PHYSICS 150

Homework 5

Due in class, Thursday November 18, 2021

1. Consider Simon's problem, i.e. we have a function $f(x)$, where x has n bits and f has $(n-1)$ bits such that $f(x) = f(x \oplus a)$ where $a \neq 0$. The quantum algorithm obtains values for x such that $a \cdot x = 0$. From these linear equations for x one deduces a.

   Consider the case of $n = 4$. You are given that *some* of the values of x for which $x \cdot a = 0$ are

   ```
   x =    3   (0011)
   x =    4   (0100)
   x =    7   (0111)
   x =    9   (1001)
   ```

   (a) Using only this information, determine a.

   (b) For this value of a, show that $a \cdot x = 1$ for $x = 1$ and 2.
   (Hence $x = 1$ and $x = 2$ would not appear as possible results.)

2. Consider the RSA scheme for encryption with $p = 11, q = 3$ so $N = pq = 33$. For the encoding integer take $c = 3$ which has no factors in common with $(p-1)(q-1) = 20$.

   (a) Using the extended Euclid algorithm, find the decoding number d which satisfies $cd = 1 \mod (p-1)(q-1)$.

   (b) Assume that the original message m is represented by the integer 7. Compute the encoded message m' given by

   $$m' = m^c \mod N. \tag{1}$$

   (c) Compute $(m')^d \mod N$, and show that you recover the original message m.

3. We stated (without proof) that any quantum gate can be made out of single qubit gates and the CNOT gate (i.e. the only gate needed with more than one qubit is CNOT). Here we illustrate this for the controlled phase gate used in Shor's quantum Fourier transform.

   The (uncontrolled) phase gate (acting on one qubit) has the matrix representation

   $$R(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}, \tag{2}$$

   so the phase is changed by θ if the qubit is in state $|1\rangle$ and is unchanged if the qubit is in state $|0\rangle$.

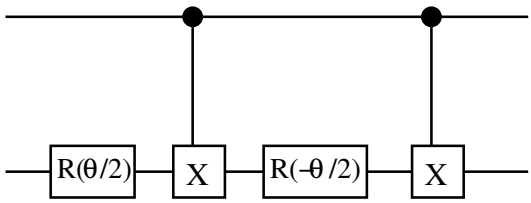
   Now we want this gate to be controlled by a control qubit such that the gate will only act on the target qubit if the control qubit is in state $|1\rangle$. We want to find out how to do this

using 1-qubit gates (including $R(\theta)$) and the CNOT (Ctrl-X) 2-qubit gate. Note that the 4×4 matrix representation for the controlled phase gate is

$$\begin{array}{c} \\ \langle 00| \\ \langle 01| \\ \langle 10| \\ \langle 11| \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix} \end{array}, \tag{3}$$

where the control qubit is to the left and the target qubit is to the right.

Show that the following circuit almost generates a controlled-phase gate:



In particular, write the 4×4 matrix representation of this circuit. From this you should be able show that if the control (upper) qubit is 0 then the qubits are unchanged (as required) but that if the control qubit is 1 (so the gate is activated) then the relative phase between the $|1\rangle$ and $|0\rangle$ states of the target (lower) qubit is θ as required, but the overall phase of these two states is not correct[1].

Show that this phase can be corrected by adding another $R(\theta/2)$ gate on the *control* qubit after the other gates have acted (i.e. at the right).

Note: If we have two or more qubits we often find it convenient to associate the global phase (or the sign in simple cases) with just *one* of the qubits. However, you should appreciate that this is simply a manner of speaking; the global phase is a property of the whole state.

4. Consider a function $f(x)$ which is periodic with period N. We are given a unitary operator U_y that performs the transformation

$$U_y|f(x)\rangle = |f(x+y)\rangle. \tag{4}$$

Show that the state

$$|\tilde{f}(k)\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{-2\pi i k x/N} |f(x)\rangle \tag{5}$$

is an eigenvector of U_y. Calculate the corresponding eigenvalue.

