Quantum Computing and its Efficiency

Srajit Mehrotra

Abstract: Quantum computers have put the best encryption algorithms in dilemma. They have provided a solution to the physical limits of conventional computers by using quantum mechanics and nature to explore the limits of computing and processing. Yet, quantum computers, as of now, cannot be used as a replacement for classical computers. Thus arises the question, are quantum computers really necessary? This paper focuses on providing a basic understanding about Quantum Computers and hence provide an answer to this question.

Introduction

The field of Quantum Computing first came to light due to the works of Paul Benioff[1] and Yuri Manin in 1980, Richard Feynman in 1982, and David Deutsch in 1985. In 1980 Yuri Manin proposed the idea of Quantum Computing. In 1981, at a conference co-organized by MIT and IBM, physicist Richard Feynman urged to build a quantum computer. He said "Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical."[2] Neil Gershenfeld and Isaac L. Chuang had predicted the problems that would eventually arise in conventional computers and explained the benefits and necessity of Quantum Computers. In their paper 'Quantum Computing with Molecules', 1980, they had stated, "Roadblocks to improving conventional computers will ultimately arise from the fundamental physical bounds to miniaturization… Yet the magic of quantum mechanics might solve both these problems."[3]

Qubit

A 'qubit' or 'quantum bit' on a quantum computer is equivalent to a 'bit' on classical computer. It is in either vertical polarization or horizontal polarization. Quantum superposition allows a qubit to be in both the states at the same time. There are two possible outcomes after measurement of a qubit, i.e. 0 and 1. But, before its measurement, qubits can also be in a superposition of both 0 and 1. Earlier it was suggested that, since the computer acts on the basis of information read or measured in a short time, the Heisenberg uncertainty principle limits the information processing rate of the computer and hence, temperature lower than that of cosmos (2.7K) are used (0.015 K) to remove the noise and corrupted readings of the electrons.

Qubits are represented by Dirac notation or 'bra-ket' notation e.g. <a|b>, where the left element (<a|) represents vector in dual space (all linear functionalities are possible) while the right one (|b>) represents vector space (Vector operations are possible). When two quantum bits (or electrons) interact, there are four possible states of electrons, i.e. 00, 01, 10, and 11. In such a case, there is no certainty over the state of electrons and they can be in any one of the states or even all of the states at the same time. Quantum logic gate is a basic quantum circuit operating on a small number of qubits, like logic gates on classical bits. A quantum gate manipulates an input of superposition, rotates probabilities and produces another superposition as its output.

Qubits have their own magnetic field and when external magnetic field is applied, just like tiny compass needles, they align with that external field. This property is known as spin. This is the lowest energy state, spin down state or 'zero' state. With some energy, qubits can be aligned exactly against the external field. This is

the highest energy state, spin up or 'one' state. Before we measure it, qubits can be in both states, i.e. in a quantum superposition. A weird and nonlocal property that qubits exhibit is entanglement. Entanglement or 'Spooky action at a distance' (as described by Albert Einstein) is a close connection that makes each of the qubits react to a change in the other's state instantaneously, no matter how far they are apart. This means, with measuring just one entangled quantum bit, we can deduce the position (properties in general) of all the qubits entangled with it[4].

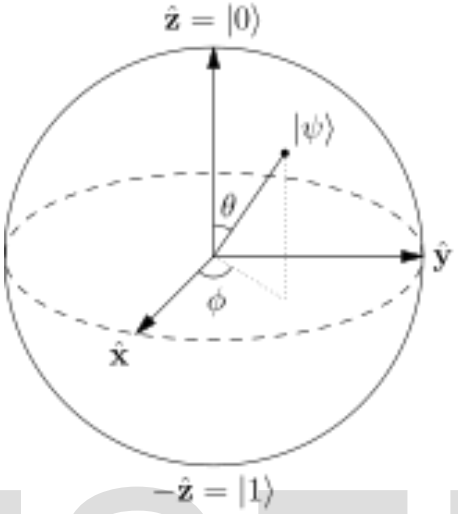

Fig 1: Bloch sphere representation of state of a Quantum bit.

Quantum Computer

"*By taking advantage of nuclear magnetic resonance, scientists can coax the molecules in some ordinary liquids to serve as an extraordinary type of computer." – Neil Gershenfeld and Isaac L. Chuang [3].* Classical computers are reaching approaching their fundamental limits. As transistors are shrinking to a size of only a few atoms, electrons may just transfer to the other side of the blocked path through quantum tunnelling. Hence, we need more powerful computers that do not have these physical and fundamental limitations. The need of Quantum Computers was recognized for the first time (as recorded) in 1981, at a conference co-organized by MIT and IBM, physicist Richard Feynman urged the world to build a quantum computer.

