Quantum Computers

Introduction:
Computers are probably the most important invention of the entire 20th century. They have progressed faster than any other technology in the history of earth and created a new age in human life. But deep down, they haven’t changed much in principle since Babbage’s adding machine. They perform one operation at a time and store a single value in each byte. Any increase in performance to the machines results in a linear increase in performance. A tinker toy calculator improves on the same scale, as does a Turing machine. As long as computers improve in a linear fashion, they cannot truly “catch up” to problems which have a running time greater than linear and so existing problems can always be extended out to larger input sizes as computer speeds increase. This is the inherent and unconquerable flaw in conventional computers.[2]

This flaw is easy to exploit and allows for both strength and weakness. For example RSA encryption, relies entirely on classic computers’ inability to perform functions that increase at a rate greater than linear, in this case factoring the product of two primes. The longest product of primes ever factored, done more as a proof of the difficulty of such a task than for any real practical purposes, was 129 digits long and took months to complete (as of 1999). Most RSA keys are up to and beyond 200 digits in length. Cracking such a
key would take several years. If a classical computer were to attempt to factor a number 1000 digits in length, it would take longer than the universe is old.[1,8]

This is where quantum mechanics steps in. Quantum mechanics relies on the dual-state nature of subatomic particles to encode and operate on multiple pieces of data simultaneously. Whereas it would take months for a classical computer to crack a single RSA key, a quantum computer could crack every RSA key in use in less than a day. By storing and manipulating multiple pieces of data in a single processing cycle, quantum computers can get an exponential rate of growth with improvements to performance.

The problem with classic computers is that they are bound by classic physics. An object can be only one thing at any given moment. So in order to achieve the exponential speed they do, quantum computers must operate in an environment where classic physics do not apply. By manipulating the energy of states of subatomic particles instead of the electrical charge of silicon circuits, quantum computers can instead operate in the realm of quantum mechanics.[4]

Quantum mechanics are almost like a religion. The nature of subatomic particles is beyond anything we experience or possibly can experience in our daily lives; instead, one must simply trust that events are happening as they are described. The nature of quantum mechanics has been proven in laboratory settings, but that doesn't make it any easier to accept. While in the normal world objects only have one state, quantum mechanics allow an object that normally has two states, e.g. the up vs. down spin of an electron, to exist in a
superposition, where both states exist simultaneously. Thus an electron can have
an up spin, down spin, or both at the same time, and so can be used to
represent a 0, 1, or both simultaneously. This “coherent superposition” is the
very basis of quantum mechanics. This is a very unusual concept, and it is even
more so in that cannot be observed directly. Of course, it gets weirder.[2]

**Qubits:**

The unit of a quantum computer is the qubit. The qubit can be any variety
of particles or states, so long as the particle is subject to quantum mechanics.
However, a lone qubit is not especially useful. It can represent a 0, 1, or both a 0
and a 1. By adding more qubits, we can develop a register of qubits, or as I
prefer to call them for brevity’s sake – qabytes (note that qabytes can be any
size, not just 8 qubits). However, a qubyte all on its own is not much use. When
separated, the superpositions of the qubits cannot be used together, and so the
whole system is relegated to a very, very tiny yet still very classic computer. The
power of a quantum computer comes not only from its ability to store many
pieces of data in one qubyte, but also in its ability to manipulate all of that data
in a single quantum cycle. Thus, in order to utilize the qubits’ quantum nature to
their full potential, they must be “entangled.” Entangling the qubits brings all of
their superpositions together to allow the qubits to simultaneously represent
every single number an equal number of normal bits can represent.[1] Once
entangled, the individual qubits lose their individual meanings and can now only
be interpreted as a whole. A qubyte comprised of \( n \) qubits can be thought of as a
Boolean array of length $2^n$. Every number that the qubyte represents at that moment is represented as a true in the array. But once superpositioned qubits are entangled, they cannot be directly observed. Doing so will collapse the superpositions into a random state and destroy the data.[2]

