Honors Theory, Spring 2002, Yap
Homework 8
(WITH SOLUTIONS

This last homework will not graded. Solution sketch will be published on Wed May 7.

Please read the lecture notes on the quantum factorization algorithm, and the provided number theory background.

NOTE: I have slightly debugged questions 1.

1. Consider classical reversible circuits to compute the following transformation: $f : \mathbb{B}^{2n} \to \mathbb{B}^{2n}$ where $f(x, y) = (x, yx \,\mathbf{mod}\, N)$ if $x, y \in \mathbb{Z}_N^*$ ($N = 2^n$), and $f(x, y) = (x, y)$ otherwise. Construct the circuit explicitly for the case $n = 3$ using the family of T_n gates.

   SOLUTION: Since $n = 3$ and $N = 8$, $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$. For most (x, y), $f(x, y) = (x, y)$, i.e., the transformation is trivial. Consider the nontrivial transformations of f.

   If $x = 3$, then we see that the second register is transformed according to the two transpositions: $1 \leftrightarrow 3$, and $5 \leftrightarrow 7$.

   If $x = 5$, then the second register is transformed according to the two transpositions: $1 \leftrightarrow 5$, and $3 \leftrightarrow 7$.

   If $x = 7$, then the second register is transformed according to the two transpositions: $1 \leftrightarrow 7$, and $3 \leftrightarrow 5$.

   We saw in class (problem session on Wednesday) how to do this for $x = 3$. Consider how to implement the $1 \leftrightarrow 3$ transposition: $|011, 001\rangle \leftrightarrow |011, 011\rangle$. Let the qubits be $|x_1x_2x_3, y_1y_2y_3\rangle$. We want a 6-input control-NOT (T_6) gate to flip y_2 iff the $x_1x_2x_3 = 011$ and $y_1y_3 = 01$. This is done is three stages:

   - First negate x_1 and y_1.
   - Then apply T_6 to flip y_2 (with all the other 5 lines as controls).
   - Finally, we negate x_1 and y_1 again (thus returning them to the original values).

   We leave it to you to draw the reversible circuit. It is clear that you can repeat this for each of the other transpositions.

2. Let $n = 3$ and $N = 2^3 = 8$. Suppose we prepare the state $|111\rangle$, and then apply Hadamard transform to each bit. Then we apply QFT to the result. What is the resulting state?

   SOLUTION: A bit tedious to carry this out. Note that $|x\rangle = H|111\rangle = \frac{1}{\sqrt{8}}(|0\rangle - |1\rangle)^{\otimes 3}$. One way is to apply the quantum circuit for QFT to this input.

   Alternatively, use the equation for $QFT(|x\rangle)$ as in the definition.

3. Let $N = 2^n$, m be an odd number less than N, and $x \in \mathbb{Z}_m^*$. We define a transformation on two quwords, each with n qubits. defined as follows: $U_{m,x}$ be

   $$U_{m,x}(|k\rangle|y\rangle) = |k\rangle|yx^k \bmod m\rangle.$$

   Here, we assume that $U_{m,x}(|k\rangle|y\rangle) = |k\rangle|y\rangle$ in case $y \geq m$.

   Let $|z\rangle = \frac{1}{\sqrt{N}} \sum_{\ell=0}^{N-1} |k\rangle|1\rangle$. To be specific, let $n = 4, m = 10, x = 3$. What is $U_{m,x}(|z\rangle)$? Suppose you measure the second quword, and obtain the result 1. What is the resulting state?

   SOLUTION:

$$\begin{aligned} U_{m,x}(|z\rangle) \quad &= \quad \frac{1}{\sqrt{16}}(\\ & |0,1\rangle + |1,3\rangle + |2,9\rangle + |3,7\rangle + \\ & |4,1\rangle + |5,3\rangle + |6,9\rangle + |7,7\rangle + \\ & |8,1\rangle + |9,3\rangle + |10,1\rangle + |11,1\rangle + \\ & |12,1\rangle + |13,1\rangle + |14,1\rangle + |15,1\rangle). \end{aligned}$$

You measure and get 1 in the second quword, the probability is 9/16, and the resulting state is

$$(|0,1\rangle + |4,1\rangle + |8,1\rangle + |10,1\rangle + |11,1\rangle + |12,1\rangle + |13,1\rangle + |14,1\rangle + |15,1\rangle)/3.$$

4. Integer Factorization: give a simple polynomial time algorithm to detect if an input integer N is a power or not. In case of a non-power, output its power factorization, namely $N = M^e$ for some $M, e \in \mathbb{N}$.

