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

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

Solution: From the anticommutation relations $\sigma_x\sigma_z\sigma_x = -\sigma_z$ and $\sigma_x\sigma_y\sigma_x = -\sigma_y$ together with eq. (4), we obtain not just eq. (5) but also the analogous expression for rotations about y: $\sigma_x\mathbf{R}_y(\theta)\sigma_x = \mathbf{R}_y(-\theta)$. Thus if we impose the ansatz

$$\begin{aligned}
\mathbf{A} &= \mathbf{R}_z(\alpha_z)\mathbf{R}_y(\alpha_y) \\
\mathbf{B} &= \mathbf{R}_y(\beta_y)\mathbf{R}_z(\beta_z) \\
\mathbf{C} &= \mathbf{R}_z(\gamma_z)
\end{aligned}$$

then eqs. (1) and (2) yield the constraints

$$\mathbf{ABC} = \mathbf{R}_z(\alpha_z)\mathbf{R}_y(\alpha_y)\mathbf{R}_y(\beta_y)\mathbf{R}_z(\beta_z)\mathbf{R}_z(\gamma_z) = 1$$

and

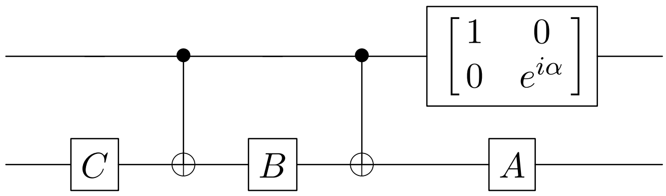
$$\begin{aligned}
\mathbf{A}\sigma_x\mathbf{B}\sigma_x\mathbf{C} &= \mathbf{R}_z(\alpha_z)\mathbf{R}_y(\alpha_y)\sigma_x\mathbf{R}_y(\beta_y)\sigma_x\sigma_x\mathbf{R}_z(\beta_z)\sigma_x\mathbf{R}_z(\gamma_z) \\
&= \mathbf{R}_z(\alpha_z)\mathbf{R}_y(\alpha_y)\mathbf{R}_y(-\beta_y)\mathbf{R}_z(-\beta_z)\mathbf{R}_z(\gamma_z) \\
&= \mathbf{R}_z(\phi)\mathbf{R}_y(\theta)\mathbf{R}_z(\psi)
\end{aligned}$$

where we used $\sigma_x^2 = 1$ in the first line, the conjugation relations in the second, and the Euler-angle decomposition of $\mathbf{U}$ eq. (3) in the third. These constraints can be solved for the angles $\alpha_z, \alpha_y, \beta_y, \beta_z, \gamma_z$ to give

$$\mathbf{A} = \mathbf{R}_z(\phi)\mathbf{R}_y\left(\frac{\theta}{2}\right)$$
$$\mathbf{B} = \mathbf{R}_y\left(-\frac{\theta}{2}\right)\mathbf{R}_z\left(-\frac{\psi+\phi}{2}\right)$$
$$\mathbf{C} = \mathbf{R}_z\left(\frac{\psi-\phi}{2}\right).$$

(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.

Solution: An arbitrary $\mathbf{U} \in \mathrm{U}(2)$ can always be written $\mathbf{U} = e^{i\alpha}\mathbf{V}$ for $\mathbf{V} \in \mathrm{SU}(2)$ and some real phase α. From part (a.) we know we can always decompose $\mathbf{V} = \mathbf{A}\sigma_x\mathbf{B}\sigma_x\mathbf{C}$ for some single-qubit unitaries $\mathbf{A}, \mathbf{B}, \mathbf{C}$ such that $\mathbf{ABC} = 1$. Therefore the following circuit does the trick:



To see this, consider the action of the circuit on inputs $|0\rangle|\psi\rangle$ and $|1\rangle|\psi\rangle$ respectively, for some arbitrary input state $|\psi\rangle$ of the bottom qubit. Keep in mind that the CNOT gate can be thought of as a controlled-σ_x.

$|0\rangle|\psi\rangle$: The CNOTs act as the identity on the bottom qubit, as does the phase gate on the top qubit $|0\rangle$. Thus the overall action is $\mathbf{ABC} = 1$ on the bottom qubit, i.e. the identity on the full state.

$|1\rangle|\psi\rangle$: Each CNOT applies σ_x to the bottom qubit, and the phase gate on the top qubit $|1\rangle$ applies an overall phase of $e^{i\alpha}$. Thus the overall action is $e^{i\alpha}\mathbf{A}\sigma_x\mathbf{B}\sigma_x\mathbf{C} = \mathbf{U}$ as desired.

(Note: due to the subtlety of the distinction between U(2) and SU(2), including the phase gate counted for one point of extra credit.)

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 $2/3$?

