CS 190/264: Quantum Computation *Instructor: Sandy Irani*

Homework 6

Due: November 21, 2018, 2PM

Note: The assignment for undergraduates and graduate students is the same this week.

1. The algorithm that uses order finding to factor must eliminate the possibility that $N = p^\alpha$, where p is prime. If $\alpha = 1$, then N is prime and can not be factored. If $N = x^\alpha$, for any integers x and α, where $\alpha > 1$ and $x > 1$, then x is a non-trivial factor of N.

   (a) If $N = x^\alpha$, for any integers x and α, where $\alpha > 1$ and $x > 1$, then what is the largest that α could possibly be?

   (b) Give a classical algorithm to determine if an input integer N is equal to x^α, where x and α are integers larger than 1. If n is the number of bits to specify N, then your algorithm should run in time at most polynomial in n. You can **only** use addition and multiplication operations as well as the fast exponentiation algorithm presented in class. However, since we are not taking the results mod N, if you are calculating x^y, you need to make sure that the result is not too large. In other words, you should only comput x^y if you are sure that the number of bits required to specify x^y is polynomial in n.

2. Suppose that $a = 1276$, $N = 1875$, and $Q = 2048$. Suppose you know that k and r are relatively prime and are both less than N. Furthermore,

$$\left| \frac{a}{N} - \frac{k}{r} \right| \leq \frac{1}{2Q}.$$

   Use continued fractions to derive a set of candidates for k and r. You can write a program to do this if you like, but don't use any online calculators for continued fractions. I did this one by hand with a calculator.

3. Consider the Order Finding Algorithm for $N = 12$, $x = 5$, and $Q = 16$.

   (a) What is the current state of the algorithm after step 3? The state after step 3 is:

$$\frac{1}{\sqrt{Q}} \sum_{y=0}^{Q-1} |y\rangle |x^y \bmod N\rangle.$$

   You need to express this state using the specific values of N, x,and Q given above. Since this may be a bit tedious to do by hand, you are welcome to write a program to do the calculation for you.

   (b) If the second register is measured, then what are the possible outcomes?

(c) Suppose you measure the second register and the outcome is the largest of all the possible outcomes. Then what is the state after measurement?

4. $N = 337123$, and $x = 29680$.

(a) Verify that x is a square root of 1 mod N. You can use a calculator, but write down in your solution the condition you are checking.

(b) Use x to factor N. Show enough work to indicate that you know how to apply the algorithm to factor N. You can use a gcd calculator if you like.