QUANTUM COMPUTATION - FALL 2006 - EXERCISE 3

Due: Wednesday 27/12/06.

1. Fourier Transform

let a, b such that $a|q$ and $b|q$ and $\gcd(a,b) = 1$. Let $S = \{0 \leq x < q \text{ s.t. } a|x \text{ or } b|x\}$, and define the state

$$|\phi\rangle = \frac{1}{\sqrt{|S|}} \sum_{x \in S} |x\rangle .$$

What is the Fourier transform modulo q of $|\phi\rangle$?

2. More on Fourier Transform

Consider the FT over Z_{3^n}. Design a quantum circuit that works with qutrits (qubits with three states, $|0\rangle, |1\rangle, |2\rangle$) and recursively computes the FT over this group.

3. Fourier Transform and Convolution

Consider two functions, f and h, from the Abelian group modulo N to the complex numbers. Define a third function g, called the *convolution* of f and h, and denoted $g = f * h$, by

$$g(x) = f * h(x) = \sum_{y=0}^{N-1} f(y)h(x-y).$$

Denote by $\hat{f}$ the Fourier transform of f, i.e. $\hat{f} = FT_N \cdot f$. Prove that for every x it holds that

$$\hat{(f * h)}(x) = \hat{f}(x) \cdot \hat{h}(x).$$

4. The uncertainty Principle

The uncertainty principle, which we have all heard of, in fact means the following thing: Fix a quantum system in the state $|\psi\rangle$. Then the uncertainty principle means that we cannot predict with certainty the outcome of a measurement we will apply on $|\psi\rangle$ in one basis, and at the same time predict with certainty the outcome if we apply a measurement in the Fourier transform basis on the same $|\psi\rangle$. (the principle is in fact quantitive: it gives a lower bound on the product of the uncertainty in one basis times the uncertainty in the Fourier basis.)

(1) Give an example of the uncertainty principle in the context of measuring the state $|0\rangle$, in two different basis.
(2) Consider a superposition over all elements in some subgroup H of an Abelian group G. Consider the measurement of this state, in the computational basis and in the Fourier basis. Define the uncertainty in each measurement as the number of possible outcomes. Can you give a quantified version of the uncertainty principle in this context? (give the best lower bound possible, of course.)

5. Shor's Algorithm

A student suggested the following idea. In the presentation in class of Shor's algorithm, in the simple case (where r devided Q) we pick many random k's, $k_1, k_2, \ldots$, where we have $k_i = m_i Q/r$. We claimed that as long as one of the m_i's is coprime with r, we are OK. The student claimed that he knows what to do even if none of the m_i's are coprime with r, but just two of them are coprime to each other.

5.1. Complete the student's idea: give a way to find r if you are given two k's, such that the relevant m's are coprime with each other.

5.2. Show how to use this to make Shor's algorithm in the simple case more efficient, using the following known theorem: The probability for two independently chosen random numbers smaller than an integer n to be coprime converges to $\frac{6}{\pi^2}$ as n goes to infinity.

5.3. Can you use this idea in some way to improve the complexity of the general case of Shor's algorithm? Explain your thoughts. (This is more of an open discussion question.)

6. Grover's Algorithm

Suppose we are at the scenario of Grover's algorithm, with M marked items, and M is unknown. Design an algorithm that would find a marked item in $\tilde{O}(\sqrt{N/M})$ queries, with probability more than, say, one percent. Guidance: The value of M lies between 2^j and 2^{j+1} for some j. Show that if you knew j you could find the marked item with the correct probability, and then proceed to show what to do if you do not know j.