Exercise Sheet 7

Quantum Information

To be returned no later than June 11, 2015

(20 points) **Problem 1: Bernstein-Vazirani problem.**
This is a variation of the Deutsch-Jozsa problem. Suppose that the quantum black box computes one of the functions f_a, where $f_a(x) = a \cdot x$ and a is an n-bit string. Our job is to determinate a. Show that Deutsch-Jozsa algorithm can solve this problem, i.e. can find the n-bit string a with probability one.

(20 points) **Problem 2: Simon's algorithm**
In order to conclude Simon's algorithm we need to find $n-1$ non-trivial ($y \neq 0$), linearly independent strings y such that $y \cdot s = 0$. There are 2^{n-1} strings such that $y \cdot s = 0$. Suppose we choose N strings successively $y_1, \ldots, y_N$. Calculate the probability that these strings are linearly independent. Estimate this probability for $N = n - 1$.
Now, repeat the entire algorithm $4m$ times. Estimate the probability of not finding a linearly independent set during one of the iterations.
If the exercise is done correctly, you can see that for any constant $\epsilon > 0$, Simon's algorithm can solve the problem with error probability at most ϵ using $O(n)$ queries to the black-box.

(20 points) **Problem 3: Grover algorithm.**
Consider the search problem of finding x_0 such that $f(x_0) = 1$ for some function $f(x) \in \{0, 1\}$. In the lecture we constructed Grover algorithm that finds such x_0 assuming that it is unique. Now assume that there are $r > 1$ solutions to the equation $f(x) = 1$. In other words, suppose that we have N states and r of them are marked. The problem is to find one of the marked states with high probability.

The multiple solutions Grover algorithm is very similar to the unique solution one, except that the oracle induces a reflection about a different vector. Find the the action of the oracle for the function f. Also find the proper vectors $|\alpha\rangle$ and $|\beta\rangle$.

Write out step-by-step Grover algorithm, estimate the number of necessarily iterations and show that the probability of finding one of the marked state is close to one after these iterations.

(20 points) **Problem 4: n-fold Toffoli gate.**
The implementation of the rotation in Grover algorithm involves n-fold Toffoli gate. Find a circuit family with two $n-1$-fold Toffoli gates and two regular 3-fold Toffoli gates that implement n-fold Toffoli gate using one ancillary qubit.

Decomposing every gate into 3-fold Toffoli gates, how many 3-fold Toffoli gates do you need to construct n-fold one using one ancillary line?

(20 points) **Problem 5: n-fold Toffoli gate - more effective construction.**
Note that in the last exercise using more ancillary qubits allows us to use exponentially less 3-fold Toffoli gates. Find a circuit family with $2n - 5$ 3-fold Toffoli gates that evaluates n-fold Toffoli gate. (Here $n - 3$ ancillary qubits are used, which are set to 0 at the beginning of the computation and return to the value 0 at the end.)