SoS Report

Ashwajit Singh

August 2023

Contents

1 Qubits

Qubits (or quantum bits) are analogous to the bits we see in classical computation and are the fundamental unit in quantum computation. However unlike a classical bit which can either be a 0 or 1, a qubit is a superposition of two states, i.e., it is of the form

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{1}$$

where α and β are complex numbers, and $|0\rangle$ and $|1\rangle$ are called computational basis states. While it exists in this form as a superposition, it is impossible to find α and β directly on measuring like we would with a classical bit. When we attempt to measure a qubit's state, we get $|0\rangle$ with a probability $|\alpha|^2$ and $|1\rangle$ with a probability $|\beta|^2$. Therefore a qubit does not exist in discrete states (unlike a classical bit) until it is measured. While their behaviour seems counter-intuitive, qubits are real and can be realised by the ground state and excited state of an atom. As we reduce the time we shine light on this atom to excite the electron, an electron can be moved to a superposition of these two states. Clearly, if we were to measure the state of the electron, it cannot exist as a superposition and would collapse to either the ground state or the excited state.

Geometrically, we can visualise qubits by rewriting the Eq. 1.1 as

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

Since $e^{i\gamma}$ has no observable effects, we can ignore it and write it simply as

$$|\psi\rangle = cos(\frac{\theta}{2})\,|0\rangle + e^{i\phi}sin(\frac{\theta}{2})\,|1\rangle \tag{3}$$

This can now be represented as a unit sphere called the Block sphere with ϕ and θ representing the angles. We can extend this idea to multiple qubits as well, keeping in mind that the probabilities of the various states must sum up to 1.

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle \tag{4}$$

Here, while we can measure both qubits and therefore obtain one of the four states, we can also measure a subset of the qubits. For example, if we were

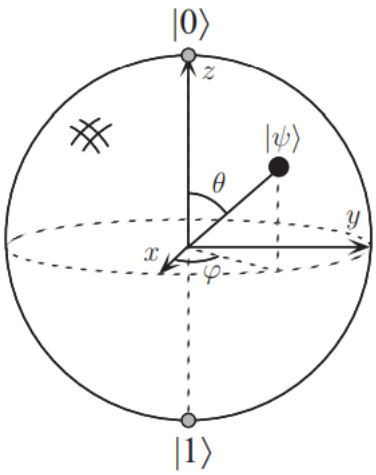

Figure 1: Bloch sphere

to measure the first qubit, we would get 0 with a probability of $|\alpha_{00}^2| + |\alpha_{01}^2|$, and the state after this measurement would be

$$\frac{\alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle}{\sqrt{|\alpha_{00}^2| + |\alpha_{01}^2|}} \tag{5}$$

where the denominator ensures that the state is normalised. Here while

The Bell state or EPR pair is a two qubit state that is essential in areas like quantum teleportation, and is represented by

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{6}$$

Here on measuring the first qubit, we obtain 0 with a probability of $\frac{1}{2}$ with the post measurement state being $|00\rangle$ and 1 with a probability of $\frac{1}{2}$ as well, leaving the post measurement state as $|11\rangle$. Thus the outcomes are correlated since on measuring the first qubit, the second qubit always gives the same result as what we obtain from the first qubit.

2 Quantum computation

Similar to in classical computation, logic gates in quantum computing help transmit and manipulate quantum information.

2.1 Single qubit gates

Analogous to the classical NOT gate, in which $0 \to 1$ and $1 \to 0$, we define a process that takes the state $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. Note however, we can only extend this idea to the superposition of these two states if we know that quantum logic gates act linearly, since we have only defined its action on the basis states. This is incidentally true, and this result is empirically necessary as nonlinearity would lead to apparent paradoxes. Thus a NOT gate acts on

$$\alpha |0\rangle + \beta |1\rangle \tag{7}$$

and takes it to the state

$$\beta |0\rangle + \alpha |1\rangle \tag{8}$$

We can represent quantum gates using matrices, with the state $\alpha |0\rangle + \beta |1\rangle$ represented by

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{9}$$

and gates represented by a 2×2 matrix. For example, the NOT gate is represented by

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{10}$$

and when it acts on the initial quantum state, it gives

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \tag{11}$$

Two other important single qubit gates are the Z gate

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{12}$$

and the Hadamard gate

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{13}$$

which is also called the square root of the NOT gate since it turns $|0\rangle$ "halfway" to $|1\rangle$, although H^2 is not a NOT gate, and is instead simply the identity matrix. This gate will be particularly useful later on in quantum teleportation.

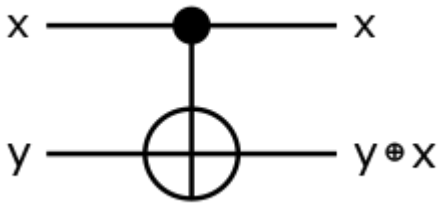

Figure 2: A CNOT gate, with x as the control qubit and y as the target qubit

The only condition for a single qubit gate is that it is unitary, i.e. for a gate A, $A^T A = I$. Note that this also ensures that if the input state is normalised, the state after the gate has acted will also be normalised.

