Introduction to Quantum Computation, UPB
Summer 2020, Assignment 7

Due: Friday, June 26 at start of tutorial

Exercises

1. As seen in class, Deutsch's algorithm is able to determine with certainty (i.e. probability 1) whether a 1-bit function is constant or balanced. Suppose you wish to run Deutsch's algorithm in your lab, but your equipment doesn't quite function as you expect. In particular, instead of preparing your desired initial state of $|0\rangle|1\rangle$ to the algorithm, your machine prepares state $|\psi\rangle|1\rangle$ for $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

   (a) Assuming the function f is balanced, what is the probability that Deutsch's algorithm on your faulty initial state $|\psi\rangle|1\rangle$ will correctly output "balanced", i.e. that the final measurement result in the algorithm has label 1?

   (b) There is only so much "error" that the algorithm can tolerate before it becomes useless — for which range of the parameter $0 \leq |\alpha| \leq 1$ is the probability of success in part 3a less than or equal to $1/2$? In other words, for which values of $|\alpha|$ is it better to forget about running Deutsch's algorithm and instead just flip a classical (unbiased) coin to "decide" if f is balanced?

2. This question will practice working through Simon's algorithm.

   (a) Consider function $f : \{0,1\}^2 \mapsto \{0,1\}^2$ such that $f(00) = 10$, $f(01) = 11$, $f(10) = 10$ and $f(11) = 11$. This function satisfies the promise required for Simon's problem, i.e. $f(x) = f(y)$ iff $x = y \oplus s$. What is the value of s for f?

   (b) Suppose $f : \{0,1\}^n \mapsto \{0,1\}^n$ is an n-bit function which slightly violates the promise required of Simon's algorithm in that f is "almost" one-to-one in the following sense: For each distinct input $x \in \{0,1\}^n$, the output $f(x)$ is unique, *except* for inputs 0^n and 1^n, which are the only pair of inputs satisfying $f(0^n) = f(1^n)$. Thus, we are very "close" to the $s = 0^n$ case, and we expect the analysis to go "similarly".

   Recall that right before the measurement in Simon's algorithm, our quantum state looks like

   $$\sum_{y \in \{0,1\}^n} |y\rangle \left(\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} |f(x)\rangle \right).$$

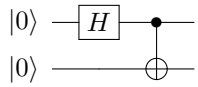
   Pick an arbitrary $\hat{y} \in \{0,1\}^n$. Show that when the first register is now measured in the standard basis, the probability of outcome $\hat{y}$ is given by

   $$\frac{1}{2^n} \pm \frac{1}{2^{2n-1}},$$

   where the $+$ occurs if the parity of y is even, and the $-$ occurs if the parity of y is odd. Here, the parity of y is defined as $\bigoplus_{i=1}^n y_i$. (Hint: One way to do the analysis is to recall that for any normalized state $|\psi\rangle = \sum_{z \in \{0,1\}^n} |z\rangle|\phi_z\rangle$, the probability of observing outcome $|z\rangle$ in the first register is $\langle \phi_z | \phi_z \rangle$. Do make sure you understand this claim first.)

3. In our analysis of Simon's problem, we assumed that one could make *intermediate* measurements when running a circuit. This process, of course, is non-unitary, and ideally we would instead like to keep the computation unitary until the very end, at which point we measure everything in the standard basis. In this question, you will show that indeed, measurements can be *deferred* to the end of a circuit, without loss of generality.

   Recall the circuit C for preparing the Bell state $|\Phi^+\rangle$:



   (a) Suppose we insert a measurement in the standard basis on qubit 1 between the Hadamard gate and the CNOT gate. What is the output state of the new circuit C'? (Hint: You will need to use the density matrix formalism ρ to describe the immediate postmeasurement state, assuming the measurement outcome is not read, and subsequently apply any unitary gates U in the circuit as $U\rho U^\dagger$.)

   (b) Show that by adding a single ancilla qubit (and appropriate additional quantum gates) to C', we can simulate the output of C' by instead measuring only at the *end* of the circuit. Specifically, add a new qubit to the circuit, which is measured only at the end of the circuit (in the standard basis).