Tadrash Shah* and Chintan M Bhatt**

*MS in Computer Science, Technology Analyst, Bank of America, New York
**Asst. Professor, Chandubhai S. Patel Institute of Technology, CHARUSAT

Quantum Computing: Fusion of Physics and Computers

We are talking about a novel way to incorporate physics into the computers. Silicon and semiconductor phenomena have long since dominated the computer design and hardware, now we shift gears and come around with a totally new computer unknown to our predecessors. Google and NASA have teamed up for this paradigm shift and as expected, the results are mind-boggling. A Quantum computer has been designed by Google and NASA, fabricated by D-Wave Systems and installed at NASA – California.

Fig. 1: Superposition analogy. Source: Snapshot from Google's Video (https://www.youtube.com/watch?v=CMdHDHEuOUE)

History

Our classical computers have been around since long but Quantum computer are the most recent development. If we go by the Moore's Law then every 18months the processor capacity doubles; in that case we can only imagine the amount of processing power we shall need by the need of this century. Thanks to Paul Bernioff at Argonne National Laboratory who theorized the quantum computers in 1981. Actually he came up with quantum Turing Machine where in the bits can be stored as *qubits*. Qubits are actually the superimposition phenomena of quantum physics. At a particular memory location a bit can have value either 0 or 1 in our current classical computer, whereas qubits can be the values both 0 and 1. This allows many parallel calculations on the processor at the same time. As a memory location can have multiple values at any point in time, different values can be used for different calculations, hence allowing inherent parallelism.

We are not keen on going into too much detail about the timeline of development of quantum computers post 1982 as that would make this article a plain history informative. We rather aim at making it more interesting,

Background and Concepts

As said earlier, by Moore's law, by the year 2020 or 2030 we shall need the circuits on microprocessor measured on atomic scale. And hence logically the next generation should steer us to quantum computers where we harness the power of atoms and molecules to perform memory and processing tasks. We use several concepts of quantum physics which are discussed as under:

1. **Superposition:** As discussed in the opening already, with QC (we shall refer quantum computer s as QC henceforth) we store the data as qubits where the memory can have the values 0 or 1 or a superposition of 0 and 1. The superposition is actually the symbols both 0 and 1 and all the points in between them. As a QC can have multiple states at the same time they can be multifold powerful than today's classical systems. This can be quantified with a fact as this : a 30-qubit system is equivalent to 10 teraflops of today's typical desktop system.

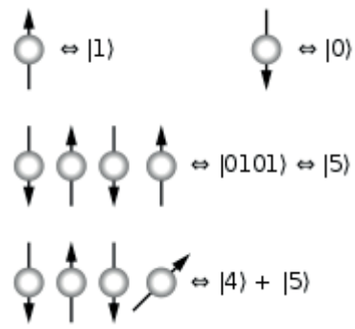

Fig. 2: qubits can have multiple spins. Source: Wikipedia

Look at the diagram below. We know that atom can have only two spins determining the value to be 0 or 1 (or at some places we choose them as +1 and -1). In case of the qubits, they can spin in any direction, allowing us values 0 and 1 at same time or any value between them.

2. **Entanglement:** When we try to look at a qubit in superposition we can only find whether the value is 0 or 1 whereas it actually would be having both the values. So in such a case, we may not directly look at the value of qubit. We need some indirect way to know the value of a qubit. As the law of entanglement goes, we can make two atoms closely related by applying outside force to two atoms. When this happens, the second atom takes on the properties of first atom. And from the second atom, applying some quantum physics methods, we can know the value of our atom of interest.
3. **Multiverse:** Quantum computing does not deny, rather support the idea of parallel universe. John Gribbin, a popular science writer believes that QC can work because they get their processing power from some other parallel universe. That said, can be interpreted as if you successfully build a quantum computer, you have all the computers from some other universe at your disposal. Well, to us, this may seem a little vague as we do

