# 1 Background Theory

## 1.1 Quantum bits

The fundamental unit of classical information is the bit, which can be in one of two states: 0 or 1. In quantum information we promote the concept of a classical bit to the quantum bit, or qubit for short. Qubits can occupy a continuum of states between 0 and 1, weighted by complex coefficients $a$ and $b$; in general, we can write the state of a qubit $q$ as

$$|q\rangle = a\,|0\rangle + b\,|1\rangle\,.$$

The ket $|q\rangle$ is referred to as its state (or often wavefunction), and the coefficients $a$ and $b$ are referred to as probability amplitudes. While a qubit occupies this coherent superposition of states $|0\rangle$ and $|1\rangle$ in isolation, when the qubit is measured it will collapse to either $|0\rangle$ with probability $|a|^2$ or $|1\rangle$ with probability $|b|^2$. Since probabilities sum to 1, it's required that $|a|^2 + |b|^2 = 1$.

The probability amplitudes are complex numbers, meaning that there would be four degrees of freedom in the general form for $|q\rangle$:

$$|q\rangle = |a|e^{i\theta_a}\,|0\rangle + |b|e^{i\theta_b}\,|1\rangle = e^{i\theta_a}\left(|a|\,|0\rangle + |b|e^{i\phi}\,|1\rangle\right), \quad \phi = \theta_b - \theta_a.$$

However, we have the condition $|a|^2 + |b|^2 = 1$, removing one degree of freedom. Further, the inclusion of the overall phase factor $e^{i\theta_a}$ has no physically observed consequences for single qubits, leaving us with just two degrees of freedom. We can construct a helpful visualization of the possible qubit states using a Bloch sphere, with the north pole ($\theta = 0$ corresponding to $|0\rangle$ and the south pole ($\theta = \pi$) to $|1\rangle$:

$$|q\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle\,.$$

A more intuitive representation is with spherical coordinates, where the state $|q\rangle$ is represented by the point vector

$$\vec{q} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)\,.$$

Most of the important applications in quantum information come from systems of multiple qubits. For example, the general form for a system of two qubits $q$ and $q'$ can be written as

$$|q, q'\rangle = a_{00}\,|0,0\rangle + a_{01}\,|0,1\rangle + a_{10}\,|1,0\rangle + a_{11}\,|1,1\rangle\,,$$

where again the $a_{ij}$ are complex coefficients, and $\sum_{i,j}|a_{ij}|^2 = 1$. Measurements on a multiple qubit systems behave similarly, where a measurement will collapse the qubits to a state $|x, y\rangle$ with probability $|a_{xy}|^2$. Quantum systems grow in complexity much quicker than classical systems, requiring $2^n - 1$ coefficients to describe the system as opposed to $n$ coefficients.

## 1.2 Entanglement

Two-qubit systems are of particular interest and importance in quantum information science. For example, consider the state

$$|q, q'\rangle = \frac{1}{2}\left(|0,0\rangle + |0,1\rangle - |1,0\rangle - |1,1\rangle\right).$$

By careful inspection we can see that this state can be written as the tensor product of two qubit states $|q\rangle$ and $|q'\rangle$:

$$|q, q'\rangle = |q\rangle\,|q'\rangle\,, \quad |q\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right), \quad |q'\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right).$$

This means that we may measure the first qubit $q$, obtain either $|0\rangle$ or $|1\rangle$ with equal probabilities, and the second qubit $q'$ will remain in its superposition of states. However, if we consider the state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0,0\rangle + |1,1\rangle\right),$$

we find that it's not possible to write $|\Phi^+\rangle$ as a product $|\Phi\rangle\,|\Phi'\rangle$. This is what we call an entangled state. The physical consequence of an entangled state is that making a measurement on one of the qubits will force the second qubit into a specific state as well. For example, if we measure the first qubit of $|\Phi^+\rangle$ and find it in the state $|0\rangle$, the second qubit must also be in the state $|0\rangle$. This state is one of four well-known entangled states known as Bell states:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0,0\rangle + |1,1\rangle\right), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|0,0\rangle - |1,1\rangle\right),$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0,1\rangle + |1,0\rangle\right), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0,1\rangle - |1,0\rangle\right).$$

Entangled pairs are incredibly important in quantum information. Many applications revolve around two parties making clever measurements on a shared pair of entangled qubits, allowing them to share information more efficiently and securely.