Quantum Computers are computational systems that make direct use of quantum-mechanical phenomenon, such as spin, superposition, and entanglement to process data. A number of qubits taken together is a qubit register. Quantum computers perform calculations by manipulating qubits within a register. This means that a quantum computer is a computational unit that consists of various qubits and performs logical quantum operations on them. A single qubit can be in zero state, one state or in a state of superposition, i.e. two coefficients are required to store the result in a classical computer. In the same way, two interacting quantum bits can be in any quantum superposition of four states (00, 01, 10, and 11), i.e. four coefficients are required to store the result in a classical computer. Further, in general a computer with n qubits can be in any superposition of maximum 2^n different states simultaneously. This means that up to 2^n coefficients will be required to store the result in a classical computer, moreover a classical computer can be only in any one of the 2^n states at a time[1][2].

Quantum computers consist of various quantum logic gates. In fact, it is a basic quantum circuit for quantum computers. A quantum gate usually works on a small number of qubits. They are equivalent to logic gates for digital circuits, but unlike many logic gates, quantum gates are reversible. A quantum gate takes superposition of qubits as input, rotates probabilities, and gives another superposition as its output. Various types of quantum gates are:

1. Hadamard gate
2. Pauli gate
3. Phase shift gates
4. Swap gates
5. Controlled gates
6. Toffoli gate
7. Fredkin gate
8. Ising gate
9. Universal Quantum gates

Theoretically, these gates cannot be constructed.

A quantum computer sets up qubits, applies quantum gates to entangle them and manipulate probabilities. Then measures the result by collapsing superpositions into a sequence of 0 and 1. Each of the qubit is in a superposition state and hence, many sequences of 0 and 1 are calculated simultaneously. Then, by use of proper gates and entanglement, the required sequence is determined.

Quantum Computers Vs Classical Computers

Speed of quantum computers in processing increases exponentially with the sincrease in qubits and hence are faster in processing as compared to classical computers. But, here is a catch, Quantum computers are efficient in performing calculations and kind of computational parallelism but basic tasks like writing a document or watching videos would be slower than classical computers. This is so because classical computers store data in 0 and 1, while qubits first need to be converted to 0 and 1, from superposition state, before storing data. Further advantages of quantum computers are:

Parallel Speedup:

Parallel computing systems offer enormous potential for significant runtime speedups over computation by a single CPU core. However, many computational tasks cannot be efficiently parallelized. Quantum computers can efficiently accomplish that task in significantly less time. The runtime speedup realized from switching from sequential to parallel computers is captured by the following formula, a refinement of Amdahl's Law:

$$T(P) = (1 - \alpha) \cdot T_{seq} + \alpha \cdot T_{par}(1/P) + T_{over}(P).$$

T(P) is the time to run a process on 'P' parallel cores. '(1 − α)' is the part of code that cannot be parallelized and 'α' is the proportion of code divided among 'P' parallel cores. Overhead is due to remote access, i.e. memory access, synchronization, etc. As the number of parallel cores increase, overhead increases and hence more time is taken. Further, the time primarily depends upon 'α', which is always less than 100% and hence the parallel speedup is always less than the ideal-speedup[5].

