April 29, 2001.
To be submitted 9/5 in Jerusalem, 10/5 TA.

PROBLEM SET 3

1. Give an analysis of the size of the circuit given in class for Quantum Fast Fourier transform. How can you make the circuit more efficient, if we only want to approximate the FFT to within ϵ? Analyze the size of the circuit in this case.

2. Show how to construct a quantum circuit which computes the Fourier transform over the group Z_N, if $N = n_1 \cdot n_2 \cdots n_m$ using as subroutines circuits c_i which compute the FT over Z_{n_i}.

3. Let $a|q$, $b|q$. What is the FT modq of the uniform superposition over all $0 \leq x < q$ such that $a|x$ or $b|x$?

4. We will construct Kitaev's alternative order finding algorithm, which uses Kitaev's lemma. (This gives an alternative factorization algorithm). We are given N and a co-prime to N, and we are looking for a's order modulo N.

   (a) First, we need a slight improvement of the lemma we saw in class. We showed how to perform $|\phi\rangle \longmapsto |\phi\rangle|\theta\rangle$, where θ is the argument in ϕ's eigenvalue. There are two approximations in this transformation: One, theta itself was found only to within exponential accuracy. The other, that the transformation that we actually achieved was only exponentially close to the transformation which writes near $|\phi\rangle$ an excellent approximation of θ. It turns out that the first approximation (in theta) can be improved if we assume that the matrix U in the lemma is such that $U^s = I$ for some polynomially small s. Explain (in a few lines) how to achieve this.

   (b) We will work over the multiplicative group Z_N^*, consisting of all integers smaller than n and that are co-prime with it.

   (c) Show that the matrix U operating on the Hilbert space Z_N^*, which takes $|x\rangle \longmapsto |axmodN\rangle$ satisfies the requirements of the lemma. (There is a delicate point here of erasing the input: I do not mean the transformation $|x\rangle|0\rangle \longmapsto |x\rangle|axmodN\rangle$. But note that you can assume that $a^{-1}modN$ can be calculated efficiently using Euclid's algorithm.)

   (d) What are the eigenvectors and corresponding eigenvalues of this matrix?

   (e) Present the state $|1\rangle$ as a combination of eigenvectors of U.

   (f) Construct an algorithm to find the order of a, using the above building blocks, and Kitaev's lemma.

5. The discrete log is the following problem. We are given a prime p, g which generates the group Z_p^* and $x \in Z_p^*$. We are looking for r which satisfies $g^r = x \bmod p$.

   (a) Write the discrete logarithm as a hidden subgroup problem. (Hint: the function $f : Z_{p_1} \times Z_{p-1} \longmapsto Z_p^*$ is defined by $f(a,b) = x^a g^{-b}$.) What is the group, the subgroup; show that it is constant on cosets.

   (b) Show how to construct the discrete logarithm from the result of the final measurement in the quantum algorithm for the Hidden subgroup problem.