So far we've treated qubits as an abstract mathematical model, but qubits in all their glory are in fact physically realizable, along with entangled pairs. Further, in physical qubit models there is no mention of distance, meaning that entangled pairs exhibit this immediate wavefunction collapse no matter how far apart they are. Applying classical intuition, it seems that if we separate a pair of entangled qubits by an arbitrarily large distance, the wavefunction collapse can violate locality! This phenomena was the source of much uneasiness for physicists in the 20th century, earning the name "spooky action at a distance."

# 2 Important Applications

## 2.1 Superdense coding

One application of entanglement is the concept of superdense coding. By sharing an entangled pair of qubits, one party may communicate two bits of classical information to another party by sending a single qubit. Let the two parties, Alice and Bob, each have one qubit in the entangled state $|\Phi^+\rangle$:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0_A, 0_B\rangle + |1_A, 1_B\rangle\right).$$

Suppose Alice has two bits of classical information she wishes to communicate to Bob. These can be either 00, 01, 10, or 11. By applying one of four unitary transformations on her qubit Alice can encode this information into the entangled state. If she sends her single qubit to Bob, he can perform a CNOT operation on his qubit (with Alice's qubit as control) and Hadamard transformation on Alice's qubit and obtain a definite state corresponding to these classical bits. Alice's specific transformation is a matter of which Bell state they share; her transformation just changes their state to a different Bell state if necessary.

For example, suppose Alice wants to send the information 10 to Bob. She would apply the quantum phase-flip gate $Z$ to her qubit (the unitary transformation corresponding to this specific bit pair), transforming the entangled state $|\Phi^+\rangle$ to $|\Phi^-\rangle$:

$$\frac{1}{\sqrt{2}}\left(|0_A, 0_B\rangle + |1_A, 1_B\rangle\right) \quad \rightarrow \quad \frac{1}{\sqrt{2}}\left(|0_A, 0_B\rangle - |1_A, 1_B\rangle\right).$$

Alice would then send her qubit to Bob, and he would first apply the CNOT operation to his qubit:

$$\frac{1}{\sqrt{2}}\left(|0_A, 0_B\rangle - |1_A, 1_B\rangle\right) \quad \rightarrow \quad \frac{1}{\sqrt{2}}\left(|0_A, 0_B\rangle - |1_A, 0_B\rangle\right).$$

Next, he applies the Hadamard transform to Alice's qubit:

$$\frac{1}{\sqrt{2}}\left(|0_A, 0_B\rangle - |1_A, 0_B\rangle\right) \quad \rightarrow \quad \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0_A\rangle + |1_A\rangle)\,|0_B\rangle - \frac{1}{\sqrt{2}}(|0_A\rangle - |1_A\rangle)\,|0_B\rangle\right) = |1_A, 0_B\rangle.$$

We see that the resulting state is exactly the state corresponding to the bits 10, the information that Alice was attempting to send. Thus by sending just one qubit she has communicated two classical bits of information.

## 2.2 Quantum encryption

An important realization in the previous scenario comes from supposing that some third party wishes to eavesdrop on the conversation, attempting to intercept Alice's qubit in transit. If this third party, say Charlie, were to then make a measurement of Alice's qubit they would obtain no information; it turns out that $\langle\psi|C_A \otimes I_B|\psi\rangle$ gives the same result for every Bell state $\psi$, meaning it's impossible for Charlie to determine which Bell state Alice constructed through her transformation. This is because Charlie does not have Bob's qubit to work with as well.