Solution: Assume no prior information about X. After querying $M < N$ bits of X, the remaining $N - M$ bits are still uniformly distributed in $\{0,1\}^{N-M}$ which leaves a probability $2^{M-N} < \frac{2}{3}$ of correctly guessing the entirety of X. Therefore we must classically query all N bits to meet this threshold.

(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.)

Solution: We claim that applying a tensor product of N Hadamard gates $H^{\otimes N}$ to $|\Psi_{X,N}\rangle$, then measuring in the logical basis will yield X with certainty. Proof: if we define $|X\rangle = |X_{N-1}\rangle |X_{N-2}\rangle \cdots |X_0\rangle$, it follows that

$$\begin{aligned}
H^{\otimes N} |X\rangle &= \bigotimes_{i=0}^{N-1} H |X_i\rangle \\
&= \bigotimes_{i=0}^{N-1} \frac{|0\rangle + (-1)^{X_i} |1\rangle}{\sqrt{2}} \\
&= \frac{1}{\sqrt{2^N}} \bigotimes_{i=0}^{N-1} \left[\sum_{Y_i\in\{0,1\}} (-1)^{X_i \cdot Y_i} |Y_i\rangle \right] \\
&= \frac{1}{\sqrt{2^N}} \sum_{Y\in\{0,1\}^N} (-1)^{X\cdot Y} |Y\rangle \\
&= |\Psi_{X,N}\rangle
\end{aligned}$$

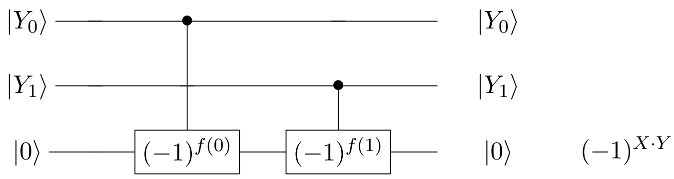
where in line 4 we have defined $|Y\rangle = |Y_{N-1}\rangle |Y_{N-2}\rangle \cdots |Y_0\rangle$ by analogy with $|X\rangle$. Since $H^{\otimes N}$ is its own inverse, it follows that $H^{\otimes N} |\Psi_{X,N}\rangle = |X\rangle$ as desired.

(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.

Solution: The following circuit implements the desired unitary in the case $N = 2$:



For general $N = 2^n$ this can still be done with a single ancilla qubit, here arbitrarily initialized to $|0\rangle$. For $0 \leq i \leq N-1$, qubit i (initialized to $|Y_i\rangle$) acts as control for a gate on the ancilla that queries $f(i)$ and applies an overall phase $(-1)^{f(i)} = (-1)^{X_i}$. Thus for $Y_i = 0$, f is not queried and the phase "applied" is $1 = (-1)^{X_i \cdot Y_i}$. For $Y_i = 1$, on the other hand, f is queried exactly once and the phase applied is $(-1)^{X_i} = (-1)^{X_i \cdot Y_i}$. Thus for any input $|Y\rangle$ in the computational basis, f is queried exactly $|Y|$ times and the overall phase acquired is

$$\prod_{i=0}^{N-1} (-1)^{X_i \cdot Y_i} = (-1)^{X \cdot Y}$$

as desired, since $|Y\rangle \otimes (-1)^{X \cdot Y} |0\rangle = (-1)^{X \cdot Y} |Y\rangle \otimes |0\rangle$.

(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 $p(N, K)$.

Solution: Recall from part (b.) that the procedure in question is (1) applying $H^{\otimes N}$ and then (2) measuring in the computational basis. Applying this to $|\Psi_{X,K}\rangle$, the probability of correctly measuring X is simply

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

as desired, where we have used the self-adjointness of H and the previously proved result $H^{\otimes N}|X\rangle = |\Psi_{X,N}\rangle$. We can straightforwardly evaluate this:

$$\begin{aligned}
p(N,K) &= |\langle \Psi_{X,N}|\Psi_{X,K}\rangle|^2 \\
&= \frac{1}{2^N M_K}\left|\sum_{Y'\in\{0,1\}^N}(-1)^{X\cdot Y'}\langle Y'|\sum_{Y:|Y|\leq K}(-1)^{X\cdot Y}|Y\rangle\right|^2 \\
&= \frac{1}{2^N M_K}\left|\sum_{Y'\in\{0,1\}^N}\sum_{Y:|Y|\leq K}(-1)^{X\cdot(Y'\oplus Y)}\langle Y'|Y\rangle\right|^2 \\
&= \frac{1}{2^N M_K}\left|\sum_{Y:|Y|\leq K}(-1)^{X\cdot(Y\oplus Y)}\right|^2 \\
&= \frac{1}{2^N M_K}\left|\sum_{Y:|Y|\leq K}1\right|^2 \\
&= \frac{1}{2^N M_K}\left|\sum_{j=0}^{K}\binom{N}{j}\right|^2 \\
&= \frac{M_K}{2^N}.
\end{aligned}$$