Any single qubit quantum gate can be decomposed as the product of rotations about different axes i.e.

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} cos(\frac{\gamma}{2}) & -sin(\frac{\gamma}{2}) \\ sin(\frac{\gamma}{2}) & cos(\frac{\gamma}{2}) \end{bmatrix} \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix} \tag{14}$$

2.2 Multiple qubit gates

In classical gates, any gate can be computed from the composition of NAND gates alone, which is known as the universal gate. The equivalent gate in quantum gates is the CNOT or controlled-NOT gate, which has two inputs, the control qubit and the target qubit. The top line represents the control qubit while the bottom line represents the target qubit. If the control qubit is set to 0, the target qubit is unchanged, and if the control qubit is set to 1, the target qubit is flipped. It is represented by the matrix

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{15}$$

The CNOT can be described as a generalised XOR gate, where the XOR of the two inputs is stored in the target qubit, i.e. $|A, B\rangle \rightarrow |A, A \oplus B\rangle$

Since unitary quantum gates can be represented by unitary matrices, which are invertible, they are always invertible. This is unlike classical XOR or NAND gates, which are non-invertible as they have an irretrievable loss of information i.e. given the output it is impossible to determined the inputs. The CNOT gate is particularly important because of the universality result that any multiple qubit quantum gate can be composed from CNOT and single qubit gates.

2.3 Other bases

While so far we have measured quantum states giving a result of 0 or 1, it is possible to perform a measurement using other orthonormal bases as well, for example $|+\rangle = \frac{|0\rangle+|1\rangle}{2}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{2}$. In general, given any two basis states $|x\rangle$ and $|y\rangle$, we can express an arbitrary state as a linear combination of the basis states i.e. $|\psi\rangle = \alpha|x\rangle + \beta|y\rangle$. In addition, if $|x\rangle$ and $|y\rangle$ form an orthonormal basis, we can perform a measurement with respect to them, obtaining $|x\rangle$ with a probability of α^2 and $|y\rangle$ with a probability β^2.

2.4 Quantum circuits

Quantum circuits differ from classical circuits in a few key ways. They are acyclic and don't allow feedback from one part of the circuit to another. They also do not allow FANIN, where wires are joined together and the resultant wire carries the classical OR operation of the individual wires, or FANOUT, where several copies of a bit are produced. Importantly, quantum mechanics does not allow the copying of a qubit, making FANOUT impossible.

If we attempt to copy a qubit using a CNOT gate, with $\psi = \alpha|0\rangle+\beta|1\rangle$ as the control qubit and $|0\rangle$ as the target qubit, we get the output $\alpha|00\rangle+\beta|11\rangle$. Note however, that this is not the copy $|\psi\rangle|\psi\rangle$, as $|\psi\rangle|\psi\rangle = \alpha^2|00\rangle+\alpha\beta|01\rangle+\alpha\beta|10\rangle+\beta^2|11\rangle$. This is the same as the output only when $\alpha\beta = 0$. It is incidentally impossible to copy a qubit, and this is referred to as the no-cloning theorem.

A convention in quantum circuits is to define a controlled-U gate for a given n-qubit quantum gate U. Here, there is one control qubit and n target qubits. When the control qubit is set to 0, the target qubits are unchanged and if set to 1, the gate U acts on the target qubits. Another important quantum circuit symbol is that for measurement, where a qubit is converted

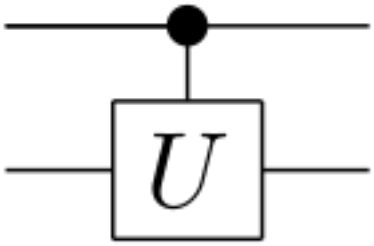

Figure 3: A controlled U gate

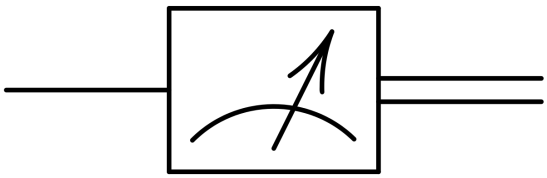

Figure 4: Circuit symbol for a measurement

into a probabilistic classsical bit (which is distinguished from qubits by the double wire.)

