Quantum Computation

Siddharth Srinivasan

2019

Abstract

Over the past few decades, the emergence of quantum mechanics and computation has changed the way we look at computation. In the 1980s , Bennet and Grassard showed that quantum systems could be used to build very secure cryptographic keys and ciphers, while Feynman and Manin showed how entaglement could be used in computation. In this article, we explain the basics of quantum computation, how it works, quantum measurement, how quantum computers can break current classical cryptographic ciphers through various algorithms, and quantum error correction.

1 Introduction and Single Qubit Systems

The Quantum Bit, or qubit, is the fundamental unit of quantum computing information, just as normal classical bits are in classical computing. Just as in normal computer science theory, we don't really care how qubits are realized(as it can be done in many ways), just as we don't when talking about normal bits(voltage, switches, etc.). In general, a qubit is just the space of all polarization states of a photon. In quantum mechanics, the polarization state of a photon is modeled by a unit vector, a linear combination of the horizontal and the vertical vectors, or $|\uparrow\rangle$ and $|\rightarrow\rangle$ (that bra-ket notation is conventional in quantum mechanics, a general notation system called Dirac's notation). In this way, an arbitrary polarization of a photon would be something like

$$|v\rangle = a|\uparrow\rangle + b|\rightarrow\rangle$$

and the coefficients are called amplitudes, and when a and b(nonzero), the photon is said to be in *superposition* of the two states. In this way, if we have a polaroid(polarization filter), the probability of absorption is $|b|^2$, and the probablity of passing through is $|a|^2$ if the filter prefers $|\uparrow\rangle$, and any photon that passes through will now be polarized in only the preferred direction. A qubit's state coefficients can be complex, if needed, as well.

1.1 Dirac Notation

We now introduce Dirac's Notation. Dirac's bra-ket notation is used throughout quantum physics to represent states and their transformations. In Dirac's notation, a 'ket' such as $|x\rangle$ refers to a vector of the state of the quantum system. A vector $|v\rangle$ is a linear combination of other vectors $|s_1\rangle, |s_2\rangle$... iff there exist complex numbers a_i such that $|v\rangle = a_1|s_1\rangle + a_2|s_2\rangle$...
We say that a set of vectors generates a space if every vector in the space is a linear combination of vectors in the set. As consistent with conventional linear algebra, define the span, bases. An inner product $\langle v_1|v_2\rangle$, or a dot product is defined on a pair of vectors in a space such that $\langle v|v\rangle$ is a nonnegative real number, $\langle v_1|v_2\rangle = \overline{\langle v_1|v_2\rangle}$, and $\langle a(\langle v_2| + b\langle v_3|)|v_1\rangle = a\langle v_1|v_2\rangle + b\langle v_3|v_1\rangle$, and

two vectors are orthogonal if their product is 0. A set of vectors is 'orthonormal' if they are all of magnitude 1 and are all orthogonal to each other.

When talking about qubits, we must always define a standard basis $|0\rangle, |1\rangle$ which respect to which all statements made must be fixed and consistent. While normal bits can only take two values, the qubit can take on any value that is the superposition or linear combination of the standard basis. We can use normal matrix notation for vectors once the bases have been specified.

In Dirac's notation, the transpose conjugate of a ket $|v\rangle$ is called a bra and is written as $\langle v|$, where if a_i are the coefficients of $|v\rangle$, then $\bar{a_i}$ are those for $\langle v|$. We can think of bras and kets as rows and column vectors, respectively.

We now define the standard inner product. Given two vectors

$$|x\rangle = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \ldots \end{bmatrix}, |y\rangle = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \ldots \end{bmatrix}$$

their standard inner product is defined to be the number that results from multiplying the conjugate of x with y:

$$\langle x|y\rangle = \langle x||y\rangle = \sum_{i=1}^{n} \bar{x_i} y_i$$

When the vectors are real, this is just the normal dot product. Dirac's notation allows for some clever wordplay, as the inner product of two vectors, which is just the product of a bra and a ket, is called a bracket.

2 A Quantum Key Distribution Protocol

We can now start to construct a key distribution protocol that has no classical computing analog. As we know, establishing secure keys is a fundamental part of cryptography, and there are two general classes of keys, public private pairs, and symmetric.

Quantum Key distribution protocols establish symmetric keys between two parties, and here we'll call them Alice and Bob. Protocols like these can basically be used anywhere classical key agreement systems like Diffie-Hellman are used. The difference is that while systems like Diffie Hellman are fairly secure against most classical attacks, the discrete logarithm problem is tractable on a quantum computer(Shor's algorith will be discussed later).