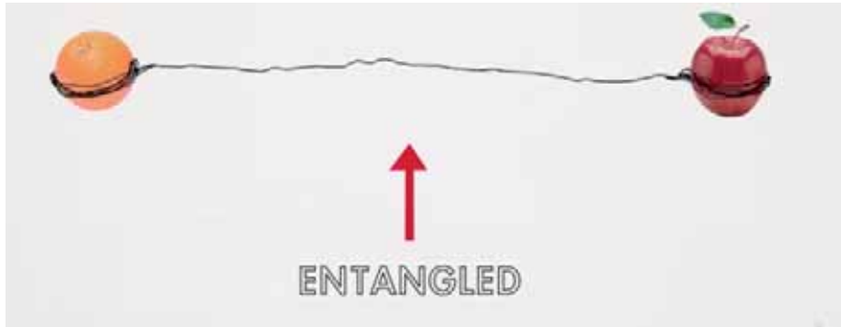

Fig. 3: Entanglement. Source: Snapshot from Google's Video (https://www.youtube.com/watch?v=CMdHDHEuOUE)

not know the cosmology behind all this; yet what should fascinate us is the processing power of these QCs.

4. **Tunneling:** The idea of quantum tunneling, i.e. a manifest of Heisenberg's uncertainty principle which ports the data to some other universe is also said to be used in design of quantum computers. The atoms, electrons, photons or other such subatomic particles are seen to cross a barrier without seeming to have crossed it. The MIT Technology Review reports to have simulated quantum tunneling on a QC. That is to say that the mathematical behavior of one computer is reproduced on the other hence looking at one system tells you all how another one would behave. (http://www.technologyreview.com/view/427931/first-simulation-of-quantum-tunneling-on-a-quantum-computer/)

All these concepts, due to brevity of the mention here, may seem so uncanny and weird to the field of computing but trust us, if you can, these behavior of subatomic particles in a QC can open the avenues of astro-physics that we have only heard off or scientists have only imagined thus far.

Quantum computing has now created a new class of algorithmic problems in the complexity theory too called BQP and BPP viz. Bounded error, Quantum, Polynomial time and Bounded error, probabilistic, polynomial time. These are the problems which can only be solved using probability theory in polynomial time. And these probabilistic problems can only be solved on a QC as it is the only set of problems QC can solve.

Applications Development

Being the newest research development there are a few applications that are being targeted to the use of Quantum computers. As many researchers of the field also agree, we still do not know the right kind of the question to ask this computer. We are still not fully aware of the applications that can really harness the computing power of this magnitude. One of the many applications that are being developed by the pioneers such as Google is, Google aims to use these for improving its web search and advertising capabilities. Given the large amount of data that is generated in search and adverts, Google is optimistic about making correct use of this computing power. Given that Google earns its more than two-thirds of revenue from advertisements, it wants to ensure its advertising technology can outperform that of any other company.

The biggest and complex problem in mathematics is to factorize a large number into two prime numbers. This is an important problem because almost all encryption methods are based on this problem. The quantum computer must be quickly able to identify these prime numbers. If quantum computers become commonly available, which surely is not going to happen soon, the current security and encryption algorithms are bound to fail. Currently the security algorithms that we use be it RSA or SHA, are bound only by the computations that they require. But with this magnitude of computing power, they can easily break-in to.

Our favorite and a wonderful example has been given by Google in a short video they have made for introducing this concept to the world (https://www.youtube.com/watch?feature=player_embedded&v=CMdHDHEuOUE)–

You want to travel from Delhi to Mumbai and want to visit multiple cities enroute. Now this is a kind of classical optimization problem (similar to travelling salesman?). Now the route can be decided on basis of several parameters: cheapest ticket, least time, least number of tolls, shortest route, travelling in buses with good legroom, travelling in vehicles that provide seamless Wi-Fi connectivity, depending on best weather to visit a particular city, carbon footprint of cities, minimum layover times, meals provided, pet restrictions, seat availability and the list goes on and on and on. This can generate vast vast vast amount of data and then it needs to be consolidated and results to be generated. If these are the number of parameters that we want to consider then the data computation goes beyond the capabilities of our current systems. But the quantum computers promise to deal with these.

With the optimism to make the self-driving cars and smart-homes a reality, Google has partnered with University of California, Santa Barbara. These concepts, being of the domain of Artificial Intelligence, require analysis and consolidation of humongous amount of data and thus huge amount of processing power which can only be provided by QC. Just for a gag, may be an algorithm made for QC can outsmart Deep Blue in game of chess; again purely because of its computing abilities.

In a nutshell, the prime interest is to apply QC to machine learning algorithms and thus to use it to understand and solve virtually any problem of the said domain, ranging from cure of a disease to understanding weather patterns to theoretical physics.

