CS 880: Quantum Information Processing 9/13/2010

Lecture 4: Elementary Quantum Algorithms

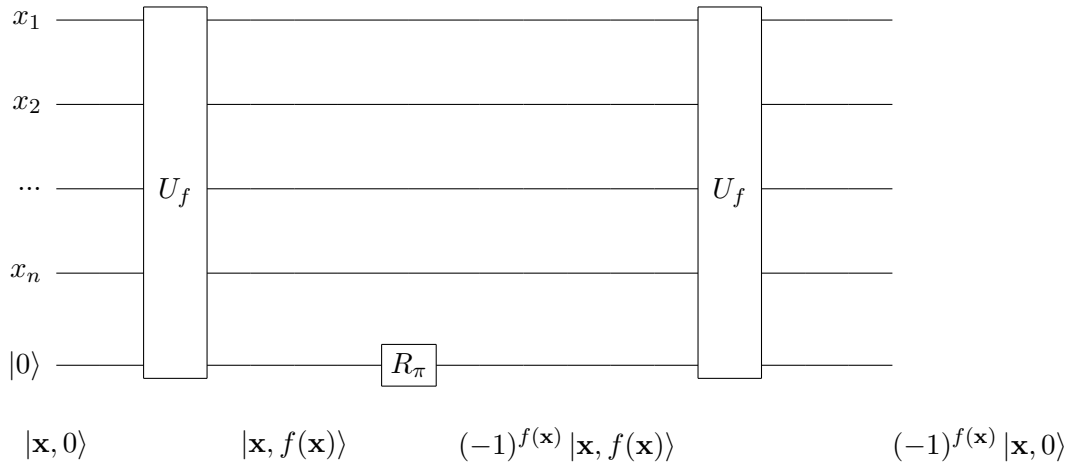
Instructor: Dieter van Melkebeek Scribe: Kenneth Rudinger

This lecture introduces several simple quantum algorithms. The particular algorithms introduced here solve their respective problems faster than their corresponding classical algorithms (deterministic or probabilistic). Specifically, we examine the Deutsch, Deutsch-Josza, Bernstein-Vazirani, and Simon problems..

1 Solving Black Box Problems

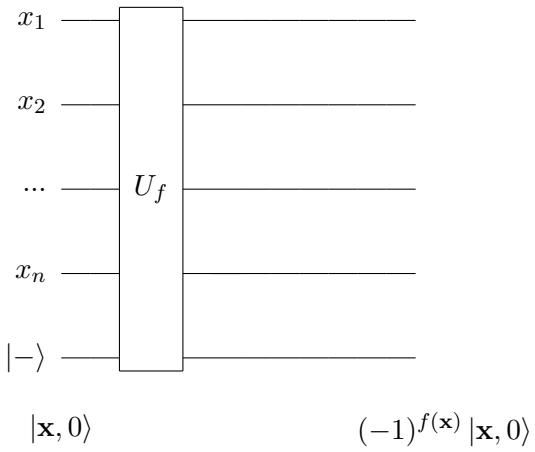
For the time being, we concern ourselves only with black box problems. A black box problem is one in which we are given a function f. All we know for certain about this function is that $f\colon \{0,1\}^n \to \{0,1\}^m$. It is our goal to determine some property of f. (If we are given further information about this function, we call it a promise function, as some property of the function has been "promised" to us.) To determine the desired property property, we are given access to a transformation (the black box) which acts on an input of our choosing (residing in $\{0,1\}^n$); the transformation's output is the function in question applied to our input. However, because valid quantum computations must correspond to invertible (more specifically, unitary) transformations, the black box actually performs the function $\tilde{f}\colon \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^n \times \{0,1\}^m : (\mathbf{x}, \mathbf{y}) \to (\mathbf{x}, \mathbf{y} \oplus f(\mathbf{x}))$. We denote the unitary transformation that realizes $\tilde{f}$ by U_f.

One example of such is a transformation where $m = 1$. If we start in the state $|\psi_0\rangle = |x\rangle\,|0\rangle$, then we see that $U_f\,|\psi_0\rangle = |x\rangle\,|f(x) \oplus 0\rangle = |x\rangle\,|f(x)\rangle$. We then apply R_π to the ancilla qubit, mapping $|x, f(x)\rangle$ to $(-1)^{f(x)}\,|x, f(x)\rangle$. Lastly, we apply U_f to the state again, sending the ancilla back to its original state of $|0\rangle$, and keeping the non-ancilla qubits in the state we desired to create, $(-1)^{f(x)}\,|x\rangle$. Pictured below is the corresponding circuit.



