Introduction to Quantum Computation, UPB
Winter 2022, Assignment 7

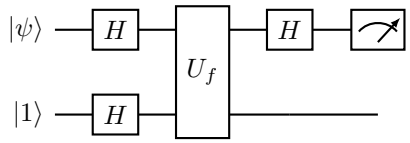
Eli Kogan-Wang

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?

   Answer: Consider the following circuit diagram for Deutsch's algorithm on our faulty initial state $|\psi\rangle|1\rangle$:



   Our whole state $|\psi_1\rangle$ after the first Hadamard gates:

$$\begin{aligned}|\psi_1\rangle &= (\alpha|+\rangle + \beta|-\rangle)|-\rangle \\ &= \frac{1}{\sqrt{2}}(\alpha(|0\rangle + |1\rangle) + \beta(|0\rangle - |1\rangle))|-\rangle \\ &= \frac{1}{\sqrt{2}}((\alpha+\beta)|0\rangle + (\alpha-\beta)|1\rangle)|-\rangle\end{aligned}$$

   After applying the unitary U_f, using phase kickback:

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\Big((\alpha+\beta)(-1)^{f(0)}|0\rangle + (\alpha-\beta)(-1)^{f(1)}|1\rangle\Big)|-\rangle$$

   Without loss of generality we can assume that $f(0) = 1$ and $f(1) = 0$ (since f is balanced), since the additional (-1) global phase doesn't affect the final measurement result.
   So:

$$|\psi_2\rangle' = \frac{1}{\sqrt{2}}((\alpha+\beta)|0\rangle - (\alpha-\beta)|1\rangle)|-\rangle$$

   Applying the second Hadamard gate:

$$
\begin{aligned}
|\psi_3\rangle &= \frac{1}{\sqrt{2}}\left((\alpha+\beta)\,|+\rangle - (\alpha-\beta)\,|-\rangle\right)|-\rangle \\
&= \frac{1}{2}\left((\alpha+\beta)(|0\rangle+|1\rangle) - (\alpha-\beta)(|0\rangle-|1\rangle)\right)|-\rangle \\
&= \frac{1}{2}\left(2\beta\,|0\rangle + 2\alpha\,|1\rangle\right)|-\rangle \\
&= \beta\,|0\rangle + \alpha\,|1\rangle\,|-\rangle
\end{aligned}
$$

Measuring the first qubit gives us $|0\rangle$ w.P. $|\beta|^2$ and $|1\rangle$ w.P. $|\alpha|^2$.

So the probability that the algorithm will output "balanced" is $|\alpha|^2$.

Additionally, for the case that $\alpha = 1$ (and $\beta = 0$), as when the preparation state is correct, the probability that the algorithm will output "balanced" is 1, as expected.

(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?

Answer: Since we know that the probability of success is $|\alpha|^2$, we can solve for $|\alpha|$:

$$
\begin{aligned}
|\alpha|^2 &\leq \frac{1}{2} \\
|\alpha| &\leq \sqrt{\frac{1}{2}} \\
|\alpha| &\leq \frac{1}{\sqrt{2}}
\end{aligned}
$$

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?

Answer: Since $f(00) = f(10)$, we know that $s = 00 \oplus 10 = 10$. (Similarly, since $f(01) = f(11)$: $s = 01 \oplus 11 = 10$, so $s = 10$ as before.)

(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.)

Answer: Using the given fact, we will consider $\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot y}\,|f(x)\rangle$ for even and odd parity of y.

In general:

$$\begin{aligned}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot y}\,|f(x)\rangle &= \sum_{x\in\{0,1\}^n\setminus\{0^n,1^n\}}(-1)^{x\cdot y}\,|f(x)\rangle + (-1)^{y\cdot 0^n}\,|f(0^n)\rangle + (-1)^{y\cdot 1^n}\,|f(1^n)\rangle \\ &= \sum_{x\in\{0,1\}^n\setminus\{0^n,1^n\}}(-1)^{x\cdot y}\,|f(x)\rangle + (-1)^{y\cdot 0^n}\,|f(0^n)\rangle + (-1)^{y\cdot 1^n}\,|f(0^n)\rangle\end{aligned}$$

Now, for even parity of y, we have that $y\cdot 0^n = 0$ and $y\cdot 1^n = 0$, so the last two terms are equal and add to $2\,|f(0^n)\rangle$.

