

IndependentStudy

Matthew Robson

September 2025

1 Classical Information and Computation

This entire section was covered by my work in Digital Electronics. If you wish to view an example of my completed work, you can access it through my Git repository.

2 One Quantum Bit

2.1 Qubit Touchdown

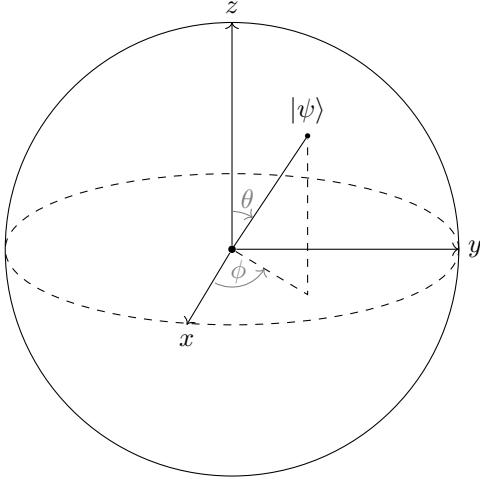
Qubit Touchdown is a game designed to introduce the player to the basics of a quantum bit.

2.2 Superposition

Qubits are represented as a super position of $|0\rangle$ and $|1\rangle$. $|0\rangle$ corresponds to the vector $(0, 0, 1)$ and $|1\rangle$ corresponds to the vector $(0, 0, -1)$. Here are the definitions of some commonly used kets:

- $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- $|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$
- $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$

Qubits can be defined by some vector $|\psi\rangle$ on the Bloch Sphere.



A common function used in quantum computing is the norm-square. The norm-square is defined as $|x|^2 = xx^*|x* = \bar{x}$.

2.3 Measurement

A qubit is most commonly measured in the z basis, as to give a $|1\rangle$ or $|0\rangle$. In the superposition $\frac{1}{\sqrt{2}}(|1\rangle + e^{\frac{i\pi}{6}}|0\rangle)$ the probability of measuring a 1 is equivalent to the norm-square of the coefficient of $|1\rangle$, as for the probability of measuring a 0. In this example, that would mean $p(|0\rangle) = |\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$, and $p(|1\rangle) = |\frac{e^{\frac{i\pi}{6}}}{\sqrt{2}}|^2 = \frac{1}{2}$. In the case where the probabilities of measuring in a basis would result in a sum of greater than one, there is a normalization constant placed in front to set the total probability to one. In our example, the $\frac{1}{\sqrt{2}}$ is the normalization constant. Measurement can be done in any basis, that is, between two positions that oppose each other on the Bloch Sphere.

2.4 Bloch Sphere Mapping

A global phase in the form of $e^{i\theta}$ may be placed in front of the superposition, but this phase will not impact the probability of measurement in any basis. Given some quantum state $|\psi\rangle$, this can be written as some $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ $|\alpha|^2 + |\beta|^2 = 1$. This means that α and β can be represented as cosine and sine, as in $\alpha = \cos \frac{\theta}{2}, \beta = e^{i\phi} \sin \frac{\theta}{2}$, explaining the above Bloch Sphere figure. In order to further understand this position, in some cases $|\phi\rangle$ will be represented using Cartesian coordinates (x,y,z). These coordinates are defined by the following set of equations.

- $x = \sin \theta \cos \phi$
- $y = \sin \theta \sin \phi$
- $z = \cos \theta$

As an additional note, by measuring a qubit, you collapse the state to one location, but if you were to measure the same qubit in alternating bases, you would be able to measure consecutive p (0.5) events. Ex. Alternate measuring in the $|0\rangle, |1\rangle$ basis, then in the $|+\rangle, |-\rangle$ basis.