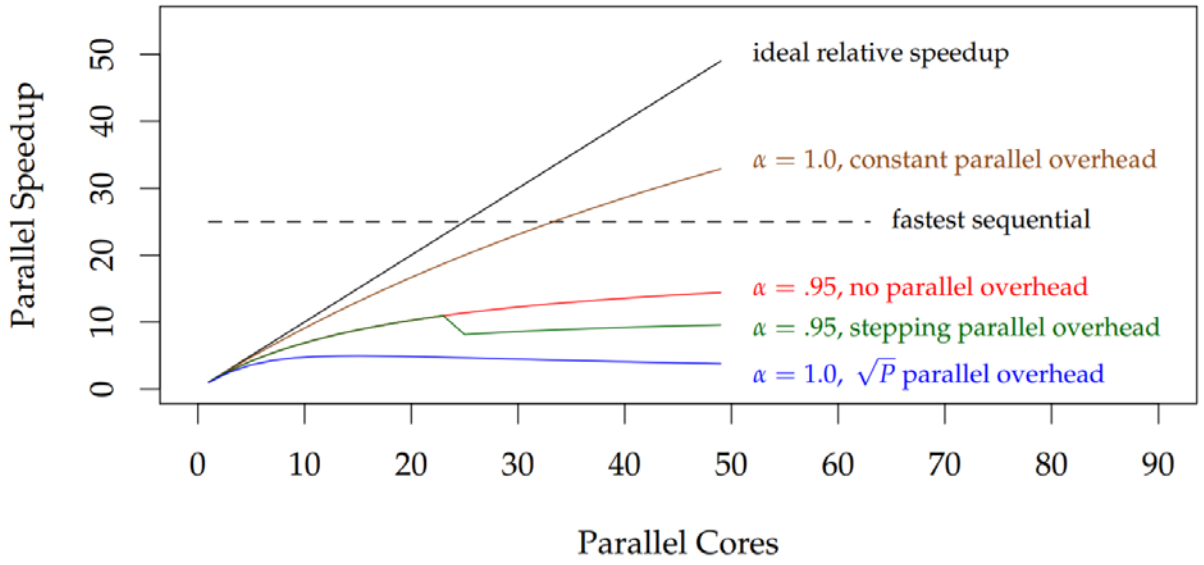

Fig 2: Parallel cores Vs Parallel speedup, where 'α' is the proportion of code divided among parallel cores.

Computational Power Consumption

Power consumption due to computation is a serious issue. The power required for computation increases with the increase in number of cores. It also includes the higher power consumption by cooling systems, as more cooling is required in more powerful computers. The world's most powerful supercomputer as of 2017 — China's Sunway TaihuLight — has an efficiency of 2.2 gigaflops per watt. More efficient computation can be achieved by the use of specialized coprocessors (usually Graphics Processing Unit). As an example, consider the 2017 state-of-the-art NVIDIA DGX-1, a highly optimized GPU. It is capable of 170 teraflops at an efficiency of 53 gigaflops per watt.

By contrast, quantum computers are way more energy efficient than classical computers (including supercomputers). This is so because the maximum part of the energy is used for maintaining extremely low temperature for the processor. For example, consider D-Wave 2000Q, a 2000-qubit system. Almost all of the power (less than 25 kW) drawn by it is used by the cryogenic refrigeration. The power consumption has been constant since the introduction of the first quantum computer, and is expected to stay constant as the computation power grows with future quantum computers[6].

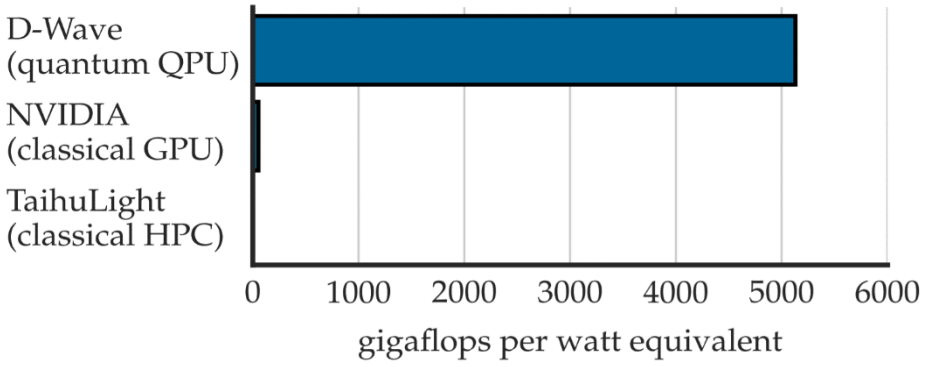

Fig 3: Compared power efficiency of, as of now, themost powerful computers.

Conclusion

The future of computing requires increased energy and time efficiency, which will depend upon increased dependence on specialized coprocessors including GPUs as we are nearing the end of Moore's Law. Quantum Processing Units (or Quantum Computers) have showed significant advantage over classical computers in terms of both, time and energy efficiency. Hence, the problems that arise due to limits(diameter of wires, Moore's Law, time efficiency and increasing power consumption) of classical computer can be easily solved using Quantum Computers, which makes them a necessity.

References

[1] Paul Benioff, "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines," Journal of statistical physics, August 1971.
[2] Dario Gill, "The Dawn of Quantum Computing is Upon Us," At a conference co-organised by IBM and MIT, May 2016.
[3] Neil Gershenfeld and Isaac L. Chuang, "Quantum Computing with Molecules," Scientific American, June 1998.
[4] Benjamin Schumander, "Quantum coding," Physical Review A, 1995.
[5] D-Wave, "Limits on Parallel Speedup for Classical Ising Model Solvers," 2017.
[6] D-Wave, "Computational Power Consumption and Speedup," 2017.