2.5 Bell states

Bell states, or EPR pairs (named after Einstein, Podolsky and Rosen), are obtained when the four basis states are passed through a Hadamard gate followed by a CNOT gate. The output states we get are

$$\beta_{00} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{16}$$

$$\beta_{01} = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{17}$$

$$\beta_{10} = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{18}$$

$$\beta_{11} = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{19}$$

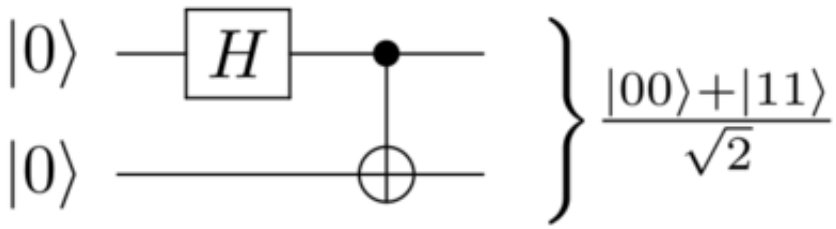

Figure 5: Generating an EPR pair using an H gate followed by a CNOT gate

2.6 Quantum teleportation

Quantum teleportation is the idea that you can move quantum states in the absence of a quantum communication channel i.e. that you can deliver a qubit using only classical information. While it seems unintuitive, especially since describing the state of the qubit would require an infinite amount of classical information, it is possible. It makes use of the idea that the people on either end of the communication channel (say Alice and Bob) created an EPR pair (assume it to be β_{00})when they were together and each took one qubit of the pair. Let's say Alice has a qubit $|\psi\rangle$ that she wants to deliver to Bob. The initial state is simply

$$\begin{aligned} |\psi_0\rangle &= |\psi\rangle\,|\beta_{00}\rangle \\ &= \frac{1}{\sqrt{2}}(\alpha\,|0\rangle + \beta\,|1\rangle)(|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}}\Big(\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle)\Big) \end{aligned} \tag{20}$$

If we now pass Alice's qubits through a CNOT gate, there is no change when the control qubit (in this case *psi*) is $|0\rangle$, and the basis states of the target qubit are swapped when the control qubit is $|1\rangle$. After the CNOT gate we get

$$\psi_1 = \frac{1}{\sqrt{2}}\Big(\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)\Big) \tag{21}$$

We now pass the first qubit through a Hadamard gate, giving

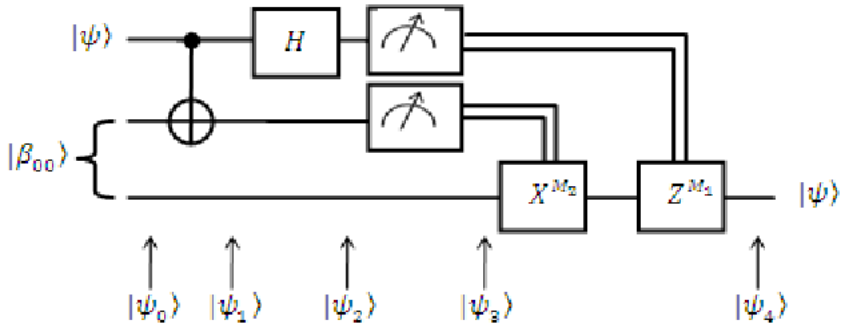

Figure 6: Quantum teleportation

$$\begin{aligned}\psi_2 &= \frac{1}{2}\Big(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\Big) \\ &= \frac{1}{2}\Big(|00\rangle\,(\alpha\,|00\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) \\ &\quad + |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)\Big) \qquad (22)\end{aligned}$$

This is very interesting, because if Alice now measures her two qubits and sends the result to Bob, he can use that information to decide what operation to perform on his qubit to obtain the original qubit ψ. If Alice measures $|00\rangle$, Bob already has the qubit that had to be delivered. If it is $|01\rangle$ for example, he would need to pass it through a NOT gate to get ψ. In spite of the name, this is not really "teleportation" because sending classical information from Alice to Bob is necessary for this process, and that can't be sent faster than the speed of light.

3 Algorithms

The problem we run into when we try and simulate classical circuits using quantum circuits is that quantum logic gates are reversible, which isn't the case for most classical logic gates as we've seen already. This is overcome by using the Toffoli gate, which is reversible but can be used to simulate a NAND gate (by setting the target gate to 1). Since all multiple bit classical gates can be composed with NAND gates, we can then simulate any classical

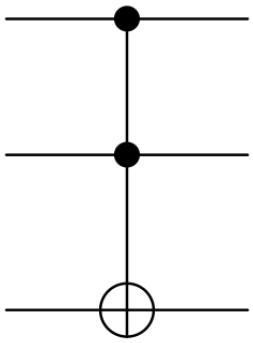

Figure 7: Toffoli gate with two control bits

circuit. The first two bits are unaffected by the gate and are control bits, while the third bit is flipped if both the first two bits are set to 1 i.e. for input bits x, y and z, $(x, y, z) \rightarrow (x, y, z \oplus xy)$. Since it is a reversible gate, it can also be implemented as a quantum logic gate and expressed as an 8×8 unitary matrix.

Another requirement to simulate non-deterministic classical computers is the ability to produce random bits. This can be done simply by passing a qubit in a basis state through a Hadamard gate, and the output is essentially a fair coin toss, there is a 50% chance of getting either a $|0\rangle$ or a $|1\rangle$.