This particular method is referred to as *phase kickback*, as $f(\mathbf{x})$ is encoded in the phase of our final state.

This transformation required two queries of our oracle U_f. Can we achieve this phase kickback with only one query? It turns out that we can. Let's instead initialize our ancilla qubit to $|-\rangle$ (Recall: $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = H|1\rangle$.) Now when we apply U_f, the ancilla remains in the state $|-\rangle$, and we pick up the desired phase, that is: $U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$. Thus we can achieve phase kickback with only one query of our oracle, as shown below.



Keeping in mind this phase kickback trick, we now turn our attention to the four problems mentioned above

2 Deutsch's Problem

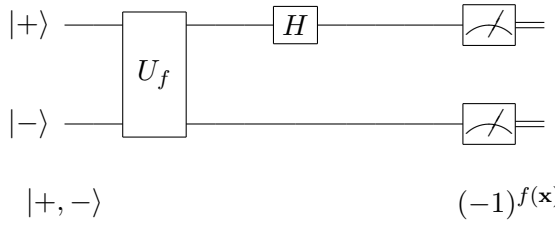
Consider a function f such that $f : \{0,1\}^n \to \{0,1\}^m$. (Here, $n = m = 1$.) The question we wish to answer is: Does $f(0) = f(1)$? Classically, we must make two queries of our oracle, one to determine $f(0)$, the other to determine $f(1)$. (Even if we use probabilistic computation instead of deterministic, we are still required to make two queries.) However, with a quantum circuit, we need only one query. We will use the phase kickback technique, recalling that:

$$|0\rangle|-\rangle \to (-1)^{f(0)}|0\rangle|-\rangle$$
$$|1\rangle|-\rangle \to (-1)^{f(1)}|1\rangle|-\rangle$$

If we apply the phase kickback to a superposition of these states, we find

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|-\rangle \to \frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)|-\rangle$$

If $f(0) = f(1)$, then this state reduces to $\pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|-\rangle = \pm|+\rangle|-\rangle$. If $f(0) \neq f(1)$, the resulting state is $\pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|-\rangle = \pm|-\rangle|-\rangle$. We note then that these two states are orthogonal. Therefore, there exists a unitary transformation which will map one of these states to $|0\rangle$ and the other to $|1\rangle$. This transformation is the Hadamard gate. Therefore, the resulting quantum circuit is:



Thus if we observe the $|0\rangle$ state, we know that $f(0) = f(1)$, and vice-versa for an observation of the $|1\rangle$. Therefore, we see that with only one query, we are able to determine the nature of f, with 100% accuracy.

3 Deutsch-Jozsa Problem

Now we consider a more general problem, where our function takes a string of n qubits:

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

Additionally, this is a promise problem; we are told some additional information about f. In this particular case, we know that f is either balanced or constant. (In the n=1 case, we see that this reduces to just the Deutsch problem.) It is our task to determine whether f is balanced or constant. How many queries are required to answer this question correctly? Deterministically, $2^{n-1}+1$ queries are required. The number of queries required using a classical randomized algorithm will depend on the allowed error. If k inputs are chosen at random, k queries will yield a correct answer with error less than or equal to 2^{1-k}. (If the function is balanced, we could discover this in a minimum of two queries, if we are lucky. The most unlucky we can be is to choose k inputs that have the same output, leading us to guess incorrectly that the function is constant. The probability of choosing k inputs with the same output, and hence guessing wrong, is 2^{1-k}.) However, there exists a quantum algorithm which yields 100% accuracy (modulo experimental error) with only 1 query, providing a tremendous speedup, from exponential to constant!