2.5 Physical Qubits

There are many ways in which qubits are created in the real world. Some of these ways include:

- Photons
- Trapped ions
- Cold atoms
- Nuclear magnetic resonance
- Quantum dots
- Defect qubits
- Superconductors

2.6 Quantum Gates

Quantum gates are defined as linear, meaning that they will be distributed across superpositions. This can be shown as $U(\alpha|0\rangle + \beta|1\rangle) = \alpha U|0\rangle + \beta U|1\rangle$. Additionally, all quantum gates will be reversible, suggesting that all reversible classical gates can be represented as a set of quantum gates. In classical computing, there are two single bit gates, the identity gate, and the not gate, both of which can be regarded as quantum gates. The identity gate does nothing and therefore can be represented as doing nothing in a quantum computer, but the not gate is represented as the Pauli-X gate. The transformation from the Pauli-X-Gate is defined as $X|0\rangle = |1\rangle, X|1\rangle = |0\rangle$ or more generally as a rotation 180° about the x-axis. There are also the Pauli-Y-Gate and the Pauli-Z-Gate, which transform in the same way, but as rotations in the y and z axes respectively. Additionally, there are a number of other defined gates, such as the phase gate (S), the t gate (T), and the Hadamard gate (H), all of which are rotations about different axes and for different angles. The Hadamard gate is particularly interesting, as it is a rotation about the x+z axis by 180°. We can define some general rotation gate U in terms of our previous rotation gates and some unit vector $\hat{n} = n_x\hat{x} + n_y\hat{y} + n_z\hat{z}$. This gives us the definition for U as $U = e^{i\gamma}[\cos \frac{\theta}{2}I - i \sin \frac{\theta}{2}(n_xX + n_yY + n_zZ)]$. This means, if we are given some general rotation we can use a unit vector and its θ value to define it in our general rotation gate.

2.7 Quantum Circuits

A popular tool for drawing quantum circuits is Quirk, which can be found at <https://algassert.com/quirk>.

3 Linear Algebra

3.1 Quantum States

As all quantum gates are linear transformations, our entire quantum circuit can be written using the laws of Linear Algebra. For example:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

suggesting that

$$|\psi\rangle = \alpha \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \beta \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

In addition to column vectors to represent these states, we can also transpose these column vectors to row vectors by applying a *transpose*. This is shown as:

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}^T = (\alpha \quad \beta)$$

More commonly in quantum computing, the conjugate transpose is used, defined as:

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}^\dagger = (\alpha^* \quad \beta^*)$$

3.2 Inner Products

This notation gives us the tools to define $\langle\psi| = |\psi\rangle^\dagger$, or more simply, the conjugate transpose of the column vector of psi is written in row vector notation. By using our bras and kets we are now able to define inner products.

$$\text{let } |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, |\phi\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}, \langle\phi|\psi\rangle = (\alpha^* \quad \beta^*) \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \alpha^* \gamma + \beta^* \delta$$

From this we can prove that $\langle\psi|\psi\rangle = 1$. Additionally, we can define two states to be orthonormal if when multiplied, result in zero. For example, the states $|0\rangle$ and $|1\rangle$ when multiplied will result in zero, and $\langle+|-\rangle = 0$. This property of our states is very useful, as if we want to calculate the amplitude of $|0\rangle$ in some $|\psi\rangle$ we can just multiply $|\phi\rangle$ by $|0\rangle$. This returns us just the amplitude for $|0\rangle$ because as previously defined, $\langle 0|0\rangle = 1$ and $\langle 0|1\rangle = 0$.

3.3 Quantum Gates

While states can be defined as vectors, a gate may be defined as a matrix. Simply, a two by two matrix is used to define a single qubit gate.

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

This is particularly useful because we can see how our states ($|0\rangle$ and $|1\rangle$) are just basis vectors that when multiplied by our gate will return us a single column of that gate. We can now define many of our gates as matrices.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$$

3.4 Outer Products

In addition to the inner products defined in the previous section, there are also outer products that can be defined as $|\phi\rangle\langle\psi|$. This results in the following:

$$|\phi\rangle\langle\psi| = \begin{pmatrix} \alpha\gamma^* & \alpha\delta^* \\ \beta\gamma^* & \beta\delta^* \end{pmatrix}$$

Additionally, we can show that based on our assertion about outer products, it must follow that for some $|\psi\rangle = \alpha|a\rangle + \beta|b\rangle$, $|a\rangle\langle a| + |b\rangle\langle b| = I$.

