33-658, 758 Quantum Computation and Information Spring Semester, 2014
Assignment No. 7. Due Tuesday, March 4

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

READING:

BLUM = "Classical Algorithms", lectures by Avrim Blum, Course web site
CLRS = Cormen, Leiserson, Rivest, and Stein, Introduction to Algorithms (Library reserve)
DPV = Dasgupta, Papadimitriou, and Vazirani. Algorithms (Library reserve)
MERMIN = N. D. Mermin, Quantum Computer Science (Library reserve)
PITTENGER = A. O. Pittenger, An Introduction to Quantum Computing Algorithms (Library reserve)
QCQI = Nielsen and Chuang, Quantum Computation and Quantum Information

Number-theoretic algorithms: CLRS Ch. 31; DPV Ch. 1; QCQI App. 4; BLUM
Complexity theory: CLRS Ch. 34; DPV Ch. 8; QCQI Ch. 3; BLUM
Public key cryptography (RSA): QCQI App. 5. A helpful summary of the associated number theory concepts will be found in QCQI App. 4. Stinson, *Cryptography: theory and practice*, Ch. 4.
Deutsch-Jozsa algorithm: QCQI Sec. 1.4; MERMIN Ch. 2; PITTENGER Sec. 3.1
Simon's algorithm: MERMIN Ch. 2; PITTENGER Sec. 3.2
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

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.

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. Compute the modular exponential $11^{491} \bmod 13$ using the scheme described in box 5.2 of QCQI (p. 228). Do the calculation by hand (or use at most a pocket calculator) and show all the steps: it is considerably easier than it may appear at first.

3. Compute the RSA decryption key for $p = 11$, $q = 17$, and encryption key $e = 3$ (or, in Mermin's notation, $c = 3$). Then use it to encrypt the message 1001001 (= 73), and check your decryption key by decrypting the result. Be sure and indicate what procedures you followed to obtain your answer, even though you need not show all intermediate results.

4. QCQI p. 144, Exercise 3.19, as corrected at www.squint.org/qci/. The REACHABILITY problem is to determine whether there is a path between two specified vertices in a graph. Show that REACHABILITY can be solved in $O(n^2)$ operations if the graph has n vertices. Use the solution of REACHABILITY to show that it is possible to decide whether a graph is connected in $O(n^3)$ operations. (Assume graphs are undirected, and that no more than one edge joins any pair of vertices.)

5. a) Show that the following functions ($x_j = 0$ or 1, $\oplus$ is addition mod 2) are balanced:

$$\text{i)} \quad f(x_3, x_2, x_1) = x_1$$
$$\text{ii)} \quad f(x_3, x_2, x_1) = x_3 x_2 \oplus x_1$$

b) For each f in (a) construct a circuit consisting entirely of controlled-not and Tofolli gates which will implement the function evaluation step

$$U_f\big(|x_3 x_2 x_1\rangle \otimes |y\rangle\big) = |x_3 x_2 x_1\rangle \otimes |y \oplus f(x_3, x_2, x_1)\rangle.$$

(Hint: A controlled-not acting on $|a\rangle|b\rangle$ yields $|a\rangle|a \oplus b\rangle$. Find a similar rule for the Toffoli gate, and use these in your construction.)

c) Optional. Carry out parts (a) and (b) for the function

$$\text{iii)} \quad f(x_3, x_2, x_1) = x_3 x_2 \oplus x_2 x_1 \oplus x_3 x_1$$

6. In connection with the Deutsch-Jozsa algorithm applied to functions $f(x)$, $f : \{0,1\}^n \to \{0,1\}$, it is of interest to consider a special type of function

$$g_{a,b}(x) = (a \cdot x + b) \bmod 2,$$

where both a and x are n-bit strings of 0's and 1's, $a \cdot x = \sum_j a_j x_j$, and $b = 0$ or 1.

a) Argue that there are $2^{(2^n)}$ distinct functions $f(x)$, but only 2^{n+1} distinct special functions $g_{a,b}(x)$. Show that for $n = 1$ all the $f(x)$ are of the special form, and that for $n = 2$ all constant and balanced functions are of the special form, but for $n \geq 3$ there are balanced functions that are not of the special form.

b) Suppose it is known that the unknown $f(x)$ is of the special form $g_{a,b}(x)$. What information about the pair (a, b) is provided by the final measurement outcome in the Deutsch-Josza algorithm?

c) Show that if $f(x)$ is of the special form $g_{a,b}(x)$ it is possible to extract the values of a and b in $O(n)$ classical queries without using any quantum tricks.