We will now first talk about the very first quantum key distribution protocol, invented by Charles Bennett and Gilles Brassard, known as BB84. What BB84 does is establish a secret key between Alice and Bob, wherein the key is a sequence of bit values 0 and 1, and BB84 ensures that is Alice and Bob do not detect anything wrong while in progress, then with high probability the key is secret, but it cannot give a guarantee.

There are two "channels" in BB84, or pathways for information exchange. There is one normal bidirectional classical channel, and one unidirectional quantum channel. The quantum channel is such that it allows Alice to send a sequence of qubits to Bob, suppose in the form of polarization states of photons, and both channels can be listened in on by our villain Eve, the eavesdropper.

To begin, Alice uses any method she wants to generate a random sequence of classical bits. Alice then randomly encodes each individual bit in the sequence by randomly choosing for each bit one of the two agreed upon bases: the standard basis with

$$0 \rightarrow |\uparrow\rangle$$

$$1 \rightarrow |\rightarrow\rangle$$

or the Hadamard Basis :

$$0 \rightarrow \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle)$$

$$1 \rightarrow \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\rightarrow\rangle)$$

and she sends the encoded sequence of photons to Bob. Bob measures the state of each photon by randomly picking either of the two bases to measure on, and they check that Bob has received and measured every photon Alice has sent. When their choice of bases agree, then Bob's measured value is the same as Alice's. If they chose different bases, there is a fifty percent chance that they agree. Since Eve eavesdrops on all conversations, Alice and Bob simply throw out all bits in which they don't agree on their bases, and the remaining bits are used as their key.

3 Quantum Algorithms

The majority of quantum algorithms use some quantum analogs of classical computing as part of their system. Many start by creating a superposition, and then inputting that into a quantum version of a system that computes a certain function. This setup is called quantum parallelism, and at this state it is no better than a classical system, but it gives a state in which the algorithms are actually built on.

3.1 The Walsh Hadamard Transformation

We start by looking at the Walsh Hadamard Transformation, the first step of quantum parallelism. It is a generalization of the Hadamard Transformation, and applied to all the qubits in a state $|0\rangle$, it generates a superposition of all of the 2^n basis vectors for n qubits, and can be viewed as the binary representation of numbers from 0 to $2^n - 1$:

$$(H \cdot H...)|0000000...\rangle = \frac{1}{\sqrt{2^n}}(|000...\rangle + |000000..1\rangle ... + |11111...1\rangle) = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$$

We call $H \cdot H...H = W$, the Walsh Hadamard Transformation, which applies the hadamard transformation to each qubit in a n-qubit state.

3.2 Quantum Fourier Transform

The Quantum Fourier Transform(QFT), is similar to the discrete fourier transform. If we take the amplitudes a_x of a state of $\sum_x a_x|x\rangle$ as $a(x)$, then the fourier transform takes $\sum_x a(x)|x\rangle \rightarrow \sum_x A(x)|x\rangle$, where the $A(x)$ are the coefficients of the discrete Fourier transform of $a(x)$, with x between $0, 2^n - 1$. For $N = 2^n$, the transform is defined as:

$$U_f : |k\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} e^{\frac{2\pi ikx}{N}}|x\rangle$$

. As we can see, the transform for $N = 2$ is just the Hadamard transformation: $|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

3.3 Shor's Algorithm

Inspired by Simon's Algorithm, in 1994, Peter Shor found a bounded polynomial time algorithm for factoring integers. The fastest classical algorithm known, the number field sieve, requires $O(e^(m^{1/3}))$ steps where m is the size of the integer, superpolynomial time. Shor's result was a monumental discovery.
Shor's algorithm provides a way to find the period of a function. It uses quantum parallelism to produce a superposition of all the values of the function in one step, and then uses the fourier transform to create a state in which the amplitudes mostly are in states close to multiples of the reciprocal of the period. Thus, with very high probability, it yields the period by classical means, which can be used to factor a number.

3.4 Reduction of Factoring to Finding the Period

We know that the order of an integer a modulo M is the smallest positive integer such that $a^r = 1 \pmod{M}$, and if none exists, the order is infinite. Consider the function $f(k) = a^k \pmod{M}$. Since $a^k = a^{k+r} \pmod{M}$ iff $a^r = 1 \pmod{M}$, for a relatively prime to M, the order r is the period of f. Thus, if r is even, we can write that $(a^{r/2}+1)(a^{r/2}-1) = 0 \pmod{M}$. As long as neither of those two is a multiple of M, both of them have nontrivial common factors with M, and thus we can factor M by: Randomly choosing an integer a and determine the period r of $f(k) = a^k \pmod{M}$. If r is even, we use the Euclidean Algorithm to find the gcd of $(a^{r/2}+1)$ and M. Repeat.
Finding the period is what Shor's algorithm seeks to solve.

