# Self-Learning Advanced Quantum Computing

Jaehah Shin

July 5, 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 textbook *Quantum Computation and Quantum Information* by Michael A. Nielsen and Isaac L. Chuang.

As I refer to this textbook and summarize it, the flow of this document is similar to the flow of that textbook.

Also, all the exericse questions are from that textbook, and the solutions are worked by me first then checked from the website https://rioweil.github.io/assets/pdf/projects/solutions/nc-solutions.pdf.

The purpose of this document is to learn the concept of quantum computing, and remember what I learned during the summer break.

This document is written in LaTeX.

# 2   Fundamental Concepts

## 2.1   Quantum Bits

Qubits are the fundamental unit of quantum information.

This is the mathematical objects with certain properties.

As a classical bit has a state of 0 or 1, a qubit also has two possible states: $|0\rangle$ and $|1\rangle$.

Nottion $|\rangle$ is called a *Dirac notation*.

The only difference is that a qubit can be in a state *other* than $|0\rangle$ and $|1\rangle$.

Also, this is possible to form a linear combinatino of $|0\rangle$ and $|1\rangle$.

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

And, this is called as a *superposition* of $|0\rangle$ and $|1\rangle$.

Numbers $\alpha$ and $\beta$ are complex numbers.

We can think as the state of a qubit is a vector in a two-dimensional complex vector space.

There are cmoputational basis states $|0\rangle$ and $|1\rangle$, and this form an orthonormal basis for the vector space.

The significant thing is we can't measure the state of a qubit in a way that reveals the values of $\alpha$ and $\beta$.

Instead, quantum mechanics tells us that we can only acquire much more limited information about the state of a qubit.

When we measure, a qubit we get either the result 0 with probability $|\alpha|^2$ or the result 1 with probability $|\beta|^2$.

Therefore, $|\alpha|^2 + |\beta|^2 = 1$.

As the probability sums up to 1.

In geometrically, the condition that the qubit's state is nomalized to length 1.

Qubit can exist in a continuum of states between $|0\rangle$ and $|1\rangle$, until it is measured.

For instance,

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

When we measure, we get the result 0 with probability fifty percent ($|\frac{1}{\sqrt{2}}|^2$) and the result 1 with probability $\frac{1}{2}$.

This state is denoted as $|+\rangle$.

## 2.2 Geometric Representation

As $|\alpha|^2 + |\beta|^2 = 1$, we can rewrite the equation as follows.

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

Where, $\theta$, $\phi$, and $\gamma$ are real numbers.

As $e^{i\gamma}$, it has no effect on the probabilities of measurement outcomes.

Then, we can ignore $e^{i\gamma}$ the front one for now.

Then this will be re-written as follows.

$$|\psi\rangle = \cos(\frac{\theta}{2})|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})|1\rangle \tag{4}$$

The numbers $\theta$ and $\phi$ are called *Bloch sphere coordinates*.

The Bloch sphere is a unit sphere in three-dimensional space.

This provides a geometric representation of the state of a qubit.

The north pole of the Bloch sphere is the state $|0\rangle$, and the south pole is the state $|1\rangle$.

The equator of the Bloch sphere is the set of all superpositions of $|0\rangle$ and $|1\rangle$.

Then how much information can we get from a qubit?

There are infinite number of points on the unit sphere, therefore, in principle, we can get infinite amount of information.

However, with the behavior of a qubit under measurment, a qubit will give only either 0 or 1.

Also, measurement changes the state of a qubit, collapsing it from its superpositino of $|0\rangle$ and $|1\rangle$ to either $|0\rangle$ or $|1\rangle$.

If measurement of $|+\rangle$ provies the result 0, then the state of the qubit is $|0\rangle$.

## 2.3 Multiple Qubits

# 3 Linear Algebra

Linear algebra is the study of vector spaces and linear maps between them.
Linear Algebra is the language of quantum computing, therefore, this is signficant to know the linear algebra.
The basic objects of study in linear algebra are vector spaces.
In quantum computing, we focus more on finite-dimensional vector spaces and complex vector spaces.

## 3.1 Vector Spaces

Complex vector space is $\mathbb{C}^n$ where $n$ tuples of complex numbers, $(z_1, z_2, ..., z_n)$, are elements of $\mathbb{C}^n$. Elements of $\mathbb{C}^n$ are called **vectors**.
Sometimes, column matrix notation is used as well for indicating a vector.

$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} \tag{5}$$

There is an addition operation for vectors.

### 3.1.1 Addition Operation

In $\mathbb{C}^n$, the addition operation is defined as follows.

$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} + \begin{bmatrix} z_1' \\ z_2' \\ \vdots \\ z_n' \end{bmatrix} = \begin{bmatrix} z_1 + z_1' \\ z_2 + z_2' \\ \vdots \\ z_n + z_n' \end{bmatrix} \tag{6}$$

This addition of complex numbers are just the addition of real and imaginary parts.

### 3.1.2 Scalar Multiplication Operation

There is a scalar multiplication operation for vectors.
In $\mathbb{C}^n$, the scalar multiplication operation is defined as follows.

$$\alpha \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} \alpha z_1 \\ \alpha z_2 \\ \vdots \\ \alpha z_n \end{bmatrix} \tag{7}$$

where $\alpha$ is a scalar.

This scalar multiplication of complex numbers are just the scalar multiplication of real and imaginary parts.

### 3.1.3 Notation

There is a standard quantum mechanical notation for vectors in a vector space.

$$|\psi\rangle \tag{8}$$

$\psi$ or $\phi$ are often used for the name of a vector.

However, any lable can be used for the name of a vector.

The $|\rangle$ is used to indicate that the object is a vector.

The $|\psi\rangle$ is called a **ket**.