4 Multiple Quantum Bits

4.1 Entanglement

It so seems that there are multiple quantum computing based board games.

4.2 States and Measurement

We must now define our final form of product, the tensor product. We let $|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle$. With two qubits, we are now given four options for our tensors. $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. We can now define a superposition of two qubits in the z-basis to be $c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$ where the probability of measuring any one of these states is equal to the norm-square of its respective c coefficient. For a more explicit definition of the tensor product, we can view it as:

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \\ \beta \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix}$$

This means, for our 2 qubit super position, it may be written as:

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix}$$

It is also important to note that a tensor product does not require the vectors to be in the same space as each other and so products such as $|1\rangle \otimes |1\rangle \otimes |0\rangle$ are perfectly valid. Additionally, you can have some set of c values such as

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

where you are creating what would be a contradiction in classical computing, as you are stating that $a_1 b_1 = \frac{1}{\sqrt{2}}$, $a_1 b_2 = 0$, $a_2 b_1 = 0$, $a_2 b_2 = \frac{1}{\sqrt{2}}$.

4.3 Entanglement

Many states are able to be factored into many separate qubits such as $(\alpha_0|0\rangle + \beta_0|1\rangle) \otimes (\alpha_1|0\rangle + \beta_1|1\rangle)$. This allows for a space complexity of $\mathcal{O}(n)$ on a classical computer (which can be effectively simulated). The issue in simulation arises for states that can not be factored. One such example was our

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

which takes up a space complexity of $\mathcal{O}(n^2)$.

4.4 Quantum Gates

Importantly, we can write multiple gates applied in succession as the tensor product between those gates. Ex:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \otimes \begin{pmatrix} A & B \\ \Gamma & \Delta \end{pmatrix} = \begin{pmatrix} \alpha \begin{pmatrix} A & B \\ \Gamma & \Delta \end{pmatrix} & \beta \begin{pmatrix} A & B \\ \Gamma & \Delta \end{pmatrix} \\ \gamma \begin{pmatrix} A & B \\ \Gamma & \Delta \end{pmatrix} & \delta \begin{pmatrix} A & B \\ \Gamma & \Delta \end{pmatrix} \end{pmatrix} =$$

$$\begin{pmatrix} \alpha A & \alpha B & \beta A & \beta B \\ \alpha \Gamma & \alpha \Delta & \beta \Gamma & \beta \Delta \\ \gamma A & \gamma B & \delta A & \delta B \\ \gamma \Gamma & \gamma \Delta & \delta \Gamma & \delta \Delta \end{pmatrix}$$

While single qubit gates are significant, in order to form a universal gate set we require two qubit gates. For example: $CNOT|a_0a_1\rangle$ which applies an inverse to a_1 if $a_1 = 1$. This give us the following matrix to represent $CNOT_{10}$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

which when acting upon a superposition gives us the result resembling a Toffoli classical gate.

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} \rightarrow \begin{pmatrix} c_0 \\ c_1 \\ c_3 \\ c_2 \end{pmatrix}$$

Additionally, we can define $CNOT_{01}$ by:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

The reason that CNOT is so significant is that it can be used to create superpositions. For example, $CNOT(|+\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$. The use of $|\Phi^+\rangle$ suggests that there are other commonly referred to super positions that should be noted. They are as follows: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle$, $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Phi^-\rangle$, $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\Psi^+\rangle$, $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\Psi^-\rangle$. For a more generalized version of the CNOT gate, we can use the CU gate, a gate where U is applied to a qubit if the other qubit is a one. This can be written as:

$$CU = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & c \\ 0 & 0 & b & d \end{pmatrix}$$

