Electronics and Computer Science
a school of the University of Southampton

QUANTUM COMPUTING

Tianyue Gao (tg5v07@soton.ac.uk) MSc Nanoelectronics
12/05/2008
Project Supervisor: Dr Kees De Groot

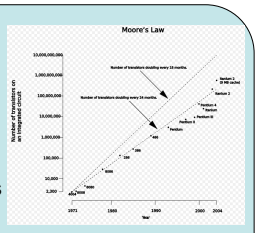
INTRODUCTION

As Moor's Low indicated in [1], the classical computer will reach the physical limit within one or two decades. The quantum computation is expected to replace the classical one due to its superiority, such as the characteristic of quantum logic gates, quantum superposition and parallelism which are presented by quantum bits (qubits) and quantum algorithms (especially Shor's and Grover's algorithms). In practical, to build a quantum computer is not a dream at present. There are lots of achievements, such as ion trap and NMR quantum computers, etc.

WHY WE NEED QUANTUM COMPUTING

1 Physical Limits

Moor's Law indicates that the density or content of chips, in another word, the number of transistors in an integrated circuit is doubling every two years, which is represented in right picture. Due to increasing exponentially, the number of transistors per integrated circuit results in the physical limit of computers. From the view of economy, the cost of building a chip plant is very huge, approximately several billion dollars, by which more and more companies are compelled to withdraw from the chip industry. For the aspect of technology, the complexity and error ratio are increasing exponentially along with the increasing density of lines on silicon.



http://en.wikipedia.org/wiki/Moore%27s_Law

2 Quantum Superposition & Parallelism

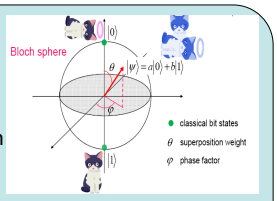
If a system with n qubits is initialized to be a starting state, superpositions of 2^n basis states are built [2], where n is the number of qubits. After this step, the process need operate 2^n states at the same time, such as calculating the value of function $f(x)$ with respect to different values of x simultaneously.

2a Qubits

The qubit is the the basic unit of quantum computation and information with the state of $|0\rangle$, $|1\rangle$, or the superposition of $|0\rangle$ and $|1\rangle$, which can be shown in right picture of Bloch sphere with Schrodinger's cat [3]. As shown in [4], qubits are the linear combinations of states, which is represented mathematically as below,

$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$

where α and β are amplitudes of states $|0\rangle$ or $|1\rangle$ respectively.



2b Qubit Gates

Corresponding to the NAND gate which is a universal gate of classical computation, arbitrary multiple-qubit gates can be acted by the composition of the controlled-NOT gate (CNOT gate) and single-qubit gate. As shown in [4], the CNOT gate is represented as followed:

$|A,B\rangle \rightarrow |A,B \oplus A\rangle$,

where A is the control qubit and B is the target qubit, and ⊕ can be seen as the XOR gate. If the control qubit is set to 0, the target qubit will keep original state; if the control qubit is set to 1, the target qubit will be flipped, which can be represented in the following truth table.

Control-qubit	Target-qubit	Result
0	0	00
0	1	01
1	0	11
1	1	10

The CNOT gate that is reversible can simulate the NAND gate, which means that arbitrary classical circuit can be simulated by the equivalent reversible circuit. This theory result makes sure that a quantum computer is able to process any computation of a classical computer.

2c Quantum Algorithms

Shor's algorithm: solving prime factoring and discrete logarithms of the large number N. For a n-qubit quantum computer $N=2^n$, using Shor's algorithm can reduce the operation count from $O(N^2)$ to $O(N\log N)$ where O is the order.

Grover's algorithm: optimal for quantum searching in an unsorted or unstructured database, and is quadratic speed-up. Compared with classical search algorithm, using Grover's algorithm can reduce the operation count from $O(N)$ to $O(N^{1/2})$.

In conclusion of Shor's and Grover's algorithms, we can find a significant advantage of the quantum computer. It is that the quantum computation is much, much faster than the classical one, which is represented in the following table.

	The number of operations	
	Factorization algorithm	Search algorithm
Classical	N^2	N
Quantum	$N\log N$	$N^{1/2}$
Ratio	$N/\log N$	$N^{1/2}$
N=100	50	10

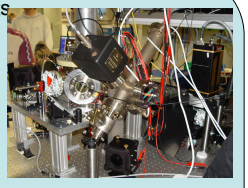
In left table, for the factorization algorithm and search algorithm of N=100, the numbers of operations in the quantum computer are 50 and 10 times less than in the classical computer, respectively.

CONCLUSION

As a result of superiority of quantum computing, quantum computers will replace silicon-based and DNA computers. Actually, a useful quantum computer in practical requires several hundred to thousand qubits in order to solve problems of the large number factoring and complex search. It indicates that the quantum computer has a tremendous prospect and a long distance away from the commercial applications. Perhaps, it will be achieved several decades, even a century later.

ACHIEVEMENTS

Ion trap quantum computers with qubits are based on electronic states of atomic ions confined by a combination of static and alternating electromagnetic fields [3]. The first ion trap quantum computer was built in 2005, which is shown in the right picture.



http://en.wikipedia.org/wiki/Image:Ionenfalle_-_Quantencomputer.jpg

http://en.wikipedia.org/wiki/Image:HWB-NMRv900.jpg

NMR quantum computers are based on the technique of NMR which is using radio frequency electromagnetic waves to manipulate and detect the states of nuclear spins [4]. This technique had applied successfully in quantum computers with 2-qubit system in 1998, even 7-qubit in 2001 [5]. The recent NMR spectrometers with 21.2 T magnetic fields that could produce 900 MHz NMR signals was built in Birmingham of United Kingdom in 2006, which is represented in left picture.

RECEFERCES
[1]. Manek Dubash, *'Moore's Law is dead, says Gordon Moore'*, *Techworld*, 2005. Available at (viewed on 27/03/2008): http://www.techworld.com/opsys/news/index.cfm?NewsID=3477
[2]. Joachim Stolze, Dieter Suter, *'Quantum Computing: a short course from theory to experiment'*, *Wiley*, Germany, 2004.
[3]. [Lecture Notes] Pro. Hiroshi Mizuta, *'Quantum Computing'*, *NSI Group, University of Southampton*, 2008
[4]. Michael A. Nielsen, Isaac L. Chuang, *'Quantum Computation and Quantum Information'*, Cambridge University Press, United Kingdom, 2004
[5]. *Wikipedia*, *'Timeline of quantum computing'*. Available at (accessed on 07/05/2008): http://en.wikipedia.org/wiki/Timeline_of_quantum_computing