Once the qubyte is superpositioned and entangled, it can be used in operations. The especially impressive fact about quantum computers is that an entire qubyte, no matter the size, can be manipulated as a whole in one cycle. Whereas a classic computer must process each bit one by one, a quantum computer uses a specially designed beam of light to perform a single action on multiple qubits of the qubyte simultaneously.[8] The action can affect all, some, or just one of the qubits at a time. By completing so many tasks at once, a quantum computer can store and manipulate numbers far beyond the capabilities of a classic computer. For example, a qubyte comprised of 250 qubits can store $2^{250}$ numbers, which is more numbers than there are atoms in the universe. To top it off, a quantum computer can then process those practically-infinite supply of numbers in one processing cycle.

Of course, all this power doesn’t come easy. There are a host of difficulties associated with functional quantum computers. The first is the difficulty of extracting the information from a qubyte. As mentioned earlier, trying to directly observe a superpositioned qubit will cause it to degenerate into a random state, 0 or 1. Further complicating the matter is that when an operation is performed on a superpositioned qubyte, it will remain
superpositioned. So this leaves a superpositioned qubyte that cannot be observed to discover the results of an operation performed on it. Instead, the individual result to be extracted from the qubyte is enhanced without directly observing the qubyte. This will encourage the qubyte to collapse into the answer upon observation. This feat has been accomplished in laboratory settings, but the physics involved are far more complex than this paper needs (or I can understand).[2]

By far the greatest challenge facing quantum computing is the problem of decoherence. As one would imagine, something as tiny and delicate as a qubyte is very susceptible to outside interference. The more qubits that are entangled together, the easier it is for the entire qubit to degenerate into a random mess due to the passing of some stray ray of energy. This challenge has proven so difficult that to date only a 4-qubit qubyte has been developed. However, the 4-qubit qubyte is so fragile that any operations performed on it cause it to fall apart and lose its superpositioning. Only 2-qubit systems can be operated on without losing their coherence. The energy purity needed to maintain qubites large enough for quantum computers to be practical is so high as to be infeasible. Fortunately a counter was developed.[4]

In 1995 Peter Shor and Andrew Steane at Oxford University developed a system to counter large qubyte’s susceptibility to decoherence. By running multiple quantum computers simultaneously on the same data, the quantum computers can form an error-checking system, similar to a RAID-5 array for hard
drives (although RAID-5 was nonexistent when this system was developed). The
quabytes of each machine are constantly compared to each other and when one
machine differs from the others, it is reset to have the same data that the other
quantum computers do at that moment. More quantum computers arrayed
together allow for more of the machines to fail at any given moment without a
loss of data, which then allows for larger quabytes to be used. An individual
machine can lose its data millions of times per second and the quantum
computer array can still correctly process the data.[2]

Quantum Algorithms:

Should all of these difficulties be overcome (which is not assured) several
algorithms have already been developed to take advantage of quantum
computers’ amazing power. Peter Shor (the same Peter Shor who developed the
redundancy system above) developed the first of these algorithms in 1994.[4] As
described earlier, factoring is an immensely difficult problem for classic
computers, with an exponential run time. Even the best factoring algorithm for a
classic computer using Fourier transformations runs in exponential time. Fourier
transformations use a sort of “getting warmer” technique to determine the
location of the target, but their exact code requires incredibly complex
mathematical formulas that are beyond the scope of this paper. Shor’s algorithm
is essentially the quantum version of this algorithm, meaning it can check every
element in the array of possible solutions to the Fourier transformation at once.
This effect is similar to dividing the runtime by n, and so turns this problem into
a problem of running time $O(L(n)^3)$ where $L(n)$ is the number of digits needed to represent $n$. However, the problem uses quantum Fourier transformations to find the factors of $n$, and Fourier transformations do not guarantee a correct result or even a result at all. By running the algorithm through a second algorithm with runtime $O(lgL(n))$, one can guarantee an error free result, meaning that if an answer is found, it will be the right answer and yield an inconclusive answer very rarely. Thus the final runtime for the algorithm is $O(L(n)^3lgL(n)).[4,3,6]$