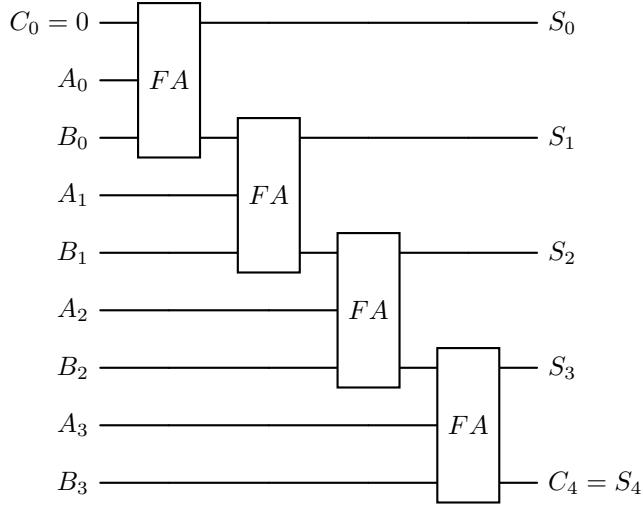
While this is useful, there are other useful two-qubit gates that this does not cover. For example, the swap gate, where two qubits are swapped. This can be given as:

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Moving on from the examples of multi-qubit gates, the *No-Cloning Theorem* states that for some quantum state, the state is not able to be copied, because by copying it it would require the knowledge of the α and β values, which measurement would result in the collapsing of the qubit.

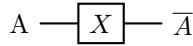
4.5 Quantum Adders

Adders in classical computing can be most simply given by:

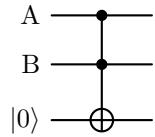


In order to construct this in a quantum circuit, we must first define how we will write classical gates with quantum gates.

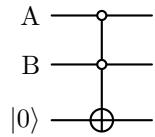
NOT:



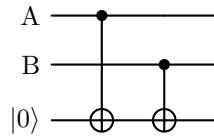
AND:



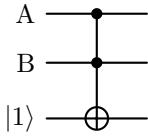
OR:



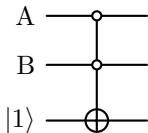
XOR:



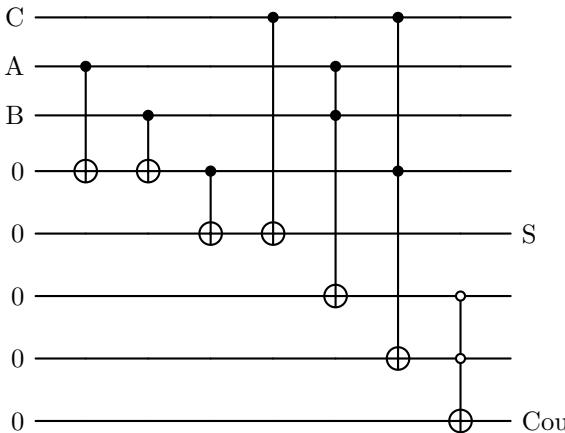
NAND:



NOR:



From these gates we are able to generate a full adder as given below.



By using these full adders, we can follow essentially the same steps as classical computing but in order to regain use of our auxiliary qubits we must undo many of the steps with inverse gates.

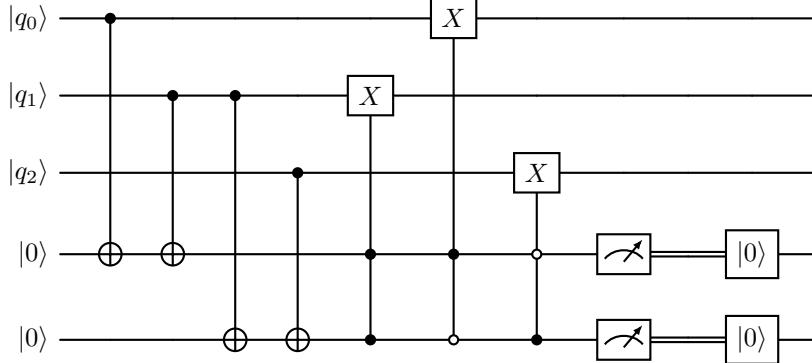
4.6 Universal Quantum Gates

The most simple way to define the universal quantum gate set is as the CNOT gate and all single qubit gates. While this is simple, it may prove useful to recognize CNOT, H, and T as a set that is also universal because H and T may approximate all other single qubit gates. In addition, the CH or controlled H gate is universal.