3.1 Quantum parallelism

One of the advantages of quantum computers is that they can evaluate a function at different points simultaneously, something that's only possible with a classical computer by using multiple circuits each computing f(x) simultaneously. Let's take a function $f(x)$ with domain and range $0, 1$. We can define a transformation called U_f (that can be represented by a unitary matrix that takes an input $|x, y\rangle$ and transforms it to $|x, y \oplus f(x)\rangle$. If y=0 then the second qubit (also called the target register, the first qubit is the data register) is simply $f(x)$. Now, if the data register carried a superposition of the basis states, $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ for example, when U_f acts on it we get

$$\frac{1}{\sqrt{2}}\Big(|0, f(0)\rangle + |1, f(1)\rangle\Big) \tag{23}$$

Note that this now contains the information for the value of f(x) at *two* positions, 0 and 1. We can extend this idea to more than one qubit as well, simply by having several Hadamard gates in parallel, that take $|0\rangle$ as input and give $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. For n qubits this gives

$$\begin{aligned} &\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^n \\ &= \frac{1}{\sqrt{2^n}} \sum |x\rangle \end{aligned} \tag{24}$$

where we sum over all x. This action is denoted by $H^{\oplus n}$. If we now pass this through U_f, we get

$$\frac{1}{\sqrt{2^n}} \sum |x\rangle \, |f(x)\rangle \tag{25}$$

From this it seems like we've obtained the value of $f(x)$ at several points simultaneously in this n qubit state, but it isn't immediately useful unless we can find some way of getting this information out of the quantum state. If we try and measure the state we only obtain the value of $f(x)$ at one point. Actually extracting this information isn't as straightforward but can be achieved using algorithms explained below.

3.2 Deutsch's algorithm

If in the above example, instead of setting the second qubit to $|0\rangle$, we instead make it $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ (by passing $|0\rangle$ and $|1\rangle$ through Hadamard gates). Recall that the actual operation that U_f performs is making the target register $y \oplus f(x)$. This is useful because if we now pass it through U_f, the target register for $f(0) = f(1) = 0$ would be

$$\begin{aligned} &\frac{(|0\rangle - |1\rangle) \oplus |0\rangle}{\sqrt{2}} \\ &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{aligned} \tag{26}$$

We get the same multiplied by -1 if we instead had $f(0) = f(1) = 1$, which in general gives us

$$\psi = \frac{1}{2}\Big(|0\rangle + |1\rangle\Big)\Big(|0\rangle - |1\rangle\Big) \tag{27}$$

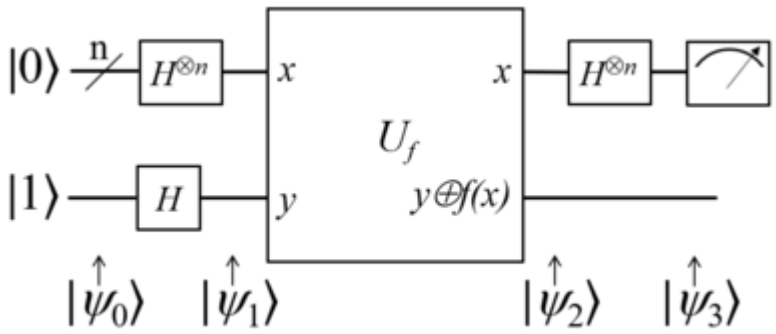

Figure 8: Implementation of Deutsch-Josza algorithm

If however we have $f(0) \neq f(1)$, we would instead get

$$\psi = \pm\frac{1}{2}\Big(|0\rangle - |1\rangle\Big)\Big(|0\rangle - |1\rangle\Big) \tag{28}$$

If we now operate a Hadamard gate on the first qubit we get something very interesting:

$$\psi = \pm\frac{1}{\sqrt{2}}|0\rangle\Big(|0\rangle - |1\rangle\Big) \tag{29}$$

when $f(0) = f(1)$ and

$$\psi = \pm\frac{1}{\sqrt{2}}|1\rangle\Big(|0\rangle - |1\rangle\Big) \tag{30}$$

If we now measure the first qubit, we know the value of $f(0) \oplus f(1)$. Thus with one evaluation in a quantum computer we have evaluated something that would require at least two evaluations in a classical computer to find the values of $f(0)$ and $f(1)$. The reason this works is because in quantum computers we can make $f(0)$ and $f(1)$ *interfere* with each other, something you can't do with classical computers where $f(0)$ and $f(1)$ are treated as distinct.

The Deutsch-Josza algorithm is a more general version of Deutsch's algorithm that works for multiple qubits. Analogous to how we found $f(0) \oplus f(1)$, for a domain consisting of $0, 1, 2, 3...2^{n-1}$, we know that a function f is either constant everywhere or is balanced i.e. it is 1 for exactly half of all values of

x. For a classical computer this could take upto $2^{n-1}+1$ evaluations, as it is possible you get a 0 the first 2^{n-1} times and then finally get a 1. With a quantum computer we can do the same with one evaluation. The process is similar to Deutsch's algorithm, except instead of one qubit we have n qubits. When we finally evaluate it, we get 0 when f is constant everywhere, and 1 when it is not, similar to with the Deutsch algorithm.

