Learning Quantum Computing

Jaehah Shin

June 16, 2023

Contents

1 Introduction

I am Jaehah Shin who is interested in quantum computing.
I am a second year Engineering Science student at the University of Toronto.
In this document, we explore the concept of quantum computing. I refer to the website [1]. As I refer to that site and summarize it, the flow of this document is similar to the flow of that site.
The purpose of this document is to learn the basic concept of quantum computing, and remember what I learned during the summer break.
This document is written in LaTeX.

2 Quantum Bits (Qubits)

2.1 Qubit States

As similar to conventional computers, quantum computers are made up of quantum bits. However, unlike conventional bits, the state of a qubit is a **two-dimenstional vector space**. And, this vector space is also knows as state space. The below represents the possible state for a qubit.

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

3 Connecting qubits to classical bits

3.1 Qubit States

There are two special quantum states which are corresponding the 0 and 1 states of a classical bit. The quantum state that corresponds to 0 is called the **computational basis state** which is $|0\rangle$.
There is a notation for the computational basis state.

$$|0\rangle := \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

The notation with $|$ and $\rangle$ is called **ket notation**. And, notations like $|0\rangle$ is called **kets**.
Important:

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

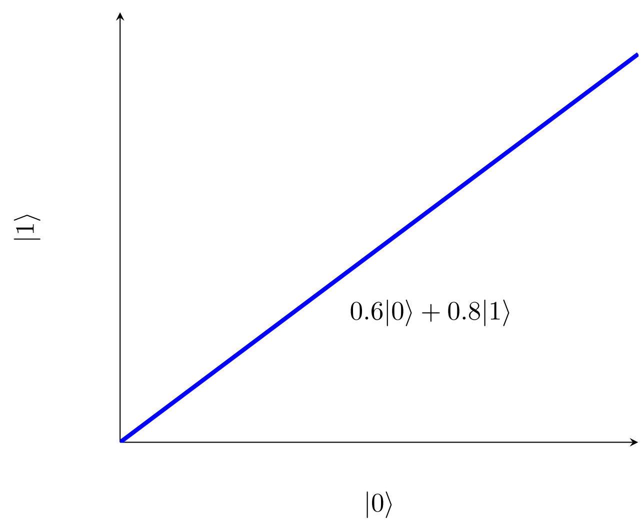
this is called as a vector, not a ket. As you can see, $|0\rangle$ has a simliar role as 0 does for a classical bit.
There is also a notation for the computational basis state for 1 which is $|1\rangle$.

As $|1\rangle$ is a notation for two-dimensional vector, therefore, this can be represented as

$$|1\rangle := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

4 General Qubit States

As quantum state is two-dimensional vector, therefore, more states are possible based on the linear combination of the computational basis states.
For example, the below is a possible state for a qubit as a graphical illustration.



This graph shows that the state of a qubit is a linear combination of the computational basis states.
More specifically, $0.6|0\rangle + 0.8|1\rangle$ is 0.6 **times** of $|0\rangle$ **plus** 0.8 **times** of $|1\rangle$.
This can be done as a normal linear combination.
Therefore, I will change the notation of $0.6|0\rangle + 0.8|1\rangle$ into usual vector notation.

$$0.6|0\rangle + 0.8|1\rangle = 0.6 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + 0.8 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0.6 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0.8 \end{bmatrix} = \begin{bmatrix} 0.6 \\ 0.8 \end{bmatrix}$$

The signficant thing is that in quantum state, generally, the entries of the vector are complex numbers.
Following example is another possible state for a qubit.

$\frac{(3+i)}{2}|0\rangle + \frac{i}{\sqrt{27}}|1\rangle$
This can be represented as a matrix

$$\begin{bmatrix} \frac{(3+i)}{2} \\ \frac{i}{\sqrt{27}} \end{bmatrix}$$

Matmmatical object of quantum state:

- **Two-dimensional Vector**
- **Complex Vecotr Space**

5 Important Terminology

When learning new things, it is important to know the terminology.
As a matter of fact, there are some terminologies that we need to get familiar with.

5.1 Superposition

One of the most common terminology is **superposition**.
Superposition is a state that is a **linear combination** of two or more states.

For instance, $0.6|0\rangle + 0.8|1\rangle$ is a **superposition** of $|0\rangle$ and $|1\rangle$.

5.2 Amplitude

Next terminology is **amplitude**. **Amplitude** is the coefficient of a state in a superposition.

For example, in $0.6|0\rangle + 0.8|1\rangle$, 0.6 and 0.8 are the amplitudes of $|0\rangle$ and $|1\rangle$ respectively.

6 Constraint of Amplitudes

Quantum state is a two-dimensional complex vector.
However, there is a constraint for the amplitudes.