4.7 Quantum Error Correction

Decoherence is the process in which a qubit is ‘bumped’, resulting in a change in phase (location on the Bloch Sphere). The ease in which a qubit can be bumped results in much more frequent bit flips in quantum computing when compared to classical computing. In order to correct for this we will implement three qubits for every logical qubit. When a full qubit flip occurs, we can use

some xors to correct for this. When a partial flip occurs (some phase shift) we can measure the xors, collapsing the error, then apply the correction xors depending on if we got a full bit flip from our measurement. This can be given by:



5.4 Other Quantum Programming Languages

There are many other programming languages for quantum computing supported by other companies.

6 Entanglement and Quantum Protocols

6.1 Measurements

In Section four we covered quantum entanglement at a high level, looking at situation where the probabilities of certain states we unable to be factored. We can now look at states and consider them to be maximally entangled if measurement of one qubit fully determines the second qubit and partially entangled if the measurement of one qubit partially determines the second.

6.2 Bell Inequalities

Quantum information can travel at speeds faster than the speed of light. In fact, quantum information travels instantaneously. While this may seem to violate Einstein's principle that nothing can travel faster than the speed of light, there is no way in which anything can be encoded in these data and therefore this does not violate his principle. This was proved using the Bell Inequality test which is a complex test where a qubit is measured in multiple bases and then summed in such a way that we can conclude some new information. There are many other interpretations of how this could be possible, such as Einstein-Rosen Bridges or even the many-worlds interpretation, but our assumed Copenhagen interpretation is the most common and what we will assume to be true.

6.3 Monogamy of Entanglement

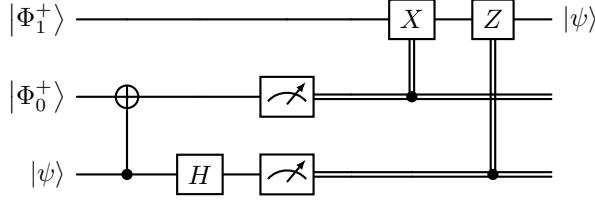
This is a claim that states that no more than two qubits may be entangled at the same time. For example, q1 and q2 can be entangled, but by attempting to entangle q3 to either q1 or q2, q1 and q2 will cease being entangled.

6.4 Superdense Coding

In quantum computing, you can send half the number of bits as in classical computing to convey the same information. This is done by encoding 00 as $|\Phi^+\rangle$, 01 as $|\Psi^+\rangle$, 10 as $|\Phi^-\rangle$, and 11 as $|\Psi^-\rangle$ and then sending the first bit (since the second bit is already at the target and is entangled with the first). To decode this message, the target must apply a CNOT gate to these qubits and then a $H \otimes I$ to return some two-qubit result.

6.5 Quantum Teleportation

Quantum teleportation is the process of sending a single bit from one space to another. It can be implemented with the following circuit:



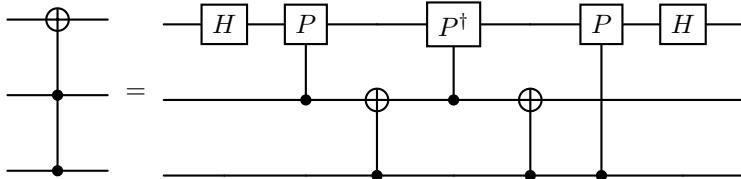
6.6 Quantum Key Distribution

Classical security such as RSA encryption can be broken by algorithms such as Shor's algorithm, making it far less secure. For this reason, we can use a quantum network to send qubits safely. This is done by the sender sending the qubits in a certain way and then revealing how they measured them. By revealing this information from both the sender and the receiver, they can discover if anyone is attempting to intercept their message, making it secure.

7 Quantum Algorithms

7.1 Circuit vs Query Complexity

An important factor in determining if a quantum algorithm is efficient is to check the circuit complexity. One common gate to consider is the Toffoli gate. In its simplest form, the Toffoli gate be represent as such:

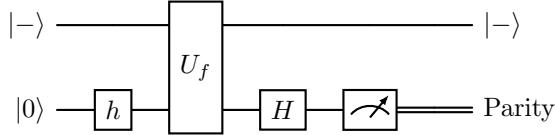


This means that in simple terms, the Toffoli gate has a gate complexity of 7 (one or two qubit) gates.

