Quantum Computers, or, You Will Be Disappointed, Crushed and Have No Privacy

What Quantum Computers Can Do, and More Importantly What They Can't

Ever since the idea of a quantum computer was proposed - that is, the idea of using superimposed quantum particles to perform classical calculations - science fiction speculators and the laymen have been equally enthusiastic about theorising, "What can these miracle machines do?" Although there is unarguably much work to be done to actually make quantum computers a practical reality, this essay attempts to give a solid answer to what these quantum computers can do *better* than classical ones and what they can do only *slightly better*. This will focus on the applications in terms of cryptographic applications such as breaking codes as well as general security issues such as ensuring that data is kept private.

How Do Quantum Computers Work?

To explain how quantum computers are useful, one of the most important things to do is examine how they work, if only cursorily. While a classical computer works on bits set to either 1 or 0, a quantum computer works on quantum bits (qubits). Due to the principles of quantum physics, which state that a quantum particle can be in many states when it isn't being observed, these qubits can be in a state of 1, 0 or a mixture of both. This is encoded in a property of the particle known as spin, which can be set to integer quantities (± 1, 0) or in fractions of integers. This superimposition of states effectively allows the user of the quantum computer to utilise parallel processing on the one computer.

So What Can These Things Do Better?

They Can Break Codes Better. Much Better.

In 1994, a Bell Labs researcher named Peter Shor published the solid proof that quantum computers could essentially make even the most tight military security obsolete. Although this pronouncement might seem slightly melodramatic, the algorithm enclosed in Shor's paper effectively demonstrated how to use a quantum computer to break the RSA codes used to secure the military and the corporations of the world. Say that we have a large number with 300-odd digits, or (depending on the security level) possibly thousands of digits. What Shor proved was that all these encoded numbers have patterns that can eventually be teased out by using a technique known as Fourier analysis[1]. This technique looks for patterns of a certain "frequency" - a pattern of frequency 12, for example, repeats every 12 digits. These patterns are the key to finding the

[1] Gribbin, John. Computing With Quantum Cats. Print.

prime factors of these large numbers, and thus the key to breaking the RSA code. A classical computer could take longer than *the age of the Universe* to find the underlying pattern for numbers hundreds of digits long, due to the complexity of the calculations involved. However, a quantum computer works by superimposition of its quantum bits, as elaborated above. By superimposing the qubits to calculate for frequency 1, 2, 3, 4, etc. until the maximum possible frequency, the quantum computer can effectively reduce the computation time needed from "the age of the Universe" to "four minutes". This effectively makes the RSA algorithm practically obsolete due to its heavy reliance on the innate (but inevitably classical) difficulty of finding the prime factors of a large number. This means that security systems relying on these kinds of algorithms like RSA would become obsolete and easily crackable by anybody with a quantum computer. However, keep in mind that quantum computers are incredibly fragile as well as expensive and difficult to make, placing a tight bottleneck on quantum codebreaking.

They Can Keep Codes Better. *Infinitely* Better.

Most of the unique properties of quantum computers revolve around the unique properties of quantum particles used in these computers and how to exploit them as effectively as possible. One of the most notable exploits involving these quantum particles is the creation of a quantum Internet. Two particles can be *entangled*, that is, a change to one particle will result in the opposite change to the other particle. Most notably, the change will travel faster than light[2]. Let us now assume that one particle is on the ground, while the other one is in space. Due to the "no-cloning rule", an exact copy of the first quantum particle cannot be made; however, we *can* transfer the first quantum particle's state to the second quantum particle, in the process destroying the first particle. While changes made through entanglement move faster than the speed of light, the speed of the transfer of the information used to actually perform that process is limited to light speed, meaning that ansibles are impossible for the time being[3]. The quantum Internet, however, would be almost completely secure. Bugs placed on the computer itself would decohere the particles, alerting the user that an attacker was eavesdropping on their communications, meaning the only way to eavesdrop on communications through the quantum Internet would be through actually eavesdropping on the satellite itself. Considering the difficulty in actually sifting through so much data at a time to search for one probably non-unique transmission (even with the use of a quantum computer), this would render the quantum Internet practically impenetrable.

[2]Nielsen, Michael A, and Isaac L Chuang. Quantum Computation And Quantum Information. Cambridge: Cambridge University Press, 2010. Print.

[3]Kaye, Phillip, Raymond Laflamme, and Michele Mosca. An Introduction To Quantum Computing. Oxford: Oxford University Press, 2007. Print.

And What These Things Do Mediocrely

Solving Most NP-Class Problems

Even though quantum computers do have an increased parallel processing ability, you mostly don't see the gigantic increases in processing speed that you do with the RSA factorisation problem. Most of the hype around quantum computers was originally initiated by Grover's algorithm, which is an algorithm designed to in essence reverse a function - that is, if we can have a function y = f(x), Grover lets us find x given y. Grover's algorithm is O(n1/2), while a classical computer could only solve it in O(n). Despite this seemingly huge computation speedup, Grover's algorithm doesn't lend itself well to certain situations. Let's take the example of chess, where we want to build an algorithm that does a depth-first search (goes as far as possible along each branch before backtracking) on as many moves as possible within a given time limit (in Deep Blue's case, it was 3 minutes). A naive understanding of Grover's algorithm would say that if Deep Blue could examine 250 million possibilities in that time, then a quantum computer could calculate 250 million squared possibilities, i.e. 6.25 x 1016 possibilities. The caveat with this is that Grover's algorithm generally doesn't work for problems with limited choices (due to the fact that chess moves are heavily limited by the rules), meaning that a quantum computer only performs a little better when compared to Deep Blue. This is because chess belongs to a general family of problems known as NP-class problems[4] (standing for non-polynomial time), including the famous "travelling salesman" problem and factorisation. Without a specialised algorithm to solve one of those problems more efficiently, these problems are extremely inefficient to solve on any computer, quantum or otherwise.

How Does This Relate To My Project?

Quantum computers, once they go into wide circulation, would fundamentally revolutionise the way computing is done. There's a large amount of unexplored territory in terms of algorithms and programming languages that could be developed for quantum computers, and this would by necessity change what would be taught in courses such as Software Design and Information Processing especially. This would necessarily require me to overhaul the content significantly, provided I'm still alive and able to draw at the time. The means by which the content would be taught could also change. As these are quantum computers, they can exactly simulate a universe that runs on quantum principles unlike classical computers[5], meaning that teaching the quantum principles behind these computers, *using these computers* with the use of virtual reality could be a fully viable method of educational use of computers, removing the need for such

[4] "P And NP". Cs.uky.edu. N.p., 2016. Web. 16 Mar. 2016.

[5] "Quantum Computing For Everyone | Michael Nielsen". Michaelnielsen.org. N.p., 2016. Web. 16 Mar. 2016.

projects as these, as visual notes can be condensed into virtual reality projects. In short, quantum computers would have a significantly destructive, although far-off effect on my project in terms of relevance and its use.