How does this algorithm work? Start with an initial state which is a uniform superposition of n qubits, tensored together with one ancilla in the $|-\rangle$ state, or:

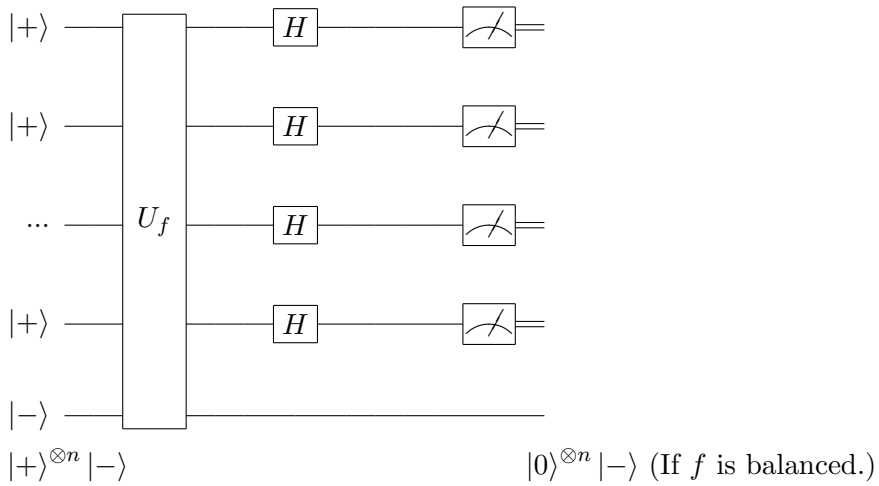
$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}}\left(\sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle\right)|-\rangle$$

Apply U_f to this state. If f is constant, we find that:

$$U_f|\psi_0\rangle = \pm\frac{1}{\sqrt{2^n}}\left(\sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle\right)|-\rangle$$

If f is balanced, $U_f|\psi_0\rangle$ takes on a more complicated form, but as in the Deutsch algorithm, $U_f^{balanced}|\psi_0\rangle$ is orthogonal to $U_f^{constant}|\psi_0\rangle$. Therefore, all we need is, as before, a unitary transformation that will send $U_f^{balanced}|\psi_0\rangle$ to a string of all 0s. Again, the Hadamard gate will serve this purpose; applying it to each (non-ancilla) wire yields the desired result. If f is constant, the final readout will be the all-0 string. As $U_f^{balanced}|\psi_0\rangle$ is orthogonal to $U_f^{constant}|\psi_0\rangle$, the final readout

for a balanced f cannot be the all-0 string. Thus in one query have we determined the nature of f, with 100% accuracy. Shown below is the quantum circuit diagram for this algorithm.



3.1 Note on the Hadamard Gate

Before proceeding, let us consider the operation of n Hadamard gates on a base state of length n: $H^{\otimes n}|x\rangle$. We see that such an operation has the following action:

$$H^{\otimes n}|x\rangle = \bigotimes_{i=1}^{n} \frac{|0\rangle + (-1)^{x_i}|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}^n}\sum_y (-1)^{\mathbf{x}\cdot\mathbf{y}}|y\rangle \tag{1}$$

($\mathbf{x}\cdot\mathbf{y}$ denotes an inner product, that is, $\mathbf{x}\cdot\mathbf{y} = \sum_{i=1}^{n} x_i y_i$.) Thus by appropriate choice of $\mathbf{x}$, we may generate all possible base states in the $\{|+\rangle, |-\rangle\}$ basis. Additionally, we can generate a uniform superposition of states if we choose $\mathbf{x}$=$\mathbf{0}$.

4 Bernstein-Vazirani Problem

Now consider the following function.

$$\begin{aligned} f : \{0,1\}^n &\to \{0,1\} \\ \mathbf{x} &\to (\mathbf{a}\cdot\mathbf{x} + b) \pmod 2 \\ (\mathbf{a} \in \{0,1\}^n, b &\in \{0,1\}) \end{aligned}$$

The promise is that f conforms to the above constraints. Our task is to determine the values of $\mathbf{a}$ and b. (We note that the Bernstein-Vazirani promise is a restriction on Deutsch-Josza, but the question is harder to solve.) With a classical deterministic algorithm, $n+1$ queries are required; 1 to determine b (query with $\mathbf{x} = \mathbf{0}$), and n to determine $\mathbf{a}$. (We also note that is, classically, the optimal algorithm, as $n+1$ bits of information are required.) A classical randomized algorithm will do no better, also requiring $n+1$ queries.