4 Quantum mechanics

4.1 Superdense coding

Along similar lines to what we've discussed already, superdense coding is the ability to transmit a certain number of classical bits of information using fewer qubits. For example, if we need to communicate 2 bits of information, let's say from Alice to Bob, we can achieve this by communicating just one qubit. We start off with Alice and Bob each having one qubit of an EPR pair. If the 2 bits are 00, Alice leaves her qubit as is. If it is 01, she passes her qubit through a Z gate to perform a phase flip, if it is 10 she passes it through a NOT gate and if it is 11 she passes it through an iY gate. If she now delivers this qubit to Bob the four possibilities we get are

$$\psi_{00} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{31}$$

$$\psi_{01} = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{32}$$

$$\psi_{10} = \frac{|10\rangle + |01\rangle}{\sqrt{2}} \tag{33}$$

$$\psi_{11} = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{34}$$

Note that these are basis states for a 2 qubit quantum state. Now if Bob measures the state keeping the EPR pairs as the basis states, he will get one of four possibilities, and so he can determine what the string of bits Alice sent was.

5 Linear algebra

Since linear algebra is so widely used in the study of quantum computing, a brief explanation of notation and certain concepts is necessary. We generally represent vectors as $|v\rangle$. A spanning set being a set of vectors $|v_1\rangle, |v_2\rangle, ..., |v_n\rangle$ such that any vector in the given vector space can be written as a linear combination of them. Linear operators are of particular importance in quantum computing since quantum gates can be mathematically expressed as linear operators. We define a linear operator between spaces V and W to be a function L from V to W such that

$$L\Big(\sum_i a_i |v_i\rangle\Big) = \sum_i a_i L\big(|v_i\rangle\big) \tag{35}$$

5.1 Pauli matrices

Pauli matrices are particularly important matrices in the study of quantum computing, and they are

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{36}$$

$$\sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{37}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{38}$$

$$\sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{39}$$

5.2 Inner products

While the concept of inner products is commonly used especially in physics, we generalise the idea to all vector spaces. We define the inner product to be a function $(\cdot, \cdot)$ from $V \times V$ to complex numbers $\boldsymbol{C}$ that satisfies the following requirements:

1. It is linear in the second argument i.e. $\Big(|v\rangle, \sum_i \lambda_i w_i\Big) = \sum_i \lambda_i \big(|v\rangle, |w_i\rangle\big)$

2. $\left(|v\rangle, |w\rangle\right) = \left(|w\rangle, |v\rangle\right)^*$ where * represents the conjugate.

3. $(|v\rangle, |v\rangle) \geq 0$, we will later see that this is used to define the norm of a vector.

5.3 Orthonormal basis

We define the norm of a vector v as the square root of the inner product of the vector and itself, i.e.

$$|| \, |v\rangle \, || = \sqrt{\langle v|v\rangle} \tag{40}$$

We define a set of vectors $|v_i\rangle$ to be orthonormal if

1. $\langle v_i|v_j\rangle = 1$ for $i = j$, i.e. the norm is 1

2. $\langle v_i|v_j\rangle = 0$ for $i \neq j$

In particular, given a basis $|v_1\rangle, |v_2\rangle, |v_3\rangle \ldots |v_n\rangle$ for a vector space V, we can produce an orthonormal basis using the Gram-Schmidt procedure. It essentially works by subtracting the part of each vector that can be expressed in terms of the other basis vectors, and then normalising it. If we define the orthonormal basis to be $|w_1\rangle, |w_2\rangle, |w_3\rangle \ldots |w_n\rangle$, $|w_1\rangle = \frac{|v_1\rangle}{||v_1\rangle||}$. We then use induction to define a particular $|w_{k+1}\rangle$ as

$$|w_{k+1}\rangle = \frac{|v_{k+1}\rangle - \sum_{i=1}^{k} |w_i\rangle \langle v_{k+1}|w_i\rangle}{|| \, |v_{k+1}\rangle - \sum_{i=1}^{k} |w_i\rangle \langle v_{k+1}|w_i\rangle \, ||} \tag{41}$$

6 Quantum information

While much of the introduction focused on closed systems (systems that have no or weak interaction with the environment around them) that behave ideally, in practice no quantum system is completely closed, and environmental factors play a role in affecting computation, by introducing noise for example. The idea of quantum operations therefore helps us as it can not only describe closed systems with little to no noise, but also open quantum systems.

6.1 Classical noise

Before analysing quantum noise and how we can correct for it, we look at a classical analogy. Let's assume we have a classical bit, that in a period of time flips with a probability p. Bit flips happen due to magnetic fields in the environment and so in principle, to obtain an accurate estimate of p, we need to know

1. the distribution of magnetic fields in the environment around this bit
2. how these magnetic fields interact with the system, in this case possibly the hard drive containing these bits.

If we can produce a sufficiently good model (since no model is ever absolutely accurate) of both the system (the hard drive in this case) and the environment (the magnetic fields), we can calculate the effect of noise more generally, beyond just single bit flips.