Constraint: the sum of the squares of the amplitudes must be 1.

The example which was provided in the previous section, $0.6|0\rangle+0.8|1\rangle$, satisfies the constraint.

$$(0.6)^2 + (0.8)^2 = 0.36 + 0.64 = 1$$

6.1 More General Example

Let's consider a more general example.

$$\alpha|0\rangle + \beta|1\rangle$$

As the constraint says, the sum of the squares of the amplitudes must be 1. Therfore, generally,

$$|\alpha|^2 + |\beta|^2 = 1$$

This called as **normalization constraint**.
The reason why we called it as normalization constraint is that **length of the state is equal to 1**(which is a **unit vector**).

One summing up sentence:
"The quantum state of a qubit is a vector of unit length in a two-dimensional complex vector space known as state space."

7 Zero Vector

$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \neq \mathbf{0}$

8 Quantum Logic Gates

The quantum logic gates are similar to the classical logic gates such as AND, OR, NOT gates.
Also, quantum logic gates are the basic foundation of quantum computation.
Quantum logic gates is a way of manipulating the quantum state of a qubit which is a quantum information.
Even though quantum logic gates are based on the classical logic gates, there are some differences.

8.1 Quantum NOT Gate

The quantum NOT gate is similar to the classical NOT gate.
This takes the $|0\rangle$ state to $|1\rangle$ state and vice versa.

$$NOT|0\rangle = |1\rangle$$
$$NOT|1\rangle = |0\rangle$$

As the computational basis states are not only the possible states for a qubit, therefore, we can also apply the quantum NOT gate to the general superposition states.
For example,

$$NOT(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$$

This acts as a linearly on the quantum state while interchanging the role of the computational basis states. However, in notation-wise, we don't use the word "NOT" for the quantum NOT gate.

Instead, we use the letter **"X"**.
Therefore, the above example can be represented as

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$$

This is the algebraic representation of the quantum NOT gate.

Below will be the quantum circuit representation of the quantum NOT gate.

$$— \boxed{X} —$$

The line that you can see in the above diagram is called **quantum wire**.
The quantum wire is a way of representing the single qubit.
The best way to interpret the quantum wire is that left-to-right is the direction of time.

Therefore, for left wire is just passage of time. (Nothing is applied to the qubit)
Then, the X gate is applied to the qubit.
Next, the quantum wire is continued, leaving the desired state of the qubit.

Some people put input and output states in the quantum circuit.

$$\alpha|0\rangle + \beta|1\rangle \;— \boxed{X} —\; \alpha|1\rangle + \beta|0\rangle$$

There is another approach to represent the X gate using the matrix.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Recall, that $\alpha|0\rangle + \beta|1\rangle$ is also vector

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

Therefore, we have:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} (\alpha|0\rangle + \beta|1\rangle) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} = \alpha|1\rangle + \beta|0\rangle = X(\alpha|0\rangle + \beta|1\rangle)$$

This demonstrates that **X** and

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

acts the same way on all vectors, therefore they are same operation.

9 Quantum Wires

The simplet quantum circuit is a single quantum wire which doesn't do anything.

This just represents the single qubit being preserved in time.
Which means when some arbitary quantum state $|\psi\rangle$ is applied to the quantum wire, the same state($|\psi\rangle$) is outputted.
This can be represented as
$|\psi\rangle$ $|\psi\rangle$

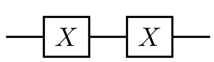
Keep in Mind:

- Mathematically, this circuit is trivial.
- Physically, this circuit is not trivial. (Really hard to implement)

The main purpose of designing system is to interact weakly with the environment mostly, and strongly with the desired time, and so serve as part of a quantum gate.

10 Multi-gate quantum circuit

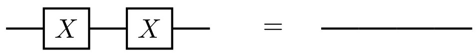
Multi-gate quantum circuit is a quantum circuit that has two X gates in a row.



First, we can approach by using arbitary imput state $\alpha|0\rangle + \beta|1\rangle$.

$$X(X(\alpha|0\rangle + \beta|1\rangle)) = X(\alpha|1\rangle + \beta|0\rangle) = \alpha|0\rangle + \beta|1\rangle$$

This is done by the fact that X interchanges the role of the computational basis states.
Therefore, no matter what the input state is, the output state is the same as the input state in the multi-gate quantum circuit.
Essentially, the multi-gate quantum circuit is the same as the single quantum wire.



Second, we can approach by using the matrix representation of the X gate.
Set the input state as arbitary as $|\psi\rangle$.
After first gate is applied, the state is $X|\psi\rangle$.
After second gate is applied, the state is $X(X|\psi\rangle)$.
Then, we can see the product XX is

$$XX = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

This represent that XX is the identity operation.
Therefore, $X(X|\psi\rangle) = |\psi\rangle$.

