Physics 84
Homework 4
3/2/17

1, 2, 3

1. What N Are Easy to Factor?

Consider the n-qubit state

$$\hat{U}_{FT}\big|\Phi_c\big\rangle = \frac{1}{\sqrt{m2^n}} \sum_{y=0}^{2^n-1} e^{i2\pi y x_c/2^n} \Big(\sum_{\ell=0}^{m-1} e^{i2\pi y \ell r/2^n} \Big) \big|y\big\rangle$$

obtained in the quantum period-finding algorithm. We have seen in class that, if $2^n/r$ is an integer, measuring this state in the computational basis will yield some value $y = h2^n/r$ with essentially unit probability. Therefore, the quantum factoring algorithm is particularly simple and successful in the case $r = 2^j$, where r is the order of a modulo N. As a consequence of *Fermat's little theorem*, a number-theoretic result we will not prove here, the order of every a modulo N is of the form $r = 2^j$ whenever N is the product of two primes $p = 2^n + 1$ and $q = 2^m + 1$.

(a) What are the smallest four *odd* prime numbers of the form $2^n + 1$?

(b) What are the smallest four *odd* values of $N = pq$ that are "easier than average" for a quantum computer to factor because of this special case? If you see papers in which a quantum apparatus has factored one of these N's, be aware that the task does not quite reach the difficulty of the general factoring problem.

(c) For the smallest N you identified in part (b) above, verify that r is of the form 2^j for every choice of $a < N$ with $\gcd(a, N) = 1$.

■

2. Eigenstates and Eigenvalues of Modular Multiplication
Consider the unitary operator $\hat{U}$ which acts on n-qubit computational basis states $\big|w\big\rangle$ via $\hat{U}\big|w\big\rangle = \big|aw \pmod N\big\rangle$ for integers N and $a < N$. Let r be the (unknown) order of a modulo N.

(a) Show that the states $\big|u_h\big\rangle$ are eigenstates of $\hat{U}$, where

$$\big|u_h\big\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} exp\Big[\frac{-i2\pi hk}{r}\Big]\big|a^k \pmod N\big\rangle.$$

(b) Find the eigenvalue associated with $\big|u_h\big\rangle$.

(c) Show that

$$\frac{1}{\sqrt{r}}\sum_{h=0}^{r-1}\big|u_h\big\rangle = \big|\mathbf{1}\big\rangle = \big|0...01\big\rangle.$$

Coupled with the discussion in your reading, these facts explain how the order-finding algorithm can be thought of as a phase-estimation algorithm for $\hat{U}$.

■

3. 2-Qubit Quantum Fourier Transform

(a) Design and draw a circuit that accomplishes the two-qubit quantum Fourier transform using only Hadamard, controlled-S, and/or CNOT gates. (Recall that $\hat{S} = \hat{T}^2$.)

(b) Write the matrix representation of the two-qubit quantum Fourier transform in the standard two-qubit computational basis.

■