[1]Note that what I mean by this overall phase is the common phase of the two states of the target qubit when the control qubit is $|1\rangle$. The existence of this phase means that there is an error in the *relative* phase between the two states when the control qubit is $|1\rangle$ and those when the control qubit is $|0\rangle$ compared with what is expected in Eq. (3)

5. We have defined the quantum Fourier transform (QFT) in terms of a transformation of basis states

$$|x\rangle \to \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \exp[2\pi i x y/2^n] |y\rangle \,. \tag{6}$$

(a) If we consider a superposition

$$|\psi\rangle = \sum_{x=0}^{2^n-1} c_x |x\rangle, \tag{7}$$

show that one can regard the QFT as a transformation of the coefficients

$$|\psi\rangle \to \sum_{y=0}^{2^n-1} \tilde{c}_y |y\rangle \tag{8}$$

where

$$\tilde{c}_y = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \exp[2\pi i x y/2^n]\, c_x. \tag{9}$$

(b) Now suppose we shift the basis states by a, say, in the sense that we define a new state

$$|\psi'\rangle = \sum_{x=0}^{2^n-1} c_x |x+a\rangle. \tag{10}$$

Show that, after the quantum Fourier transform

$$|\psi'\rangle = \sum_{y=0}^{2^n-1} \tilde{c}'_y |y\rangle \tag{11}$$

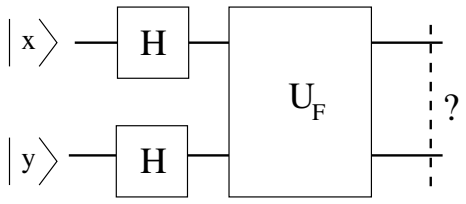
where

$$\tilde{c}'_y = e^{2\pi i a y/2^n} \tilde{c}_y \tag{12}$$

This is called the "shift-invariance" property of the Fourier transform.

6. (a) Write down the 4×4 matrix for the Fourier transform for $N = 4$ (2 qubits).

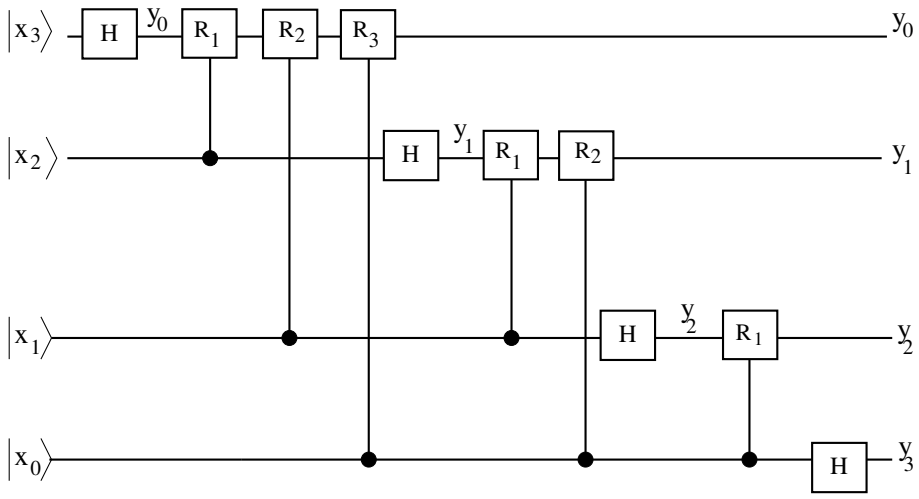
(b) Consider the circuit diagram below,



where F indicates the quantum Fourier transform.
What is the final state if $x = y = 0$?

(c) What is the final state for the other possible values of x and y?

7. The circuit for the quantum Fourier transform with 4 qubits is shown in the figure below. (The final swap gates are omitted).



Write down the following states of the system:

(a) Immediately after the R_3 gate on the top qubit.

(b) Immediately after the R_2 gate on the next to top qubit.

(c) Immediately after the R_1 gate on the second from top qubit.

(d) The final state at the right.

8. *Continued Fractions*
Consider the Shor algorithm for $n = 10$, so $2^n = 1024$. Recall that there are peaks in the quantum Fourier transform in the vicinity of $y_m = m2^n/r$, for integer m, where r is the period that we wish to determine. Suppose we measure $y = 695$, which, with high probability will be close to one of the peaks.

(a) Go through the continued fraction calculation to determine the period.

(b) Compare the resulting value of $y_m = m2^n/r$ with the measured (integer) value of 695.

Note:

- Recall you want the continued fraction with the largest denominator less than N, the number being factored. Since we take 2^n to be comparable to N^2, as discussed in class, you may assume that N is no bigger than 50.
- Note that the period could, potentially, be a multiple of the denominator, r_0, you found in the continued fraction. In a real situation, this would be checked by seeing if $a^{cr_0} \mod N = 1$, for $c = 1, 2, \cdots$. Neglect this possibility here and take the period r to equal the denominator r_0.
- If you wish you may use a package such as Mathematica, or write your own computer program, to help with evaluating the continued fraction.