In general for a single stage process the output probabilities $\vec{p}$ are related to the input probabilities $\vec{q}$ by

$$\vec{q} = E\vec{p} \tag{42}$$

where E is a matrix of transition probabilities, which are essentially the conditional probabilities $p(A = a|B = b)$ where A is the final state of the system and B is the initial state.

We can extend this idea beyond single stage processes to multi stage processes by assuming them to be Markov processes, which is usually a safe assumption to make. This assumes that the noise in each consecutive process acts independently, i.e. the environment causing noise in the first stage acts independently of the environment causing noise in the second stage and so on. Note particularly that since $\vec{p}$ and $\vec{q}$ are probabilities, this places certain conditions on E. First, since the entries represent conditional probabilities, they cannot be negative. In addition, all the columns of E must sum up to 1, which is called the completeness requirement.

6.2 Quantum operators

We describe quantum measurements by a collection of operators M_m where m is the index representing the outcome of the experiment. Immediately

before performing the measurement the probability of getting outcome m on performing the measurement is

$$\langle\psi|M_m^+ M_m|\psi\rangle \tag{43}$$

where M_m^+ is the adjoint of M_m. Further, the state of the system after the measurement is

$$\frac{M_m\,|\psi\rangle}{\sqrt{\langle\psi|M_m^+ M_m|\psi\rangle}} \tag{44}$$

Further, note that from equation 43, the probabilities of getting all possible m must sum to 1, which leads to the completeness equation:

$$\sum_m M_m^+ M_m = I \tag{45}$$

With this background, we define a quantum operation $\mathcal{E}$ as a map that transforms a given state ρ.

$$\rho' = \mathcal{E}(\rho) \tag{46}$$

We've already seen that we can define describe changes to a closed quantum system by a unitary transform. To extend this idea to an open system, we treat it as an interaction between the quantum system, or the principal system, and an environment, which together form a closed system (the environment is included in this closed system.)

Before we proceed further, an understanding of tensor products is required. Quite simply, given two vector spaces V and W of dimensions m and n respectively, the tensor product $V \otimes W$ forms an mn dimensional space. If $|i\rangle$ and $|j\rangle$ are bases of V and W respectively, the basis of their tensor product is $|i\rangle \otimes |j\rangle$. Tensor products have some fairly straightforward properties:

1. multiplying the product by a scalar is the same as multiplying one of the vectors by a scalar

2. it is distributive over addition

We now need a mathematical way to describe the state of a system A given two physical systems A and B whose state is together described by ρ^{AB}. We do this using the reduced density operator, which is given by

$$\rho^A \equiv tr_B(\rho^{AB}) \tag{47}$$

tr_B here is the partial trace over system B, which is intuitively just a way of summing over the system B, so we can better study A, which is the state we actually care about. It is an operator defined by

$$tr_B(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2| \equiv |a_1\rangle \langle a_2| \, tr(|b_1\rangle \langle b_2|) \tag{48}$$

The justification for the reduced density operator describing the state of a system is that it provides accurate statistics when we make a measurement on the system.

With this background, we assume that the closed system that we have created by combining the principal system and the environment is a product state $\rho \otimes \rho_{env}$. This assumption is not very accurate as quantum systems constantly interact with their environment, causing a correlation, and so simply treating the system as a superposition doesn't hold in general. But if we operate under this assumption, after the transformation of the system by operator U we get

$$\mathcal{E}(\rho) = tr_{env}\left[U(\rho \otimes \rho_{env})U^+\right] \tag{49}$$

This is however a reasonable assumption to make given that when performing an experiment usually the correlation built up is undone, and so it can be treated as a product state.

6.3 Quantum noise

We often express quantum operations in a form called the operator sum form, which is simply restating it in terms of the Hilbert space alone, as below:

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^+ \tag{50}$$

A bit flip channel is a simple quantum operation that has many uses in error correction. All it does is flip the state of a qubit from $|0\rangle$ to $|1\rangle$ and vice versa with a probability of $1-p$ and retains the state with a probability of p. It has operation elements

$$E_0 = \sqrt{p}I = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{51}$$

$$E_1 = \sqrt{1-p}X = \sqrt{1-p}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{52}$$

This change is visualised in the Bloch sphere below. Note that the x axis is left as is, while the sphere is compressed along the y and z axes to $1-2p$ the size of the original sphere.

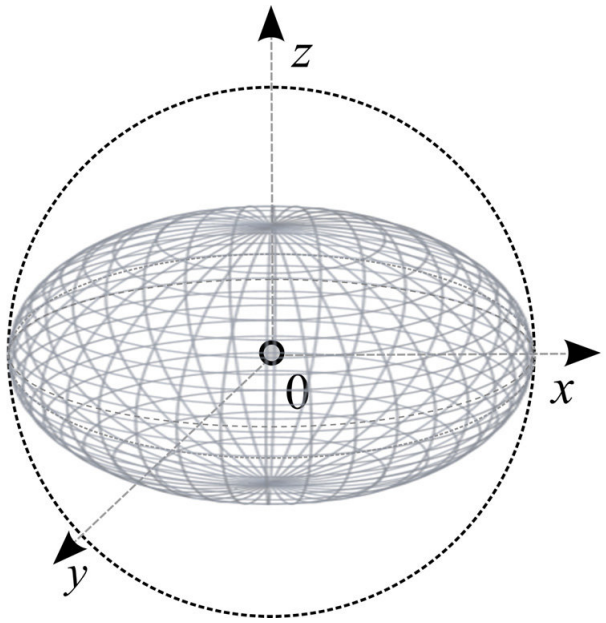

Figure 9: A bit flip channel

Similarly, the phase flip channel has elements

$$E_0 = \sqrt{p}I = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{53}$$

$$E_1 = \sqrt{1-p}Z = \sqrt{1-p}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{54}$$

