March 2, 2006

Physics 681-481; CS 483: Assignment #4

(please hand in after the lecture, Thursday, March 16th)

I. Probabilities for solving Simon's problem.

As described on pages 16-18 of Chapter 2, to estimate how many times a quantum computer has to invoke the subroutine $\mathbf{U}_f$ to solve Simon's problem, we must answer a purely mathematical question. We have an n-dimensional space of vectors whose components are either 0 or 1, on which vector addition and inner products are both carried out with modulo 2 arithmetic. We are interested in the $(n-1)$-dimensional subspace of vectors orthogonal to a given vector a. We have a quantum computer program that gives us a random vector y in that subspace. If we run the program $n+x$ times, what is the probability q that $n-1$ of the vectors y will be linearly independent? I argue in Chapter 2 that

$$q = \Big(1 - \frac{1}{2^{2+x}}\Big)\Big(1 - \frac{1}{2^{3+x}}\Big)\cdots\Big(1 - \frac{1}{2^{n+x}}\Big). \tag{1}$$

Consider the case $n = 3$, $x = 1$, and $a = 111$. There are 4 different y's (including $y = 0$) that satisfy $a\cdot y = 0$, and therefore in four runs the quantum computer can produce $4^4 = 256$ equally likely quartets of such y's. Confirm that (1) is correct by explicitly enumerating all of the 256 sets of four y's that fail to contain at least two linearly independent vectors.

II. Defeating RSA encryption with period finding.

Here we examine RSA encryption and how it can be defeated by an efficient period-finding program, by working everything out in a particular case. The notation and terminology are that of Sections A and B of Chapter III. You will not get a feeling for what is involved if you use a computer or calculator. I did it all with pen and paper while eating breakfast.

(a) The two numbers Bob announces publicly are $N = 55$ and $c = 17$. Let Alice's message a be 9. What number between 1 and 54 is Alice's encrypted message $b = a^c$ (mod 55)? Do not ask your calculator or computer to tell you the answer. Noting that 17 in binary is 10001, you can work it out efficiently by listing the square of 9 modulo 55, the square of that number, etc. Your write-up should list the values of all the powers of 9 modulo 55 that you had to calculate to construct b. (I found it simpler to express a few of them as negative numbers modulo 55.)

(b) Since you have in your head the computational resources needed to find the prime factors of 55, you are in a position to find Bob's decoding number d. What is it? (I got it using the Euclidean algorithem as described in Appendix A2 of Chapter 3.) Confirm that $b^d = a \pmod{55}$, by the same process of successively squaring that you used in (a).

(c) Eve, listening in to the public communication picks up Bob's publicly announced $N = 55$ and $c = 17$ as well as Alice's encoded message b. Using her quantum computer she calculates the period r of b modulo N. What is r? Although you lack a quantum computer you can factor N in your head, and therefore know the order of G_N. Since r must divide that order there are not very many possibilities to examine.

(d) Find the inverse, d' of c modulo r. (This turned out to be so simple that I didn't need the Euclidean algorithm.) Confirm that $b^{d'} \equiv a(\text{mod } 55)$.