3.5 Outline

Here, we give the general outline of Shor's algorithm:
1. Randomly choose an integer a such that $0 < a < M$, where M is the number you wish to factor. Use any efficient method, such as the Euclidean Algorithm, to determine if a and M are relatively prime, and if they are, proceed, and if not, we have found a factor already.
2. Use quantum parallelism to compute $f(x) = a^x \pmod{M}$ on the superposition of inputs, and apply a quantum fourier transform to the result. It suffices to consider input values $x \in 0, ..., 2n1$, where n is such that $M^2 \leq 2^n < 2M^2$
3. We measure, and with high probability, a value close to a multiple of $\frac{2^n}{r}$. Call this v.
4. Use classical computing methods to conjecture a period p from q.
5. If q is even, use the Euclidean algorithm to find the gcd of $(a^{q/2}+1), M$ or $(a^{q/2}-1), M$, to determine whether they have any nontrivial factors.
6. Repeat if necessary

When we have our parallelism superposition $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle$, it makes it simpler to just measure the second register which returns a value u for f, simplifying this to: $C\sum_x g(x)|x\rangle|u\rangle$ where $g(x)$ returns 1 when $f(x) = u$ and 0 when not

3.6 Run Through of Shor's Algorithm for 21

We illustrate how Shor's algorithm works by walking through the process for $M = 21$. Since $M^2 = 441 < 2^9 < 2M^2 = 882$, we take the inputs as $x \in 0...8$. Since the ceiling of $\log M$ is 5, the

second register requires 5 inputs.
Thus, we have our state of :

$$\frac{1}{\sqrt{2^9}}\sum_{x=0}^{2^9-1}|x\rangle|f(x)\rangle$$

a fourteen qubit state, with 9 inputs in the first and 5 in the second register. According to protocol, assume our random integer we choose is $a = 11$. Assume that when measuring the second register, we get that $u = 8$. Then, suppose that the measurement of the state returns $v = 427$. Since v and 2^n are coprime, we use the continued fraction method to obtain a guess for q, the period.
When the period r is a power of 2, the fourier transform returns exact multiples of $2^n/r$, in this case, the value of $v = k\frac{2^n}{r}$ for some k. Here, we can just reduce $\frac{v}{2^n}$ into lowest terms, into j/r given that j, r are coprime as they usually are, and extract r from the denominator. If r is not a power of 2, we need some additional steps.
In general the quantum fourier transform gives only approximate multiples of the frequency. When it is not a power of 2, we can use the continued fraction expansion of $v/2^n$ to get a good estimate. To use the continued fraction, there is an algorithm as outlined by Shor: Let $[x]$ be the greatest integer less than x. Using the following sequences: $a_0 = [\frac{v}{2^n}], \epsilon_0 = \frac{v}{2^n} - a_0, a_i = [\frac{1}{\epsilon_i - 1}], p_0 = a_0, p_1 = a_1a_0 + 1, p_i = a_ip_{i-1} + p_{i-2}, q_0 = 1, q_1 = a_1, q_i = a_iq_{i-1} + q_{i-1}$, compute the first fraction p_i/q_i such that $q_i \leq M \leq q_{i+1}$. In the case of $v = 427$, we use this to obtain $q = 6$ as our guess for the period, as $q_2 = 6, q_3 = 253$. Since 6 is even, $(a^{6/2} - 1) = 1330, (a^{6/2} + 1) = 1332$ are likely to have a shared factor with 21, and so we have that gcd(1332, 21)=3, gcd(1330, 21) = 7, and we're done.

4 Conclusion

As time goes on, it is inevitable that as a race, we will get faster, stronger, smarter, and more powerful. Just as 100 years ago, when what millions carry in their pocket was a fantasy, we live to see what the future holds. Quantum Computing is one of the most cutting edge and innovative ideas and technological advancements in our era, and it has major implications for the future. Will RSA be broken soon? Will we have to reinvent all our securities and systems? These questions linger in the wake of innovation, and it left to us to decide what we do next.

References

[1] S. Rubinstein-Salzedo, "Cryptography," *Springer*, 2018.

[2] E. Rieffel and W. Polak, "Quantum computing: A gentle introduction," *The MIT Press*, 2018.

[3] V. Scarani, "Six quantum pieces." World Scientific Publishing Co. Pie. Ltd., 2010.