33-658, 758 Quantum Computation and Information Spring Semester, 2014
Assignment No. 8. Due Tuesday, March 18 (Revised)

ANNOUNCEMENT. There will be no classes on March 11 and 13, as this is CMU spring break.

NOTICE: This course has no final exam. In place of that you are required to write a term paper on the topic of your choice, as long as the instructor approves it. It is always best to write about some subject that interests you. Aim for 20 to 25 double-spaced pages (5000 to 6000 words, 40,000 to 50,000 characters). One possibility is to survey in your own words the material in a small set of preprints or papers, or even a single paper if it is sufficiently significant. Material in QCQI that is not being covered in the course is appropriate for a term paper. Some possibilities for titles are listed below, including some used by students in past courses. You can also get ideas by looking at articles in the Phys. Rev. A section on quantum information, or go to http://arxiv.org/ and look in the Quantum Physics (quant-ph) section.

Adiabatic Quantum Computation
Classical Simulation of Quantum Algorithms
Entanglement Distillation
Graph Isomorphism Using Quantum Methods
Hidden Subgroup Problem
Josephson Junctions for Quantum Computation
Optical Lattices for Quantum Information Procesing
Quantum Complexity Classes
Quantum Information in a Black Hole
Quantum Information Processing Using Nitrogen Vacacncy Defects in Diamond
Quantum Random Walks
Quantum Search Algorithms
Quantum Computation Using Optics
Security Issues in Quantum Key Distribution

READING:
MERMIN = N. D. Mermin, Quantum Computer Science (Library reserve)
PITTENGER = A. O. Pittenger, An Introduction to Quantum Computing Algorithms (Library reserve)
QCKOP = “Quantum Channels, Kraus Operators, POVMs” on course web page
QCQI = Nielsen and Chuang, Quantum Computation and Quantum Information

Shor factoring: QCQI Ch. 5 (not too easy); MERMIN, Ch. 3; PITTENGER, Secs. 3.4 to 3.7; E. Gerjuoy, Am. J. Phys. 73 (2005) 521; “Shor Factorization Algorithm”

Quantum Fourier transform: QCQI Sec. 5.1

Modular exponentiation circuit: QCQI Sec. 5.2 (Has a lot more material than we can cover in class); MERMIN Sec. 3.8; PITTENGER Secs. 3.4 to 3.7

Grover search algorithm: QCQI Sec. 6.1; PITTENGER Sec. 3.3

READING AHEAD:
Quantum channels/operations: QCQI Secs. 8.1, 8.2, 8.3; QCKOP

EXERCISES:

1. Turn in at most one page, and not less than half a page, indicating what you have read, examples or exercises (apart from those assigned below) that you worked out, difficulties you encountered, questions that came to mind, etc. You may include complaints about the course. **Provide a *tentative* topic for the term paper due at the end of the course. You are welcome to add some explanatory comments. A later assignment will ask for an abstract.**

1b. Only for students enrolled in 33-758: Summarize in half a page to a page what you learned from the most recent seminar.

2. This exercise concerns some general features of Shor's factoring algorithm, and then explores how the number of qubits m in the argument register influences what one learns about the period r in the case of $f(x) := 2^x \bmod 21$, and how the value of r can be extracted using continued fractions.

a) Suppose that $f(x)$, $0 \le x \le M-1$, $M = 2^m$, has period r. In general the state on the two registers A and B after the function evaluation step (F gate) can be written as

$$|\Psi_2\rangle = \sum_{\bar{x}=0}^{r-1} |\Phi_{\bar{x}}\rangle \otimes |f(\bar{x})\rangle; \quad |\Phi_{\bar{x}}\rangle = \frac{1}{\sqrt{M}} \big\{ |\bar{x}\rangle + |\bar{x}+r\rangle + \cdots |\bar{x} + (\mu_{\bar{x}} - 1)r\rangle \big\}.$$

