Homework 3
Due 2005/12/29

Oded Regev & Amnon Ta-Shma
Dept. of Computer Science
Tel Aviv University

1. The QFT circuit uses 2-qubit gates (the controlled-R$_k$ gates). Show that if we want to measure the state after the QFT circuit in the computational basis (as is done in Shor's algorithm), then the circuit can be modified to use only 1-qubit gates.

2. (a) Let $Q = \{0,1\}^n$ be the n-dimensional Hamming cube equipped with the Hamming distance d. Prove that there exists a subset $C \subseteq Q$ such that for any $x, y \in C$, $x \neq y$, we have $d(x, y) \in [0.4n, 0.6n]$ and whose size is at least 2^{cn} for some constant c. Hint: what is the relative volume of a Hamming ball of radius $0.4n$?

   (b) Prove that there exists a set of 2^{cn} unit vectors in $\mathbb{R}^n$ such that the inner product between any two different vectors is at most 0.2 in absolute value.

   (c) Describe a way to 'encode' any classical string x of length k bits into a quantum state $|\psi_x\rangle$ on $O(\log k)$ qubits with the following property: there exists a quantum circuit that given any two encodings $|\psi_{x_1}\rangle$, $|\psi_{x_2}\rangle$, decides with confidence greater than, say, 80% whether $x_1 = x_2$ or not.

3. A (simple, undirected) graph G on the vertex set $\{1, \ldots, n\}$ can be represented by an $\binom{n}{2}$-long bit-string by indicating for each $1 \leq i < j \leq n$ whether $\{i, j\}$ is an edge in G or not. We write $|G\rangle$ for the $\binom{n}{2}$-qubit state that corresponds to this representation. Let S_n be the group of all $n!$ permutations on n elements (the *symmetric group*). Define $\pi(G)$ as the graph obtained from G by renaming each vertex v to $\pi(v)$. In other words, $\{i, j\}$ is an edge in G iff $\{\pi(i), \pi(j)\}$ is an edge in $\pi(G)$.

   (a) Given a graph G, show how to create the state $(n!)^{-1/2} \sum_{\pi \in S_n} |\pi, \pi(G)\rangle$. You may assume that there is a representation of a permutation using $\lceil \log n! \rceil$ bits in which the first $n!$ bit strings are legal. Moreover, you may assume that there exists a classical circuit that computes $\pi(i)$ given i and the representation of π.

   (b) Assume that one has a way to generate the state $\sum_{\pi \in S_n} |\pi(G)\rangle$ (after normalization) given any graph G. Show that this would imply a solution to the graph isomorphism problem (i.e., given two graphs G and H, determine if they are isomorphic or not).

4. We say that a matrix H is *Hermitian* if it satisfies $H^\dagger = H$ (this is the analogue of symmetric matrices). We say that H is *positive semidefinite* if it is Hermitian, and, moreover, all its eigenvalues are non-negative. Prove that the following are equivalent:

   (a) H is positive semidefinite.

   (b) For any vector $|\varphi\rangle$, $\langle\varphi|H|\varphi\rangle$ is (real and) non-negative.

   (c) There is a matrix B of the same dimensions such that $H = B^\dagger B$.

5. Often, quantum gates cannot be implemented precisely. Let us define the distance between two unitaries U and V as

$$E(U, V) = \max_{|v\rangle, \||v\rangle\|=1} \|(U - V)|v\rangle\|.$$

(a) Show that this measure is sub-additive, i.e., prove that

$$E(U_1U_2, V_1V_2) \leq E(U_1, V_1) + E(U_2, V_2)$$

holds for any four unitaries U_1, U_2, V_1, V_2.

(b) Show how to construct a circuit that approximates the QFT on $\mathbb{Z}_{2^n}$ to within $1/p(n)$ for an arbitrary polynomial $p(n)$ using only $O(n \log n)$ gates (recall that in the original circuit we have $O(n^2)$ gates). Hint: most R_k are close to the identity

(c) Prove that the circuit you found can be used in Shor's factoring algorithm.