Ph125c Spring 2017
Prof. Sean Carroll
seancarroll@gmail.com

Homework - 7

Assigned TA: Charles Xu
cxu3@caltech.edu

Due: 5:00pm, 5/31/2017

---

1 Controlled Gates [6 points]

In class we generalized the CNOT (controlled-NOT) gate to other "controlled" gates, i.e., gates that act on one qubit depending on the value of another control cubit. Let's see a little more explicitly how to make that happen.

(a.) [3 points] If $\mathbf{U}$ is a unitary 2×2 matrix with determinant one (i.e., an element of the group SU(2)), find unitaries $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ such that

$$\mathbf{ABC} = 1 \tag{1}$$

and simultaneously

$$\mathbf{A}\sigma_x\mathbf{B}\sigma_x\mathbf{C} = \mathbf{U}. \tag{2}$$

Hint: a 2×2 unitary matrix can be thought of as encoding a rotation in three-dimensional space, via the Euler-angle construction:

$$\mathbf{U} = \mathbf{R}_z(\phi)\mathbf{R}_y(\theta)\mathbf{R}_z(\psi), \tag{3}$$

where $\mathbf{R}_i(\alpha)$ is a 2×2 matrix implementing rotation around the ith axis by an angle θ. An explicit representation of a rotation around an axis $\mathbf{e}_i$ by an angle θ is

$$\mathbf{R}_i(\theta) = e^{-i(\theta/2)\sigma_i} = \cos(\theta/2)\mathbf{1} - i\sin(\theta/2)\sigma_i. \tag{4}$$

These rotation matrices can be conjugated by the Pauli matrices, for example

$$\sigma_x\mathbf{R}_z(\phi)\sigma_x = \mathbf{R}_z(-\phi). \tag{5}$$

(b.) [3 points] Construct a circuit using CNOT gates and single-qubit gates that implements a controlled-$\mathbf{U}$, where $\mathbf{U}$ is an arbitrary 2×2 unitary transformation.

2 Finding a Function [14 Points]

Imagine we are given a black box that calculates a function from n bits (i.e., $N = 2^n$ possible input values) to one bit,

$$f : \{0,1\}^n \to \{0,1\}. \tag{6}$$

One way of completely specifying what such a function does is simply to list, for every input value k, the output value $X_k = f(k)$. We could then construct a binary string

$$X = X_{N-1}X_{N-2}\cdots X_1X_0. \tag{7}$$

This string tells us the full action of the function. Our goal is to obtain (with high probability) the complete function, i.e. the exact value of the string X. In terms of resources, all that matters to us is the total number of times we query the box.

(a.) [2 Points] How many classical queries are needed to find X with probability of success at least 2/3?

(b.) [3 points] Suppose that someone (not you) has prepared a state that encodes the exact value of X in a certain convoluted way, to wit:

$$|\Psi_{X,N}\rangle = \frac{1}{\sqrt{2^N}} \sum_{Y\in\{0,1\}^N} (-1)^{X\cdot Y}|Y\rangle, \tag{8}$$

where $X \cdot Y$ is the "mod 2 bitwise inner product":

$$X \cdot Y = (X_{N-1} \cdot Y_{N-1}) \oplus (X_{N-2} \cdot Y_{N-2}) \oplus \cdots \oplus (X_1 \cdot Y_N) \oplus (X_0 \cdot Y_0). \tag{9}$$

Describe a way that we can use this state find the value of X with certainty, by applying a simple unitary and then performing a measurement. (In other words, all the difficulty in constructing a quantum algorithm to find X will be in constructing this kind of state.)

(c.) [4 points] We would like to perform a unitary transformation

$$\mathbf{U} : |Y\rangle \to (-1)^{X\cdot Y}|Y\rangle. \tag{10}$$

Explain how to do this using $|Y|$ queries of the box, where $|Y|$ is the "Hamming weight" of the string Y, which is simply equal to the number of 1's in the string.

(d.) [5 points] Now prepare a state (which doesn't depend on X), given by superposing basis vectors with less than a certain Hamming weight:

$$|\Phi_K\rangle = \frac{1}{\sqrt{M_K}} \sum_{Y:|Y|\leq K} |Y\rangle, \tag{11}$$

where

$$M_K = \sum_{j=0}^{K} \binom{N}{j}. \tag{12}$$

Then we apply the unitary $\mathbf{U}$ from part (c.) at most K times, to obtain

$$|\Psi_{X,K}\rangle = \frac{1}{\sqrt{M_K}} \sum_{Y:|Y|\leq K} (-1)^{X\cdot Y}|Y\rangle. \tag{13}$$

Show that, by applying the procedure from part (b.), we can determine the value of X with probability of success

$$p(N, K) = |\langle\Psi_{X,K}|\Psi_{X,N}\rangle|^2, \tag{14}$$

and compute the value of $p(N, K)$.