Show that applying the quantum Fourier transform Q to $|\Phi_{\bar{x}}\rangle$ yields $Q|\Phi_{\bar{x}}\rangle = \sum_v c_{\bar{x}}(v)|v\rangle$ with

$$c_{\bar{x}}(v) = \frac{e^{2\pi i \bar{x} v/M}}{M} \times \begin{cases} \mu_{\bar{x}} & \text{if } rv/M \text{ is an integer,} \\ \left(\dfrac{1 - \exp[2\pi i \mu_{\bar{x}} rv/M]}{1 - \exp[2\pi i rv/M]} \right) & \text{otherwise.} \end{cases}$$

b) Use this to argue that if after the Fourier transform the argument register is measured, the probability $\Pr(v)$ of an outcome $0 \le v \le M-1$ is a sum of terms of the form

$$g_M(v,\mu,r) := \begin{cases} \mu^2 & rv/M = \text{integer} \\ \dfrac{\sin^2(\pi\mu rv/M)}{\sin^2(\pi rv/M)} & vr/M \ne \text{integer.} \end{cases}$$

multiplied by appropriate constants. (You may want to first work out the specific example in (c) below before considering the general case.)

c) ($m = 4$) Now consider $f(x) = 2^x \bmod 21$ and suppose that $m = 4$. Provide explicit expressions for $|\Phi_{\bar{x}}\rangle$ for $x = 0, 1, 2, \dots r-1$ and find $\mu_{\bar{x}}$ for each case. Plot $\Pr(v)$ as a function of $v = 0, 1, \dots (2^m - 1)$, preferably in the form of a bar graph or histogram. Use a software package (such as MAPLE or MATHEMATICA) to do the plotting.

d) ($m = 5$) Repeat part (c) for $m = 5$. The expressions for $|\Phi_{\bar{x}}\rangle$ can be written using only the first two and then the last computatonal basis states, $|a\rangle + |b\rangle + \cdots |c\rangle$.

e) ($m = 5$) Use the results of part (d) to provide the values of v at which the probability of measurement is peaked. For each such v use the continued fractions algorithm to determine the nearest fraction k/r' where $0 \le k < r' \le 20$ to $v/2^m$. Indicate whether the resulting r' is correct or not.

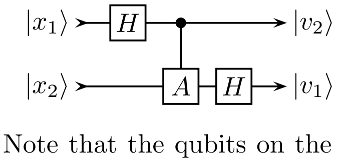
f) ($m = 6$) Repeat the above for $m = 6$.

3. a) Work out the quantum Fourier transform (QFT)

$$\sqrt{M}\, Q|x\rangle = \sum_{v=0}^{M-1} e^{2\pi i x v/M} |v\rangle$$

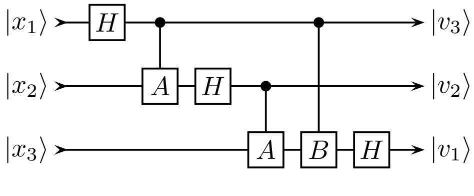
explicitly in the case $M = 4$, for $x = 0$, 1, 2, and 3, where with a bit representation $x = x_1 x_2$, $|x\rangle = |x_1\rangle \otimes |x_2\rangle$; and the same convention for v and $|v\rangle$. Show that for each x it is the case that $Q|x\rangle$ is a tensor product on the space of the two v qubits. You may want to compare your answer to Eq. (5.4) in QCQI.

b) Show that the QFT for $m = 2$ qubits, $M = 2^2 = 4$, can be carried out using the circuit



with a suitable choice of the gate A. Note that the qubits on the right side, with the most significant bit (v_1) on the bottom, are in the reverse order to those on the left: Hint: Take a look at the circuit in Fig. 5.1 of QCQI.

c)A similar circuit for the QFT of 3 qubits has the form



where A is the same gate as in (b). What is B? Give some reason(s) for your answer.