Lov Grover has also developed one of the basic quantum algorithms, this one for unstructured searches. Unstructured searches are those where the data has no existing structure to it, such as an unsorted array. Conventional computers can only perform this task using a linear search, which takes $O(n)$ time. Grover’s quantum algorithm takes just $O(\sqrt{n})$ time. A simplified version of this algorithm says that the qubyte, composed of $2^x$ qubits where $2^x \geq n$, is given a value of 1 for every value contained in the set of values P. The value of the number to search for is enhanced 4 $(\pi/4 * \sqrt{n})$ times to make sure it is the one found when the superposition is observed. This is done using a series of quantum logic gates. It should be noted that when the data is encoded into the superposition its content is unknown. The quantum logic gates function as a sort of quantum AND, meaning that the desired result will be enhanced for all its bits with each iteration, while the incorrect answers will be enhanced for only a portion of their bits (this is a simplification, but is the general idea of the algorithm). Furthermore, Grover’s technique for unstructured search can be
applied to structured searches and turn $O(\lg(n))$ algorithms into $O(1)$ algorithms on a quantum computer (the exact technique for doing so differs with each algorithm).\[4,6\]

These algorithms do not apply to all NP-complete problems. Unless a quantum algorithm for the problem can be designed, the problem cannot be brought into quantum P and will be run in the same manner on a quantum computer as it is on a silicon computer. While computer scientists will continue to devise quantum algorithms that can turn non-P (i.e. not solvable in polynomial time) problems on classic computers into P problems on quantum computers, it is still possible that some problems will never become P problems for any computer design, quantum or otherwise.\[4\]

**Possibly Impossible:**

Quantum computers may never be a reality. The difficulties with making such a complex, delicate, and expensive computer available for common use may prove insurmountable. But the research is still worthwhile. Just like the research of NASA has created great strides in earth-bound science, so does quantum computing create technological advances in other areas of science. For example, the entangled qubits that make up a qubyte are linked in more ways that just data sharing. They can also transfer energy between each other no matter the distance involved. Thus entangled qubits could provide a means for instantaneous, infinite-distance communication (like the Holonet from Star Wars). It is very strange phenomenon, but it is in fact possible, and proven, due
to the unifying nature of entangling. By entangling the qubits, they almost become a single quantum bit, thus the ability to operate on every qubit at once. Energy is applied to the transmitting qubit. The transmitting qubit absorbs the energy. However, because the qubit is entangled with another receiving qubit, the two qubits are essentially a single particle, even if they are separated. Thus the energy wave is transferred to the second receiving qubit instantaneously because it is in fact the same particle, despite the distance separating the qubits, as the transmitting qubit received the energy wave at the exact same moment that the transmitting qubit received the energy wave. However, this transmission cannot be tapped into. Trying to tap in to the energy at either end will collapse the superposition and so no data can be received.[2]

Even more intriguing is the nature of matter and energy at that level. At quantum levels, the lines between energy and matter are blurred. Thus, if the energy transferred between two entangled qubits can be converted back into matter at the other end, one would have a functional teleporter straight out of Star Trek. While storing the data necessary to accurately rebuild a human being, or even a single atom, using this technique would be immense, that’s what those 250 qubits are for, right?[7]

Conclusion:

Quantum computers hold amazing potential. They can make old encryption techniques worthless but make new ones that truly are unbreakable, not just slow to solve. They have the ability to allow for whole new database
designs that can take advantage of the qubites to store more data in less space and manipulate it as a whole, allowing for search times that put even Google to shame. They hold the secret to instant, ultra fast communication, or even teleportation. However, classic computers will never be completely outmoded. Quantum computers are only needed for large tasks that normal computers balk at. Performing a quantum operation requires a significant amount of setup time as the data is encoded and entangled in the quantum computer. Even after the data is encoded, it must be maintained millions of times a second across multiple quantum computers for a single operation to be completed. A personal quantum computer is a distant possibility at best. But while they may never become as far reaching as their silicon brethren, quantum computers still have the potential to change our world on the same scale as ENIAC did over fifty years ago.