For odd parity of y, we have that $y\cdot 0^n = 0$ and $y\cdot 1^n = 1$, so the last two terms cancel out.

Now, for the $x\in\{0,1\}^n\setminus\{0^n,1^n\}$ term, we know that all $|f(x)\rangle$ are all orthogonal to each other, so getting the magnitude of the vector is as easy as counting the terms.

For both cases we have 2^n-2 terms in the sum, additionally for even parity we have $2\,|f(0^n)\rangle$ and for odd parity we have 0.

Now the magnitude squared of the vector for even parity is $(2^n-2)\cdot 1^2 + 2^2 = 2^n+2$ and for odd parity is $(2^n-2)\cdot 1^2 = 2^n-2$.

We do not need to consider $x\cdot y$ since $(-1)^2 = 1^2$.

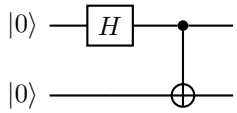
Working with $2^n \pm 2$, and dividing by $\left(\frac{1}{2^n}\right)^2$:

$$\begin{aligned}\left(\frac{1}{2^n}\right)^2\cdot(2^n\pm 2) &= \frac{2^n}{2^{2n}} \pm \frac{2}{2^{2n}} \\ &= \frac{1}{2^n} \pm \frac{1}{2^{2n-1}}\end{aligned}$$

As desired.

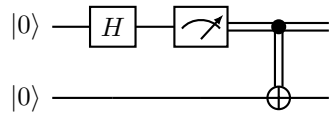
3. In our analysis of Simon's problem, we assumed that one could make *intermediate* measurements when running a circuit. This process, of course, is non-unitary, and ideally we would instead like to keep the computation unitary until the very end, at which point we measure everything in the standard 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 $U\rho U^\dagger$.)

   Answer: Consider C':



After applying the Hadamard gate and measuring, we have:

$$\rho_1 = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) \otimes |0\rangle\langle 0| = \frac{1}{2}\left(|00\rangle\langle 00| + |10\rangle\langle 10|\right)$$

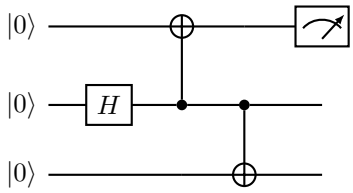
Now, we apply the CNOT gate. Recall that $\text{CNOT}^\dagger = \text{CNOT}$.

$$\begin{aligned}\rho_2 &= \text{CNOT}^\dagger \rho_1 \text{CNOT} \\ &= \text{CNOT}\frac{1}{2}\left(|00\rangle\langle 00| + |10\rangle\langle 10|\right)\text{CNOT} \\ &= \frac{1}{2}\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right)\end{aligned}$$

Giving us our output state.

(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).

We modify C' to C'':



Our ancilla qubit is the first one.

Since we only use the second qubit as a control qubit, the partial trace after application of CNOT remains unchanged.

Our state just before measurement is thus:

$$\psi_{\text{before measurement}} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

After measurement on the ancilla qubit, we have:

$$\rho_{\text{after measurement}} = \frac{1}{2}\left(|000\rangle\langle 000| + |111\rangle\langle 111|\right)$$

Taking the partial trace over the ancilla qubit, we have:

$$\rho_{\text{after measurement}} = \frac{1}{2}\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right)$$

Which is our desired result.

Additionally, since the measured qubit is only used as a control qubit, we may even dispense with the ancilla qubit and simply measure any single qubit at the end of the circuit.