Physics 84
Homework 2
2/9/17

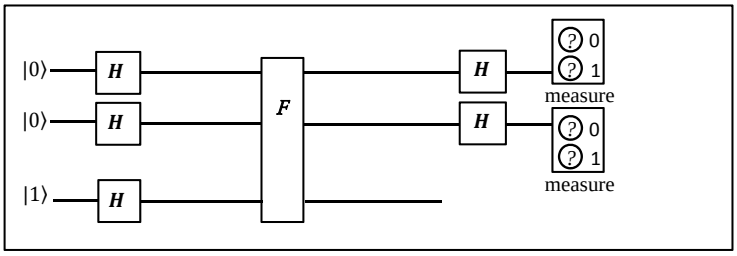
1, 2, 3, 4

1. The 2-bit Deutsch-Jozsa algorithm

The n-bit Deutsch-Jozsa algorithm determines whether a two-valued function of an n-bit string, $f : \{0,1\}^{\otimes n} \to \{0,1\}$, is constant or balanced. (For $n > 1$ most functions are neither constant *nor* balanced, but in this scenario we are assured that f must be either one or the other; we only need to decide which.) An oracle F takes an n-bit input x (or $|x\rangle$) and a single target bit y (or $|y\rangle$). It computes $f(x)$ by taking y to $y \oplus f(x)$ (or $|y\rangle$ to $|y \oplus f(x)\rangle$) just as in the one-bit algorithm. In the quantum case, $|x\rangle$ is an n-qubit basis state; *e.g.*, $|0\rangle\,|1\rangle\,|0\rangle\,|0\rangle\,...\,|1\rangle$ to represent $x = 0100...1$.

In the classical case, we call the oracle on different x inputs and record all the $f(x)$ values. We argued in class that the oracle must be called $2^{n-1}+1$ times in the worst-case scenario. In this problem, you will show that a quantum circuit requires just one call to the oracle.

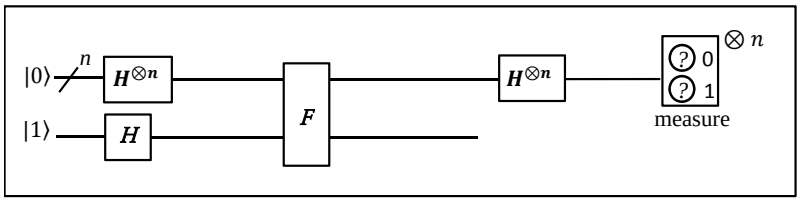
(a) Let f be a constant or balanced function $f : \{0,1,2,3\} \to \{0,1\}$, or using binary notation for the input numbers, $f : \{00,01,10,11\} \to \{0,1\}$. Explain, by determining the relevant properties of the 3-qubit state through the stages of the computation, what two-qubit measurement result you must get in the circuit below if the oracle encodes a constant f.



(b) Consider the same circuit as in part (b), but let the oracle encode a balanced function f. Show that you can *never* get the same two-qubit measurement result as you were guaranteed in part (b). [Hint: Show that the state after the oracle F for a balanced function is orthogonal to the state after the oracle F for a constant function. Unitary evolution preserves orthogonality, so now you know that the state right before measurement for a balanced function is orthogonal to the state right before measurement for a constant function. Use that to show the measurement always yields different results for a balanced function vs. a constant one.]

1. cont.

(c) Now let f be a constant or balanced function $f : \{0,1\}^{\otimes n} \to \{0,1\}$. Explain, by determining the relevant properties of the $(n+1)$-qubit state through the stages of the computation, how the following quantum circuit solves the problem with a single call to the oracle. This solution is the n-bit or generalized Deutsch-Jozsa algorithm; though David Deutsch and Richard Jozsa contributed greatly to its development, the algorithm in its present form was actually published by Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca in 1998. (See, *e.g.*, arxiv.org/abs/quant-ph/9708016 after you have solved this homework problem.)



■

2. Creating entangled states

One of the entangled "Bell states" of two qubits is

$$|\Psi^-\rangle = \frac{|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B}{\sqrt{2}}.$$

Design a quantum logic circuit, using gates we have discussed in class, to create this two-qubit state starting from input qubits in the computational basis states $|0\rangle$ or $|1\rangle$. Show that your circuit produces the state $|\Psi^-\rangle$ as its output.

■

3. Measurements on one member of an entangled pair

Consider the two-qubit state $|\Psi^-\rangle$, but imagine that we perform a measurement on qubit A only.

(a) Consider measuring qubit A in the $\{|0\rangle_A, |1\rangle_A\}$ basis. The probability of finding qubit A in state $|0\rangle_A$ is given by

$$\langle\Psi^-|\hat{P}_{0,A} \otimes \hat{I}_B|\Psi^-\rangle;$$

here, the single-qubit projection operator $\hat{P}_0$ acting on qubit A is tensored with the identity operator $\hat{I}$ acting on qubit B since no measurement is performed on qubit B. Show that the probability of finding qubit A in state $|0\rangle_A$ is $1/2$.

(b) We may choose to write each qubit's state, not as a superposition of $|0\rangle$ and $|1\rangle$, but as a superposition of $|\psi\rangle$ and $|\psi_\perp\rangle$, where $|0\rangle = \alpha|\psi\rangle + \beta|\psi_\perp\rangle$, $|1\rangle = -\beta^*|\psi\rangle + \alpha^*|\psi_\perp\rangle$, and $|\alpha|^2 + |\beta|^2 = 1$. Show that:

$$|\Psi^-\rangle = \frac{|\psi\rangle_A|\psi_\perp\rangle_B - |\psi_\perp\rangle_A|\psi\rangle_B}{\sqrt{2}}.$$

(c) If we measure qubit A in *any* $\{|\psi\rangle_A, |\psi_\perp\rangle_A\}$ basis, show that the probability of finding qubit A in the state $|\psi\rangle_A$ is $1/2$. Thus the state of qubit A by itself, independent of the state of qubit B, is completely uncertain and contains no information. This is the hallmark of complete entanglement between two particles.

■

4. Controlled U from CNOT and single-qubit unitaries

In class, we constructed a general two-qubit controlled U gate from CNOT and single-qubit unitaries by first writing U as $U = e^{i\alpha}AXBXC$. Here $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and A, B, and C are unitary matrices such that $ABC = I$.

(a) Show that $XR_y(\Delta)X = R_y(-\Delta)$, where $R_y(\Delta) = \begin{bmatrix} \cos\frac{\Delta}{2} & -\sin\frac{\Delta}{2} \\ \sin\frac{\Delta}{2} & \cos\frac{\Delta}{2} \end{bmatrix}$ represents rotation by angle Δ about the y axis on the Bloch sphere.

(b) Show that $XR_z(\gamma)X = R_z(-\gamma)$, where $R_z(\gamma) = \begin{bmatrix} e^{-i\frac{\gamma}{2}} & 0 \\ 0 & e^{i\frac{\gamma}{2}} \end{bmatrix}$ represents rotation by angle γ about the z axis on the Bloch sphere.

(c) Show that

$$A = R_z(\beta')R_y(\frac{\Delta}{2})$$
$$B = R_y(-\frac{\Delta}{2})R_z(-\frac{(\beta+\beta')}{2})$$
$$C = R_z(\frac{\beta-\beta'}{2})$$

satisfy the conditions set out above for expressing an arbitrary U. That is, show that $ABC = I$ and that $e^{i\alpha}AXBXC$ gives a form we discussed in class for a general 2x2 unitary matrix.

■