Exercise 1. *Show that any classical randomized algorithm that solves the Bernstein-Vazirani problem with reasonable error makes at least $n+1$ queries.*

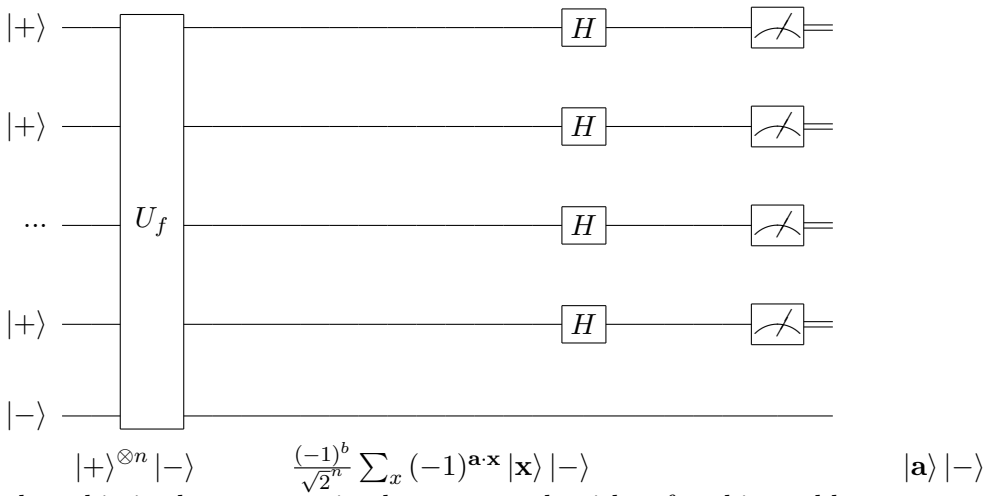
Turning to the quantum algorithm, we will discover that there exists a solution that requires only two queries, solving with 100% accuracy. As before, one query is required for b, but now also only one query is required for $\mathbf{a}$. b is determined in the same manner as in the classical algorithm. To determine $\mathbf{a}$, we initialize to:

$$|\psi_0\rangle = |+\rangle^{\otimes n} |-\rangle$$

We note then that:

$$U_f |\psi_0\rangle = \frac{1}{\sqrt{2^n}}\Big(\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{f(\mathbf{x})} |x\rangle\Big) |-\rangle = \frac{(-1)^b}{\sqrt{2^n}}\Big(\sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{\mathbf{a}\cdot\mathbf{x}} |\mathbf{x}\rangle\Big) |-\rangle$$

If we simply apply a Hadamard gate to each non-ancilla qubit, then the final readout will be of $|\mathbf{a}\rangle$ (along with the ancilla), as illustrated by equation (1).



It turns out that this is the most optimal quantum algorithm for this problem; one cannot do better.

5 Simon's Algorithm

Now we examine a function which maps not to $\{0,1\}$, but to $\{0,1\}^n$ instead. More specifically

$f : \{0,1\}^n \to \{0,1\}^n$ such that either:

(1) f is one-to-one (f is a permutation.)

or

(2) $\exists \mathbf{s} \neq \mathbf{0} \forall (\mathbf{x}, \mathbf{y}) f(\mathbf{x}) = f(\mathbf{y}) \iff \mathbf{x} \oplus \mathbf{y} = \mathbf{s}$ (f is two-to-one.)

(It should be noted that (1) is a special case of (2), with $\mathbf{s} = \mathbf{0}$.) Our goal here is to determine if f falls into category (1) or (2), and also determine the value of $\mathbf{s}$. If one were lucky, and f fell into the second category, one could solve this problem classically with only two queries (by appropriately choosing $\mathbf{x}$ and $\mathbf{y}$ such that $f(\mathbf{x}) = f(\mathbf{y})$). However, this is not a reliable method, nor could it tell us if f is one-to-one. The general lower bound is achieved by picking k possible values for $\mathbf{s}$ (k different spacings), eliminating $\binom{k}{2}$ values for $\mathbf{s}$. Thus the lower bound is approximately $2^{\frac{n}{2}}$ queries. A randomized algorithm requires $\Omega(2^{\frac{n}{2}})$ queries. However, there exists a quantum algorithm which can solve this problem in $O(n)$ time. The demonstration of this technique is forthcoming in the next lecture (Lecture 5).