Note here that the z axis is unaltered while the sphere is compressed along the x and y axes.

And finally, the bit-phase flip channel geometrically results in a compression along the x and z axes leaving the y axis as is. Its elements are

$$E_0 = \sqrt{p}I = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{55}$$

$$E_1 = \sqrt{1-p}Z = \sqrt{1-p}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{56}$$

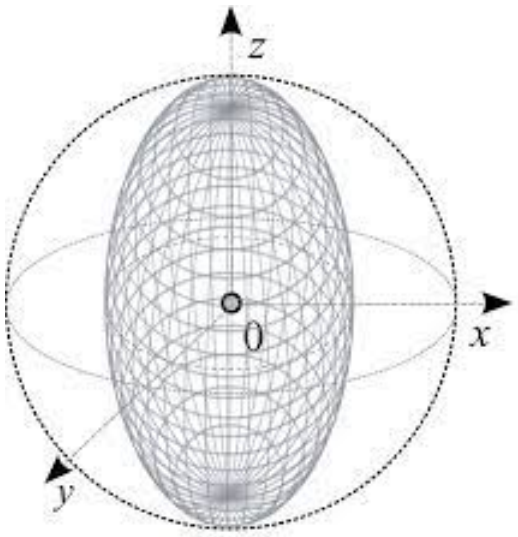

Figure 10: A phase flip channel

Finally, the depolarising channel is an important type of quantum noise. As the name suggests, it is an operator that with probability p leaves the qubit depolarised or in the completely mixed state, $I/2$. This essentially results in a symmetric contraction of the Bloch sphere, as the probability of having the original untouched qubit is now less than 1. It is simply

$$\mathcal{E}(\rho) = \frac{pI}{2} + (1-p)\rho \tag{57}$$

6.4 Error correction

The classical approach to error correction is to introduce some form of redundancy, the idea being that even if one or some of the bits are flipped

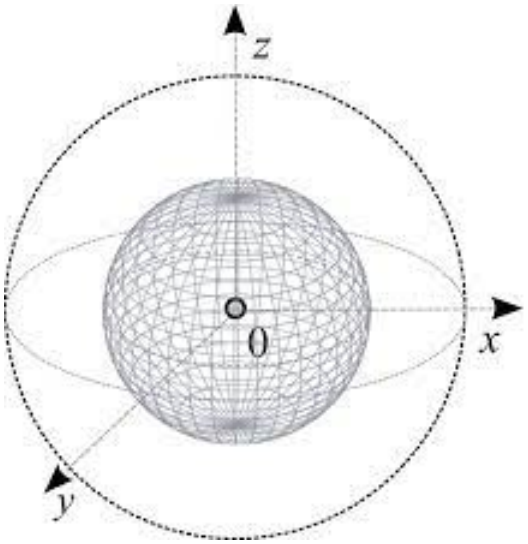

Figure 11: A depolarising channel

by noise in the environment, the original message can be recovered using this redundancy. At first glance however, there are certain problems with extending this idea to qubits.

- The no cloning theorem prevents us from simply duplicating qubits to build this redundancy, like we could with classical bits.
- Unlike classical bits which take two discrete values, qubits take an entire range.
- Measuring a qubit destroys the information stored in it, and makes it irrecoverable.

These problems can however be overcome. Similar to how if we want to add redundancy to the transmission of a single classical bit 1 we may add two redundant bits to make it 111, given a qubit $a\,|0\rangle + b\,|1\rangle$, we can encode it as $a\,|000\rangle + b\,|111\rangle$. We do this using 2 CNOT gates connected to the qubit ψ we want to encode.

If there is now a bit flip, we can detect it using the projection operators that can operate on the quantum state:

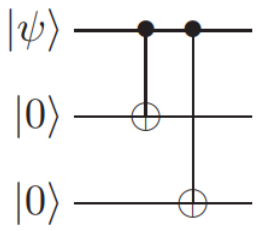

Figure 12: Encoding the qubit using 2 CNOT gates

$$\begin{aligned} P_0 &= |000\rangle\langle 000| + |111\rangle\langle 111| \\ P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011| \\ P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101| \\ P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110| \end{aligned} \tag{58}$$

If there is no error, then note that $\langle\psi|P_0|\psi\rangle = 1$ always. Similarly if there is an error in the first bit then $\langle\psi|P_1|\psi\rangle = 1$, and so on.