On a completely separate note, we can define some query complexity for a program by the number of times that we must call some function in it. A common problem that quantum computing is used for is what is called the oracle problem. In this problem we have some oracle that can tell us if our input is correct. For a classical computer, the time complexity to find the correct input is $\mathcal{O}(n)$. With Grover's algorithm we can compute the same task with a quantum computer in $\mathcal{O}(\sqrt{n})$. This can be represent as the quantum equation $|x\rangle|y\rangle \rightarrow |x\rangle|y\rangle \otimes f(x)\rangle$ where we let x be our input and y be our target or answer. We can now define the phase oracle as the oracle that only takes in an input where we let $|y\rangle = |-y\rangle$. This phase oracle when applied gives us $|x\rangle|-y\rangle \rightarrow |x\rangle|-y\rangle (-1)^{f(x)}$.

7.2 Parity

If you have some bits b_0 and b_1 and you want to find the parity of them with a classical computer, you have to measure both bits and then compare them. Fortunately in quantum computing, you can do this in only one step. By querying with a qubit that is equally split you can determine parity with only one operation. This circuit can be given by:



Mathematically, this can be shown by the following:

$$\frac{1}{\sqrt{2}}[-1^{f(0)} |0\rangle + -1^{f(1)} |1\rangle]$$

Which can be simply simplified to:

$$(-1)^{b_0} \frac{1}{\sqrt{2}} [|0\rangle + (-1)^{b_1-b_2} |1\rangle]$$

Simplifying even further tells us that if we get a negative number then b_0 and b_1 are equal, and vice versa. Finally, this can be generalized to the case of n qubits where the time complexity is $\mathcal{O}(n/2)$.

7.3 Constant vs Balanced Functions

We can let some constant function be such that it always returns a 0 or always returns a 1, regardless of the value of the input. A balanced function is one such that exactly $1/2$ of the outputs are 1 and the other half are 0. We can clearly see that the time complexity of a n qubit input will take $\mathcal{O}(n^2)$ time. With a quantum computer, we can reduce this to an $\mathcal{O}(1)$ time. This is done by taking a similar approach as before by Hadamarding each qubit, then querying the qubits.

7.4 Secret Dot Product String

This method of using Hadamard gates to solve problems is very effective. It can be used again when one considers some function that performs a dot product between the input and some inside vector s . In a classical computer, it would require n queries to determine s , but with a quantum computer it takes only one.

7.5 Secret XOR Mask

We can also take this a step further in the case that we are looking for some s in a function f where $s \oplus x = s \oplus y$. Additionally, we can summarize that the quantum algorithms lead to significant speed up in terms of query complexity.

7.6 Brute-Force Searching

Now for the most significant discovery Grover's algorithm. We can interpret this function as a rotation of some vector across all dimensions that are perpendicular to the solution dimension by performing flips. This algorithm is not only impressive, but has been proven to be the most efficient possible method.

7.7 Discrete Fourier Transform

Fourier transforms are used most frequently when considering the constituent parts of a wave. Creating a FT in classical computing takes $\mathcal{O}(n \log n)$ whereas a quantum computer takes $\mathcal{O}(1)$. Additionally, an inverse QFT can be designed by transposing the previously found matrix.

7.8 Phase / Eigenvalue Estimation

To calculate eigenvalues you can create a quantum computer where you use a mixture of Hadamard gates and the use of an IQFT.

7.9 Period of Modular Exponentiation

Calculating some $n^k \bmod m$ can be very time consuming for a classical computer, but a quantum computer can speed up the query time significantly.

7.10 Factoring

Algorithms such as Shor's algorithm may be used to factor numbers very quickly.

8 Next Steps

8.1 Careers in Quantum Computing

Many established companies recognize the growing importance of quantum computing which leads to their introduction of quantum computing jobs. Additionally start up companies looking to make breakthroughs in quantum also provide an avenue for students to study.

8.2 Technical Next Steps

It is suggested to read the book Quantum Computation and Quantum Information to further my understanding of quantum computing.

8.3 Questions

Resources such as stackexchange can contain relevant information relating to quantum computing.