Homework 8

Introduction to Quantum Information Science
Due Monday, April 10th at 11:59 PM

1. The Birthday Paradox. Your favorite local radio station is running a new give-away contest that works as follows: Each day at 5pm the phone lines open up to the public to call in and leave their name and birth-date which is then added to a running list. The contest runs until a matching birth-date (month and date) between any two contestants on the list is found. At that point the contest closes and everyone on the list up to that point is a winner. Assume that it is equally likely to be born on every day of the year and that no contestants are born during a leap year (so that we can ignore Feb. 29^{th}).

You are free to use numerical software of your choice to help solve the problem.

a) What is the minimum number of people who need to call in before the probability of a match being found is at least 50%?

b) How about the minimum number of people needed before there is a 99% chance of the contest coming to a close?

Imagine after running the contest for a few days the station decides they aren't being generous enough and so change the rules as follows: Instead of the contest ending as soon as there's a match found between any two contestants on the list it now ends when a match is found between specifically the first caller of the day and any other contestant.

c) Under these new rules what is the minimum number of people needed before there is a 50% chance of the contest closing? How about for a 99% chance?

2. Some useful notes on Shor's algorithm are available here: `https://people.eecs.berkeley.edu/~vazirani/f04quantum/notes/lec9.pdf`. In this problem, we'll work through the use of Shor's algorithm to factor $N = 21$ into $p = 3$ and $q = 7$.

a) List the elements of the multiplicative group mod N. How many are there?

b) Calculate the order of each element x within the multiplicative group (that is, the least s such that $x^s = 1 \pmod{N}$). Which fraction of the x's have even order?

c) For each x that has even order s, calculate both $x^{s/2} - 1$ and $x^{s/2} + 1$. Among the x's that have even order, for what fraction of them is neither $x^{s/2} - 1$ nor $x^{s/2} + 1$ an integer multiple of N?

d) Pick an x that survives the tests in (b) and (c). Show how, by calculating $\gcd(x^{s/2}-1, N)$ and $\gcd(x^{s/2}+1, N)$, we can recover the prime factors of N.

e) Pick an x that survives the tests in (b) and (c), and whose order is not a power of 2.

Let $f(r) = x^r \pmod{N}$, and let $Q = 512$. Consider the state:

$$\frac{1}{\sqrt{Q}} \sum_{r=0}^{Q-1} |r\rangle \, |f(r)\rangle$$

Write out enough terms in this state that one can see the periodicity of f (you need not write out all 512 terms!).

f) Write down one possible state $|\psi\rangle$ of the $|r\rangle$ register of the above state, after the $|f(r)\rangle$ register has been measured. Again, you need not write out all the terms; use of an ellipsis is fine.

g) Suppose the Quantum Fourier Transform F_Q is applied to $|\psi\rangle$, and then the result is measured in the computational basis. Pick some y that's the nearest integer to an integer multiple of Q/s. Calculate the probability that $|y\rangle$ is observed when $F_Q \, |\psi\rangle$ is measured. Next, pick some z that's not the nearest integer to an integer multiple of Q/s. Calculate the probability that $|z\rangle$ is observed when $F_Q \, |\psi\rangle$ is measured.

h) Pick two different y's that are the nearest integers to some integer multiple of Q/s (a different multiple for each y). For each one, show how the continued fraction algorithm can be used to recover either the period s, or partial information about s, given y together with N.

3.

a) What can go wrong in Shor's algorithm if Q is not taken to be sufficiently large? Illustrate with an example.

b) What can go wrong if the function, f, satisfies $f(p) = f(q)$ if s divides $p - q$, but it's not an "if and only if" (i.e., we could have $f(p) = f(q)$ even when s doesn't divide $p - q$)? Note that this does not actually happen for the function in Shor's algorithm, but it could happen when attempting period finding on an arbitrary function. Illustrate with an example.

c) What can go wrong in Shor's algorithm if the integer N to be factored is even (that is, one of the prime factors, p and q, is equal to 2)? Illustrate with an example.