Challenges

There are various challenges that are foreseen with QC. Well, we are no extra-ordinnaire to list them all but depending on the understanding and case studies that have been done to write this article, we can list a few to give you all a flavor of them.

1. A problem is because you have deal with the subatomic particles, you can change their values inherently without even knowing it. Hence, the data integrity becomes critical. If we try to look at a qubit in superposition,

it will return us the values either 0 or 1 where as it should be operating at a value in between 0 and 1 or both the values.

2. Quantum computer can run only probabilistic algorithms and that too with a rigid limit that the answer/ solution will be right with high probability. Hence, our classical algorithms that we have been using it so far cannot be used directly, not even the overwhelmingly comptatutional part of classical algorithms be accelerated.
3. Current 16-qubit QC that has been designed by D-Wave systems requires a rigorous temperature control to be maintained on the chip. And hence, thought the chip is quite small in dimensions, the housing is quite huge. And thus expensive to maintain and operate.
4. There are people who doubt whether QC designed and fabricated by D-Wave systems really operate as a QC or not. As we cannot look inside the hood of quantum computing because that would disturb the computation reason being that when we see the state of atom which is its spin then the superposition gets disturbed as explained earlier), these doubts are raised and so far there is no way out found to prove it. And this also questions the stability of the quantum states.
5. Programming of these computers has steered D-Wave systems to a new software architecture and language. Every algorithm fed in should be probabilistic one as already noted. Microsoft is also taking interest in the same at Microsoft Research. David Wecker from Cambridge is associated with Microsoft for this project and has already implemented a software architecture called LIQUi which translated high level program, representing quantum algorithm, to technology specific lower level program.

Current Research

Researchers of Princeton University have built a rice grain-sized device laser power-driven by single electrons tunneling through artificial atoms known as quantum dots. They built the device which uses about one-billionth the electric current needed to power a hair dryer by exploring how to use quantum dots, which are bits of semiconductor material that act like single atoms, as components for quantum computers. Currently researchers are doing research on following topics:

- Quantum Internet
- Quantum Chips
- Quantum Computer Networks
- Quantum Machine Learning (including concept of Big Data)

Conclusion

So, we are taking the macro to the micro level; or actually we are taking the phenomena of Universe to the chips in the computer. Of course, the currently built computers are of the size of a room, keeping the legacy of their ancestors going. But eventually they will evolve to fit into our laptops. We no longer live in an age where we see or need an entire lifetime to see the research output materialize especially not if it is to build a machine.

References

[1] http://www.theguardian.com/science/2014/mar/06/quantum-computing-explained-particle-mechanics
[2] http://mashable.com/2013/10/13/google-quantum-computing-video/
[3] http://computer.howstuffworks.com/quantum-computer3.htm
[4] http://www.theguardian.com/commentisfree/belief/2009/oct/06/multiverse-quantum-computers-philosophy
[5] http://en.wikipedia.org/wiki/Quantum_computing
[6] http://getpocket.com/a/read/740917422
[7] http://www.nas.nasa.gov/quantum/
[8] http://www.dwavesys.com/tutorials/background-reading-series/introduction-d-wave-quantum-hardware
[9] http://phys.org/news/2015-01-rice-sized-laser-powered-electron-bodes.html

About the Authors

Tadrash Shah has completed his B.E. in Computer Engineering from Gujarat Technological University in 2012. Prior to starting his M.S. in Computer Science from State University of New York at Stony Brook, he worked on projects with IIT-Gandhinagar, IIT-Bombay, IIM-Ahmedabad and United Nations. He has been serving as Technical Program Committee Member on several conferences and has manyresearch publications. Currently he is working at Technology Analyst at Bank of America Merrill Lynch in New York. His research areas include - High Performance Computing, Algorithms and Database. Teaching also interests him apart from his coveted corporate job.

Chintan M Bhatt has received B.E. and M. Tech. Degrees from Gujarat University (CITC (now CSPIT)) and Dharmsinh Desai University in Computer Engineering. He is currently pursuing PhD in Computer Science. He is a member of CSI, AIRCC (Academy & Industry Research Collaboration Center), IAENG (International Association of Engineers), ISTE, IEEE, SDIWC, EIA etc. His areas of interest include Data Mining, Web Mining, Networking, Mobile Computing Security and Software Engineering. He has more than 4 years of teaching and research experience. He is working as a Technical Program Committee member/Reviewer in many reputed international journals/conferences.