangle = |10\rangle, C'|11\rangle = C|11\rangle = |01\rangle$.

10.7 (a) For each of the gates, it is sufficient to argue about the behavior of the gates when applied to the basis states as it extends to a superposition state by linearity. Since the NOT gate maps a $|0\rangle$ to $|1\rangle$ and vice-versa, applying it twice brings $|0\rangle$ to $|0\rangle$ and $|1\rangle$ to $|1\rangle$ and hence $NOT(NOT(|x\rangle)) = |x\rangle$

For any basis state, the CNOT gate applies a NOT on the second qubit if the first qubit is 1. Since the first qubit is left unchanged, applying the gate twice restores the second qubit and hence the original state. Similarly, applying the C-SWAP gate twice does nothing if the first qubit is 0, and swaps the last two qubits twice if it is 1. In each case, we get back the original state.

(b) We give inputs a,b,0. We observe that is $a = 1$ then the third output qubit equals $a \wedge b = b$. If $a = 0$ then it equals $a \wedge b = 0$.

(c) We can easily verify that fan out can be achieved (at the first and second outputs) if we give input $a, 0, 1$ to the C-SWAP gate.

(d) The set of classical gates {AND,NOT} is universal for classical computation. In (b) and (c) we have shown that AND and fan out can be implemented by C-SWAP gates, which on input $|x, 0, 0\rangle$ outputs $|x, y, z\rangle$ (the desired output is at the second qubit and the last qubit contains some junk). Adding the NOT gate, we conclude that any classical circuit can be implemented using NOT and C-SWAP gates.

(e) As shown in (a) above, the C-SWAP and NOT gates are the reverses or themselves. Assume that $Q = G_1 G_2 \cdots G_k$, where G_i are either C-SWAP or NOT gates. Then, $Q^{-1} = G_k \cdots G_2 G_1$.

(f) We use some extra zeroes (denoted by w with $|w| = |y|$ and initialized to 0), which are not used by the circuit constructed in the previous parts. First apply Q to $|x, 0, 0, 0\rangle$ to get $|x, y, z, 0\rangle$. We can now apply a CNOT gate to each bit pair (y_i, w_i) using the bits of y as control bits. This gives the state $|x, y, z, y\rangle$. Finally, we apply Q^{-1} to get $|x, 0, 0, y\rangle$. Renumbering the outputs gives the desired state $|x, y, 0, 0\rangle$.

10.8 (a) Let r denote the order of x. From Fermat's Little Theorem, we know that $x^{p-1} = 1 \mod p$. It is well-known that the multiplicative group modulo a prime number is a cyclic group, so there exists an element g that generates all elements of the group, in the sense that every element x can be written $x = g^k \mod p$. Since x is uniformly random, the probability that k is odd is 1/2. Also, $g^{kr} = 1 \mod p$ and as $g^i \neq 1$ for any i between 1 and $p - 2$, we must have $p - 1|kr$. Since $p - 1$ is even, given that k is odd, r has to be even. This even happens with probability at least 1/2.

(b) By the Chinese Remainder Theorem, picking x uniformly mod$N$ is equivalent to picking $x_1 \mod p$ and $x_2 \mod q$. Let r_1, r_2 the order of x_1, x_2 respectively. Clearly, $r_1|r$ and $r_2|r$. Observe that r is even if either r_1 is even of r_2 is even. By (a) the probability of this event is at least 3/4.

(c) Let $x^{r/2} = \pm 1 \mod N$. Then $x^r = 1 \text{mod} p$ and $x^r = 1 \mod q$. There are only two square roots of 1 modulo a prime. By Chinese Remainder Theorem,there are only four square roots of 1 modulo N. Therefore $x^{r/2} = \pm 1 \mod N$ for only two of them,i.e. with probability at most 1/2.