   SOLUTION: Assume N is an n-bit number. Note that e ranges from 2 to at most n. If you fix any e, then M has at most $m = \lfloor n/e \rfloor$ bits. We can determine each of the m bits of M, starting from the most significant bit: for instance if $M = (b_1 b_2 \cdots b_m)_2$, then we check if $b_1 = 1$ by computing T_1^e and comparing it to N. Here, $T_1 = (10\cdots 0)_2$ is a m-bit number. If this number is equal to N, we are done. If it is greater than N then b_1 must be 0. Otherwise, it must be 1. We continue to test for b_2 by considering $T_2 = (b_1 10\cdots 0)_2$, and comparing T_2^e against N. And so on. This is easily seen to take $O(n^4)$ time. Since we have to test for each e, the overall algorithm is $O(n^5)$.

   You can speed up this simple algorithm is you use fast FFT based multiplication, and exploit the fact that to test successive bits, you can reduce this to addition.

5. Find all the square roots of 1 modulo 45. Describe your method for finding them.
   NOTE: we want you to do your calculations by hand (not by writing a program to do it, for instance).
   SOLUTION:

   The squareroots of 1 modulo 45 are $\{1, -1 \equiv 44, 19, -19 \equiv 26\}$.

   METHOD: We start with $\mathbb{Z}_{45}^* = \{1, 2, 4, 7, \cdot 44\}$, and try to eliminate elements.

   One way is observe that if x is a squareroot of 1, then $x \,\mathbf{mod}\, 9$ and $x \,\mathbf{mod}\, 5$ must be ± 1.

   Another way is to note that $45|(x-1)(x+1)$ and therefore $3|(x-1)$ or $3|(x+1)$. Hence, x must be adjacent to 3. Similarly, we can observe that x must be adjacent to 5. Antonio notes

   When the list is small enough, you can just bruteforce check. It is useful to remember that you can operate modulo 45. For instance, to check 19 is a squareroot of 1, we compute $19^2 = (20-1)^2 = (400 - 40 + 1) = (-50 + 5 + 1) = 1(mod 45)$.

6. Let $x \in \mathbb{Z}_n^*$. If $h(x) = (g_1, \ldots, g_m)$ where each g_i is a generator and $2\ell = \mathtt{LCM}(\phi(q_1), \ldots, \phi(q_m))$. Characterize the conditions where $x^\ell \equiv -1 (\mathrm{mod}\, n)$.

   SOLUTION: Write $h(x^\ell) = (y_1, \ldots, y_m)$ where each $y_i \in \{\pm 1\}$. Hence we require $y_i = -1$ for all i. Since $\phi(q_i)|2\ell$ and $\phi(q_i) \nmid \ell$, we must have $\mathrm{v}_2(\phi(q_i)) = \mathrm{v}_2(2\ell)$. Thus $\mathrm{v}_2(\phi(q_i) = \mathrm{v}_2(\phi(q_j))$ for all $i, j = 1, \ldots, m$.

   EXTRA EXERCISES:

7. Consider the following linear equation:
   $$ax = b(\mathrm{mod}\, n)$$
   where $a, b \in \mathbb{Z}_n$ are given. We want to find $x \in \mathbb{Z}_n$. Let $d = \mathtt{GCD}(a, n)$.
   (i) The linear equation has a solution iff $d|b$.
   (ii) In case $d = 1$, the solution is unique and given by $x = ba^{-1} \,\mathbf{mod}\, n$.
   (iii) In case $d \geq 2$, there are exactly d solutions. Find these solutions. HINT: consider the "reduced equation" $a'x = b'(\mathrm{mod}\, n')$ where $a = a'd, b = b'd, n = n'd$.

   SOLUTION: This problem is a standard result in congruence arithmetic. Write $a = a'd, n = n'd$.

   (i) If $d|b$ then a solution is $b = b'd$. Then $ax = b(\mathrm{mod}\, n)$ is the same as $a'x = b'(\mathrm{mod}\, n')$. But then $x = b'(A)^{-1}$ is a solution where $Aa' = 1 \,\mathrm{mod}\, n'$ (so A is the inverse of a' mod n'). Conversely, if we have a solution $ax = b(\mathrm{mod}\, n)$ then $n|ax - b$. Since $d|n$ and $d|a$, it follows that $d|b$.

   (ii) This comes from the first part of the proof of (i).

   (iii) If x_0 is any solution, then so is $x_0 + in/d$ where $i = 1, \ldots, d-1$. These solutions are distinct.