11 The Hadamard Gate

The Hadamard gate is one of the most important quantum logic gates.
Following will shows how this gate acts on the computational basis states.

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

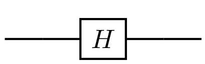
As those are not only possible states for a qubit, therefore, we can also apply the Hadamard gate to the general superposition states.
This acts as a linearly on the quantum state.
Hadamard gate takes a superposition $\alpha|0\rangle+\beta|1\rangle$ to corresponding superposition of outputs:

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

This can be simplified by using algebra. (combining the like terms)

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

Following is the quantum circuit representation of the Hadamard gate.



Not suprisingly, the Hadamard gate is also represented as a matrix.

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

To check if this matrix is correct, we can apply this matrix to the computational basis states.

We will use $|1\rangle$ as an example.

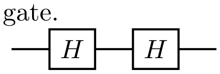
$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Let's check the other computational basis state which is $|0\rangle$

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

By expanding the range of states we can acess(or the range of dynamical operations we can generate)beyond the classcial computer performs, then it is possible to perform tasks that are impossible classically.(or take shortcuts in the computation)

Following diagram shows the quantum circuit representation of the Hadamard gate.



We can apply the first H gate to the $|0\rangle$.
As we proved this in the previous section, the output state is $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$.
Then, we can apply the second H gate to the output state.
Output will be,

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

This will be,

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

In the fashion, we can use the $|1\rangle$ as an input state.
Then, this will be:

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

This will be,

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

This demonstrates that net effect of the circuit is to leave the input state unchanged.

Another approach is to use the matrix representation of the Hadamard gate.
Set the input state as arbitary as $|\psi\rangle$.
After first gate is applied, the state is $H|\psi\rangle$.
After second gate is applied, the state is $H(H|\psi\rangle)$.
Then, we can see the product of HH is identity matrix which is $HH = I$.

$HH|\psi\rangle = I|\psi\rangle = |\psi\rangle$

This proves that the net effect of the circuit is to leave the input state unchanged.

Important:

- Cancellation-or-reinforcement is crucial in quantum computing.

There are some exercises in the website [1].

I will solve some of them.

11.1 Exercise 1

Verify that $HH = I$, where I is the 2x2 identity matrix,

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Solution:

$$HH = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1+1 & 1-1 \\ 1-1 & 1+1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

11.2 Exercise 2

Suppose that instead of H, we'd defined a matrix J by:

$$J := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

At first, it might seem that J would make an interesting quantum gate, along lines similar to H.
For instance, $J|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $J|1\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$.
These are both good, normalized quantum states.
But what happens if we apply J to the quantum state $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$?

Why does this make J unsutable for use as a quantum gate?

Solution:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}\frac{1}{\sqrt{2}}(\begin{bmatrix}1\\ 0\end{bmatrix}-\begin{bmatrix}0\\ 1\end{bmatrix})) = \frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}\begin{bmatrix}1\\ -1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1-1\\ 1-1\end{bmatrix} = \begin{bmatrix}0\\ 0\end{bmatrix}$$

This shows that when you apply J to the quantum state $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, the output state is zero vector.
Therefore, this is not a valid quantum gate.
When you apply this J to the quantum state $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, it will result in the state being collaped to the zero state, with no information preserved.

11.3 Exercise 3

Consider the quantum circuit:

$$|\psi\rangle \; - \boxed{H} - \boxed{X} -$$

Explain why the output from this circuit is $XH|\psi\rangle$, not $HX|\psi\rangle$, as you might naively assume if you wrote down gates in the order they occur in the circuit. This is a common gotcha to be aware of - it occurs because quantum gates compose left-to-right in the circuit representation, while matrix multiplications compose right-to-left.

Solution:
Key Point:

- Quantum gates compose left-to-right in the circuit representation.
- Matrix multiplications compose right-to-left.

Therefore, the output from this circuit is $XH|\psi\rangle$, not $HX|\psi\rangle$.

12 Measuring a Qubit

When we start from unknown quantum state, we can't know what the state is. For example, $|\alpha|0\rangle + \beta|1\rangle$ is a possible state for a qubit, however, we can't figure out the value of α and β, we can't know what the state is.
"To put it a slightly different way, the quantum state of any system – whether it be a qubit or a some other system – is not directly observable." We can't measure the quantum state directly.
However, there are other ways to get information about the quantum state out of a qubit.

12.1 Measurment in the computational basis

This is the way to extract informatino from the quantum computers.

Suppose that a qubit is in the state $\alpha|0\rangle + \beta|1\rangle$.
Then, we can measure the qubit in the computational basis.

References

[1] "Quantum computing via code." https://quantum.country/qcvc. Retrieved June 14, 2023.