Further, because of the no-cloning theorem in quantum mechanics, it would be impossible for Charlie to intercept this qubit and make a measurement on it without Alice and Bob noticing. Thus not only does quantum encryption ensure the security of their communication, it also alerts them of someone else's presence.

## 2.3 Quantum Fourier transform

The discrete Fourier transform is an extremely useful tool in many fields, transforming a set $x_i$ of complex numbers into a set $y_i$ by

$$y_k = \frac{1}{\sqrt{N}} \sum_j e^{2\pi i jk/N} x_j.$$

We can define a quantum Fourier transform by constructing a unitary transformation $U$ acting on basis states $|i\rangle$ as

$$U|i\rangle = \frac{1}{\sqrt{2^n}} \sum_k e^{2\pi ijk/2^n} |k\rangle .$$

Using quantum algorithms to compute the Fourier transform turns out to be exponentially faster than computing it classically. This quantum Fourier transform can be used to efficiently solve many problems, one of which being the problem of factoring very large integers using Shor's algorithm. Since factoring large integers is one of the bottlenecks in breaching secure communications through classical networks, the quantum encryption we discussed earlier is all the more important.

# 3 Achieving a Physically Realizable Network

## 3.1 Entangling qubit pairs

We first need to find a physical model for qubits before we can go about developing an entire quantum network. Since physical particles are inherently quantum mechanical it's not difficult to obtain single qubits, but entangled pairs of qubits aren't trivial to produce. As a simple case we can consider a pair of spin 1/2 particles that together produce a composite system of total spin 0. Then we know if one of the particles is measured to have spin up, the other must have spin down. If both particles have equal probability of being spin up or down, then we form the entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left( |\uparrow, \downarrow\rangle + |\downarrow, \uparrow\rangle \right).$$

This is just a simple introduction, and not the typical method for generating entangled states. More often we see pairs of photons entangled through their polarizations through a method called spontaneous parametric down-conversion. This creates a pair of photons with perpendicular polarizations:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left( |H, V\rangle + |V, H\rangle \right).$$

There are multiple other physical models of qubits, but the general consensus is that photons are the best candidates as qubits. By constructing physical systems that are sensitive to photon polarizations we can realize the quantum algorithms described previously.

## 3.2 Distributing entangled photons

Now we have our entangled photons, we need a way of distributing them between different nodes in the network. The most efficient way of doing this is to utilize existing telecommunications fiber optic infrastructure. However, fiber optics are subject to exponential losses with increasing distance making it practically impossible to reliably transmit single photons over hundreds of kilometers. For example, if Alice sends Bob single photons at a rate of 10 GHz over a distance of 10 km, Bob will receive ~95% of the photons. Increasing the distance to a less modest 500 km, Bob now receives ~1 photon per second. At 1000 km, Bob's rate of reception drops to 1 photon every 300,000 years!

An important property of classical information is that a classical signal can be relatively easily amplified making it possible to establish long distance communication. As for quantum information, since the "no-cloning theorem" prevents duplication of an arbitrary unknown quantum state we cannot hope to amplify a quantum signal. This poses a difficult obstacle to transmitting qubits over long distances. Although the challenges of decoherence and fiber optic losses are dauntingly significant, the problem of amplification can be circumvented by what is known as a quantum "repeater." A quantum repeater does not amplify a signal, but rather exploits the bell state measurement to perform "entanglement swapping" which serves to repeat the quantum state while avoiding direct measurement and hence wave function collapse.

## 3.3 Quantum Repeaters

The function of a true Quantum Repeater is to extend the range of quantum communication. There are three main components of a repeater: (1) Entanglement Sources (2) Bell State Measurement (BSM) Devices (3) Quantum Memories. An entanglement source is necessary to generate deterministic single photon pairs, in our case, through spontaneous parametric down conversion. BSM devices are required for entanglement swapping and quantum memories are needed to store quantum information while entangled links are prepared.

