Lecture Notes on Quantum Computation and Quantum Information Processing.

Instructor: Sudebkumar Prasant Pal: Scribe: Sima Das.

March 8, 2004

1 Quantum algorithms

We discuss the use of quantum parallelism due to the superposition of multiple amplitudes from multiple qubits, resulting in interesting states that form the basis for quantum algorithms, giving them their unique computing power.

1.1 Quantum parallelism

Let f be a one bit boolean function $f : \{0,1\} \rightarrow \{0,1\}$. A way to compute $f(x)$ on a quantum computer is to consider a circuit which transforms $|x, y\rangle$ into $|x, y \oplus f(x)\rangle$. We say that this circuit applies the unitary operator U_f: $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$. This operator is also its own inverse. If $y = 0$, the second qubit is indeed $f(x)$. U_f can be applied to the superposition $((|0\rangle + |1\rangle)\sqrt{2})|y\rangle$ as much as it can be applied to $|0\rangle|y\rangle$ or $|1\rangle|y\rangle$ (for the variable $|x\rangle|y\rangle$). The resulting state transition would then be $|(|0\rangle + |1\rangle)/\sqrt{2}, |0\rangle\rangle \rightarrow (|0, f(0)\rangle + |1, f(1)\rangle)/\sqrt{2}$. Here, we have both $f(0)$ and $f(1)$ within the resulting second qubit state. This is an example of quantum parallelism due to superposition of two amplitudes coming from each of the two qubits. Reading the second qubit gives $f(0)$ or $f(1)$ with 50% probability each.

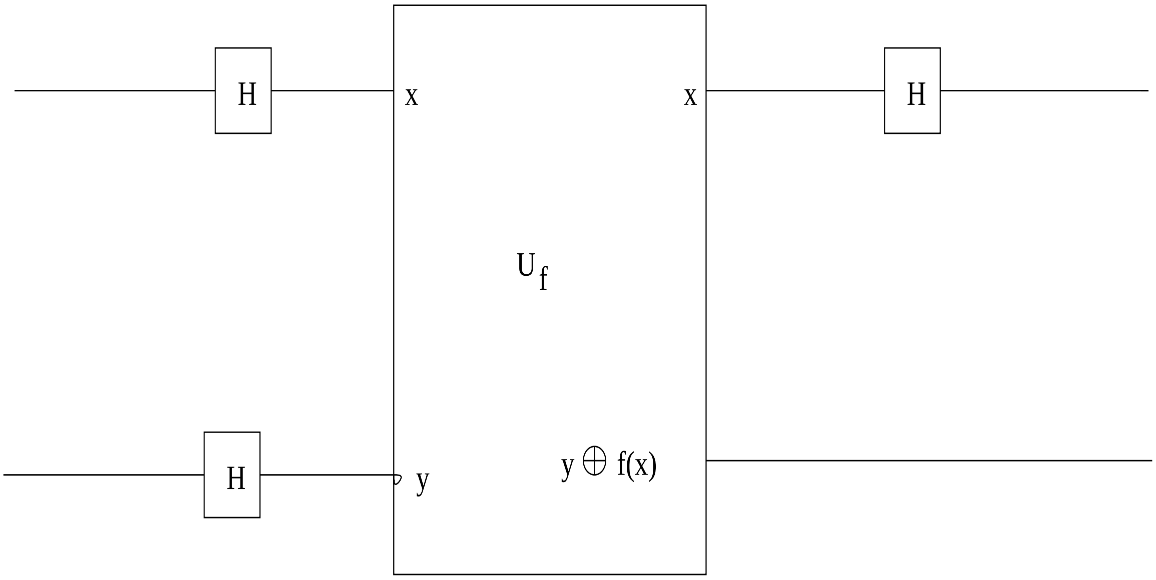

Figure 1: Circuit for implementing Deutsch's algorithm

1.2 The development of Deutsch's algorithm

Suppose we start in the state $|\psi_0\rangle = |01\rangle$. After applying the Hadamard operator on each qubit we get the state $|\psi_1\rangle = [(|0\rangle + |1\rangle)\sqrt{2}]\ [(|0\rangle - |1\rangle)\sqrt{2}]$. The controlled-$f$ operation is realized as the unitary operator $U_f : |x, y\rangle = |x, y \oplus f(x)\rangle$. Note that $U_f = U_f^{-1}$. A minus sign results if $f(x) = 1$, which is encoded as $(-1)^{f(x)}$. This comes from the second qubit due to $y \oplus f(x)$ for $f(x) = 1$. In other words, the qubit y is toggled if $f(x) = 1$. So, U_f applied to the state $|x\rangle(|0\rangle - |1\rangle)\sqrt{2}$ results in the state $(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)\sqrt{2}$. Now since $|x\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ we have, $|\psi_2\rangle$ (after the U_f) as $(|0\rangle/\sqrt{2})(-1)^{f(0)}((|0\rangle - |1\rangle)/\sqrt{2}) + (|1\rangle/\sqrt{2})(-1)^{f(1)}((|0\rangle - |1\rangle)/\sqrt{2})$. This is the same as $= \pm(|0\rangle + |1\rangle)/\sqrt{2}(|0\rangle - |1\rangle)/\sqrt{2}$, if $f(0) = f(1)$ and, $\pm(|0\rangle - |1\rangle)/\sqrt{2}(|0\rangle - |1\rangle)/\sqrt{2}$, if $f(0) \neq f(1)$. So, $|\psi_3\rangle$ after the last Hadamard operator is, $\pm|0\rangle(|0\rangle - |1\rangle)/\sqrt{2}$, if $f(1) = f(0)$ $(f(1) \oplus f(0) = 0)$ and, $\pm|1\rangle(|0\rangle - |1\rangle)/\sqrt{2}$, if $f(1) \neq f(0)$ $(f(1) \oplus f(0) = 1)$. So, $|\psi_3\rangle = \pm|f(1) \oplus f(0)\rangle(|0\rangle - |1\rangle)/\sqrt{2}$. Therefore, if we measure the first qubit, we get $f(0) \oplus f(1)$. We indeed get $f(0) \oplus f(1)$ with 100 % certainty. The value $f(0) \oplus f(1)$, is not computable with one evaluation of the function f in a classical boolean circuit; here we can compute it with just one U_f quantum operator.