Introduction to Quantum Computation
Master's Programme in Mathematics and Statistics
Fall 2018
Exercise set 6

Exercise 1. Suppose we apply Grover's algorithm (see previous exercise set) to a 3 qubit register, assuming there is exactly one solution to the search problem. What is the probability of measuring the solution state after applying the Grover iterate (i.e. the operator DO 0,1,2,3 times?

Exercise 2. In showing the optimality of Grover's search, we compared the states $\left|\psi_x^k\right\rangle$ and $|\psi_k\rangle$ that result from the start state $|\psi\rangle$ by either applying k oracle calls (and some unitary operators in between) or omitting the oracle calls:

$$\begin{aligned}\left|\psi_x^k\right\rangle =& U_k O_x U_{k-1} O_x \dots U_1 O_x U_0 \left|\psi\right\rangle, \\ |\psi_k\rangle =& U_k U_{k-1} \dots U_1 U_0 \left|\psi\right\rangle.\end{aligned}$$

Let $F_k = \sum_x \| |x\rangle - |\psi_k\rangle \|^2$, where x runs over all N many basic states. Show that $F_k \geq 2N - 2\sqrt{N}$.

Shor's factoring algorithm for input a composite N is:

(a) If N is even, return 2.
(b) If $N = a^b$, return a.
(c) Randomly choose x in the range 1 to $N-1$. If $\gcd(x, N) > 1$ then return the factor $\gcd(x, N)$.
(d) Use the order-finding subroutine to find the order r of x modulo N.
(e) If r is even and $x^{r/2} \neq -1 \pmod N$, compute $\gcd(x^{r/2} - 1, N)$ and $\gcd(x^{r/2} + 1, N)$ to find a nontrivial factor of N and return that factor. Otherwise return 'FAIL'.

Exercise 3. What is the smallest N for which the order-finding subroutine is used in Shor's algorithm and why?

Exercise 4. Factor 91 using Shor's algorithm (but calculate all subroutines e.g. using a classical calculator).