Consider two entanglement sources both emitting an entangled pair of photons, say $|A_1\rangle$, $|A_2\rangle$ and $|B_1\rangle$, $|B_2\rangle$. Let each individual qubit be sent to a respective quantum memory (four in total). The quantum memories must be able to store an entangled state without disturbing it and hence destroying the fragile quantum information. If $|A_1\rangle$ and $|B_1\rangle$ are then sent to a BSM device the measurement will result in collapse to one of the four bell states and will simultaneously project the remaining stored qubits $|A_2\rangle$ and $|B_2\rangle$ into an entangled state despite having never interacted directly. This is how

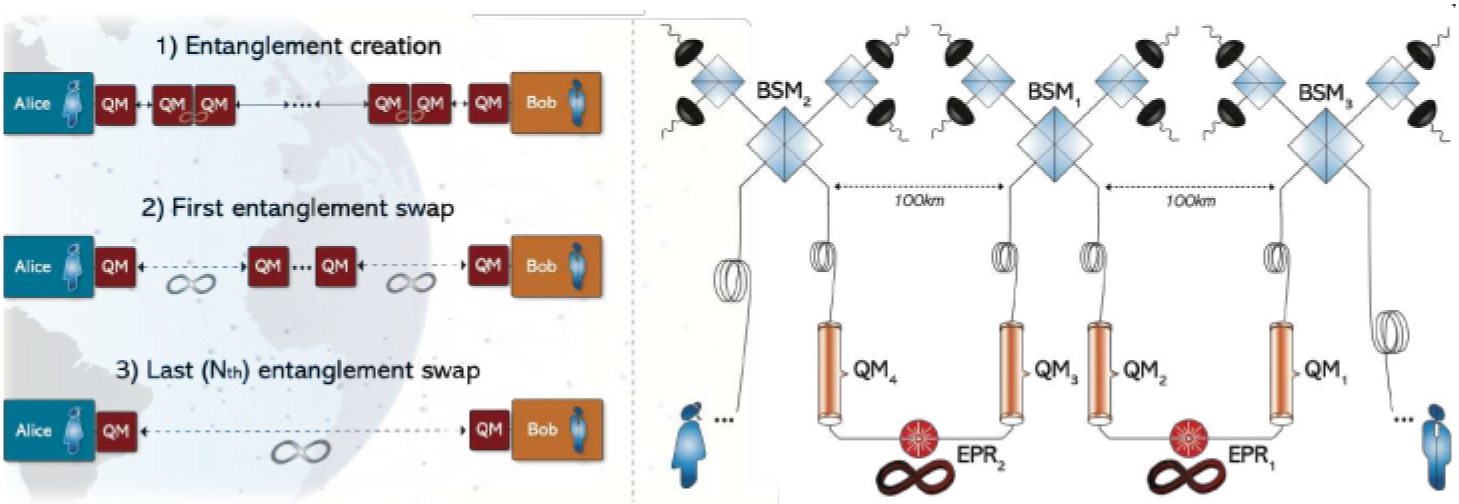

Figure 1: This figure shows two entangled photon pairs being sent to four individual quantum memories. The photons from QM$_2$ and QM$_3$ are sent to BSM$_1$ and measured such that their information content is destroyed. As a consequence of this BSM, the entangled state is shared with photons in QM$_1$ and QM$_4$. This process can then be repeated allowing the entangled state to be transmitted over long distances.

the process of entanglement swapping is accomplished such that a quantum signal may be repeated without violating the no-cloning theorem. With the combination of these three quantum systems (ent. sources, BSM devices, quantum memories), a network of repeaters could be established in either a linear or hierarchical fashion to extend quantum communication over an arbitrarily long distance.

## 3.4 Quantum Internet

Although a true Quantum repeater has yet to be demonstrated it wont be long before they become a reality. Our team of quantum information scientists at Stony Brook University have been working to establish a network of room-temperature quantum devices capable of being integrated into existing telecommunications infrastructure. Once a fully functional quantum repeater exists it will possible to link more of such devices together into an interconnected web of repeaters. Utilizing these quantum networks along with methods of quantum encryption it will be possible to develop an ultra-secure unhackable ”quantum internet”.