If we do detect an error, then to correct for it is fairly straightforward. If the error is in the first qubit, then we simply flip the qubit again to obtain the original state. Note however that this three qubit flip code is not adequate as there is noise that can affect the state of a qubit by a small amount, and not necessarily cause a bit flip.

Instead of measuring P_i we can achieve the same result by measuring Z_1Z_2 (or $Z \otimes Z \otimes I$)and Z_2Z_3.

$$Z_1Z_2 = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I \tag{59}$$

Note that we have decomposed Z_1Z_2 as a projective measurement (similar to how we worked with P_i), with projectors $(|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I$ and $(|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I$, and so effectively we are comparing the signs of the first two qubits. If they are different, we get -1 from the second term, and if they are the same, we get +1. This then helps us identify which qubit has a different sign and has therefore undergone a bit flip, allowing us to correct for it.

Similar to the three qubit bit flip code, we also have the phase flip code, which helps us correct for phase flips. We follow a similar procedure, except with the addition of a Hadamard gate as shown in the figure, to work in the basis $|+\rangle$ and $|-\rangle$. This is useful because in this basis, the effect of a phase flip is essentially the same as a bit flip, $|+\rangle$ becomes $|-\rangle$ and vice versa.

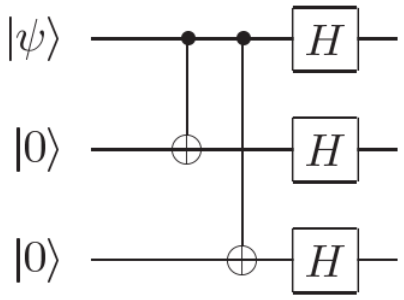

Figure 13: A three qubit phase flip code

6.5 Shor code

Shor code is a quantum code that can protect against any errors on a single qubit, and it uses the two codes we have seen above. We first encode each qubit using the three qubit phase flip code, and then using the bit flip code (with $|+\rangle$ being encoded as $(|000\rangle + |111\rangle)/\sqrt{2}$. This results in a nine qubit code (as in each step we triple the number of qubits) as below:

$$|0\rangle \to |+++\rangle \to \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \tag{60}$$

$$|1\rangle \to |---\rangle \to \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}} \tag{61}$$

This is achieved by simply having the gates that perform the two operations in series.

Now, if we wish to detect a bit flip, we simply measure Z_1Z_2, and Z_2Z_3. If only the first gives a negative result, then we can say with high certainty that the first qubit has undergone a bit flip. If on the other hand, both give

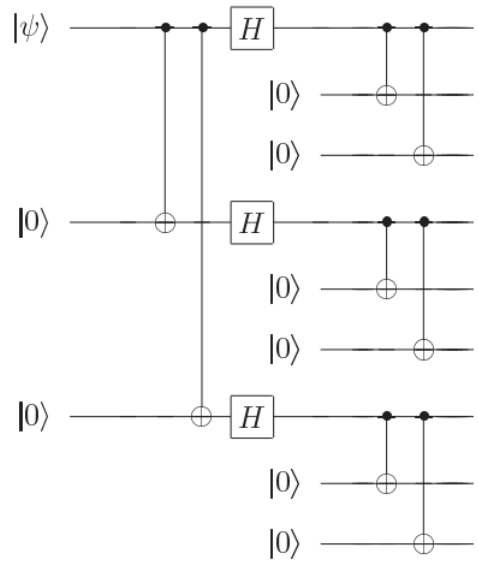

Figure 14: Shor code

a negative result, i.e. they have opposite signs, it is likely the second qubit has undergone a bit flip. We can then correct for this simply by operating on the qubit again, flipping it back to the original state.

Similarly, for a phase flip, we measure X_1X_2 and X_2X_3, with the signs of the results telling us which of the qubits has undergone a phase flip. Note however, so far we haven't shown that this corrects for any arbitrary error.

We protect against this by using an idea discussed earlier, which is that an operator can be expressed in operator sum form as a sum of operation elements E_i. If for the sake of simplicity we assume this noise only affects the first qubit, we then get the new state as $\sum_i E_i |\psi\rangle \langle\psi| E_i^+$. We can express each of these E_i in turn as the sum of the identity, the bit flip, the phase flip, and a combination of them.

$$E_i = a_0 I + a_1 X_1 + a_2 Z_1 + a_3 X_1 Z_1 \tag{62}$$

Since we have now written the operator as a superposition of states, measuring the error as we have done above will collapse the state to one of these four, from which the original state can be obtained by simply performing the inversion operation. This is a powerful idea because even though we don't

know the exact effect the noise has had, the process of measuring the state collapses it to a state that we can observe and perform the required inversion operation on. There are issues with extending this idea to errors that affect more than just one qubit, but if we assume the noise affecting each qubit to be independent (which is not necessarily true), we can express its total effect as a sum of terms with errors on no qubit, one qubit, and so on, with the higher order terms approaching zero.