Lecture Notes on Quantum Computation and Quantum Information Processing.

Instructor: Sudebkumar Prasant Pal

Scribe: Sima Das

23rd March 2004

1 Quantum algorithms : Part II

1.1 Deutsch-Jozsa Problem

Here we look forward to a generalization of Deutsch's problem. The following solution to the Deutsch-Jozsa problem requires the exploitation quantum parallelism as illustrated below. The input register x has n qubits. The boolean function f is a mapping from an n bit input to a 1 bit output, defined as $f : \{0,1\}^n \rightarrow \{0,1\}$. As in the Deutsch's problem, here too we count the number of times the function f has to be computed to solve the problem of determining whether f is balanced or constant. In the case where $n = 1$, we have the Deustch's problem and parity determination for f is identical to the determination of the constancy or balance in f. For $n > 1$, we wish to find whether all the 2^n possible values of x have $f(x)$ identical or whether exactly half (2^{n-1}) of them are of one value (zero or one).

Setting the input to $|0\rangle_n\ |1\rangle$, the application of the Hadamard operator on all the $n+1$ qubits as $H^{\otimes n+1}\ |0\rangle_n\ |1\rangle$ gives the state $1/2^{n/2}\ \sum_{x=0}^{2^n-1} |x\rangle$ $(|0\rangle - |1\rangle)/\sqrt{2}$. The application of U_f ($U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$) to this superpositioned state produces the state $1/2^{n/2}\ (\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle)\ (|0\rangle - |1\rangle)/\sqrt{2}$. The application of U_f acts as a controlled-f operator (very much like the CNOT operator) by toggling the second qubit, depending on the value of $f(x)$ for each x in the input superposition. Now a Hadamard operation on the first n qubits (input register) will lead to the state $H^{\otimes n} \otimes I$ $(1/2^{n/2}(\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle))\ (|0\rangle - |1\rangle)/\sqrt{2} = (1/2^n \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1}(-1)^{f(x)}(-1)^{x \cdot y}|y\rangle)$

$(|0\rangle - |1\rangle)/\sqrt{2}$
$= 1/2^n \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{f(x)+x.y} |y\rangle)\ (|0\rangle - |1\rangle)/\sqrt{2}$. Note that the n-qubit input register (or query register) has probability amplitude for $|0\rangle_n = 1$ (0), depending on f is constant for all x or balanced over all x. When f is balanced, all the 2^n terms add up to zeros with half of them being $1/2^n$ and half of them being $-1/2^n$. Otherwise, the amplitudes add up to give a value 1. So, we observe $|0\rangle$ if and only if f is constant. So, in a single run of the algorithm we are able to know whether f is balanced or constant with 100% certainty. However, if we would have employed a classical deterministic algorithm to determine whether f is constant, we would have required no lesser than $2^{n-1}+1$ queries or evaluations of the function f. For this specific problem exponential speedup is achieved proving the efficiency of quantum computing.