### 3.1.4 Zero Vector

The zero vector is usually defined as $\mathbf{0}$.

This satifisfies the following equation.

$$\mathbf{0} + |\psi\rangle = |\psi\rangle \tag{9}$$

for any vector $|\psi\rangle$.

(We don't usually use the ket notation for the zero vector.)

Scalar multiplication of the zero vector is also defined as follows.

$$z\mathbf{0} = \mathbf{0} \tag{10}$$

for any complex number $z$.

### 3.1.5 Things to Note

- $(z_1, z_2, ..., z_n)$ is to denote a column matrix with entries $z_1, z_2, ..., z_n$.

- In $\mathbb{C}^n$, the zero element is $(0, 0, ..., 0)$.

- Vector space of a vector space V is a subset W of V such that W is a vector space which means that W is closed under addition and scalar multiplication.

## 3.2 Table of Notations and Descriptions

| Notation | Description |
|---|---|
| $z^*$ | Complex conjugate of the complex number $z$ . e.g. $(1+i)^* = 1 - i$ |
| $|\psi\rangle$ | Standard quantum mechanical notation for vectors. Known as a *ket*. |
| $\langle\psi|$ | Vector dual to $|\psi\rangle$. Known as a *bra*. |
| $\langle\psi|\phi\rangle$ | Inner product of $|\psi\rangle$ and $|\phi\rangle$. |
| $|\phi\rangle \otimes |\psi\rangle$ | Tensor product of $|\phi\rangle$ and $|\psi\rangle$. |
| $|\psi\rangle|\psi\rangle$ | Shorthand for $|\psi\rangle \otimes |\psi\rangle$. |
| $A^*$ | Complex conjugate of the matrix $A$. |
| $A^T$ | Transpose of the matrix $A$. |
| $A^\dagger$, (1) | Hermitian conjugate or adjoint of the matrix $A$, $A^\dagger = (A^T)^*$. |
| $\langle\phi|A|\psi\rangle$, (2) | Inner product of $|\phi\rangle$ and $A|\psi\rangle$. |

(1):

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix} \tag{11}$$

(2): Equivately, inner product between $A^\dagger|\phi\rangle$ and $|\psi\rangle$.

## 3.3 Bases and Linear Independence

A *spanning set* for a vector space is a set of vectors $|\mathbf{v}_1\rangle, |\mathbf{v}_2\rangle, \ldots, |\mathbf{v}_n\rangle$ such that any vector in the vector space can be written as a linear combination:

$$|\mathbf{v}\rangle = \sum_{i=1}^{n} \alpha_i |\mathbf{v}_i\rangle \tag{12}$$

of vectors in that set. For example, spanning set for the vector space $\mathbb{C}^2$ are following vectors.

$$|\mathbf{v}_1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |\mathbf{v}_2\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{13}$$

As any vector

$$|\mathbf{v}\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \tag{14}$$

in $\mathbb{C}^2$ can be written as a linear combination of $a_1|\mathbf{v}_1\rangle$ and $a_2|\mathbf{v}_2\rangle$. $|\mathbf{v}_1\rangle$ and $|\mathbf{v}_2\rangle$ span the vector space $\mathbb{C}^2$.

As there are infinitely many spanning sets for a vector space, following also can be a spanning set for $\mathbb{C}^2$.

$$|\mathbf{v}_1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, |\mathbf{v}_2\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \tag{15}$$

This can be represented with the $|\mathbf{v}\rangle = (a_1, a_2)$ as follows, since $|\mathbf{v}\rangle$ can be written as a linear combination of $|\mathbf{v}_1\rangle$ and $|\mathbf{v}_2\rangle$.

$$|\mathbf{v}\rangle = \frac{a_1 + a_2}{\sqrt{2}}|\mathbf{v}_1\rangle + \frac{a_1 - a_2}{\sqrt{2}}|\mathbf{v}_2\rangle \tag{16}$$

### 3.3.1  Linear Dependence

A set of non-zero vectors $|\mathbf{v}_1\rangle, |\mathbf{v}_2\rangle, \ldots, |\mathbf{v}_n\rangle$ is said to be *linearly dependent* if there exist complex numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$ with at least one of the $\alpha_i$ non-zero such that

$$\sum_{i=1}^{n} \alpha_i |\mathbf{v}_i\rangle = 0 \tag{17}$$

### 3.3.2  Linear Independence

A set of non-zero vectors $|\mathbf{v}_1\rangle, |\mathbf{v}_2\rangle, \ldots, |\mathbf{v}_n\rangle$ is said to be *linearly independent* if only the trivial linear combination of the vectors is equal to the zero vector.

$$\sum_{i=1}^{n} \alpha_i |\mathbf{v}_i\rangle = 0 \Rightarrow \alpha_i = 0 \text{ for all } i \tag{18}$$

### 3.3.3  Basis

Any two sets of linearly independent vectors in a vector space V have the same cardinality. (number of elements) We call this set as a *basis* for V.
The basis always exists for a vector space.

### 3.3.4  Dimension of a Vector Space

The dimension of a vector space is the number of elements in a basis for that vector space.
In this quantum computing textbook, we will only consider finite-dimensional vector spaces.

## 3.4  Exercise 2.1

Show that (1,-1), (1,2) and (2,1) are linearly dependent.
**Solution**

$$1(1, -1) + 2(1, 2) + (-1)(2, 1) = (0, 0) \tag{19}$$

Therefore, (1,-1), (1,2) and (2,1) are linearly dependent as there exist $\alpha_1, \alpha_2, \alpha_3$ with at least one of the $\alpha_i$ non-zero such that

$$\sum_{i=1}^{3} \alpha_i |\mathbf{v}_i\rangle = 0 \tag{20}$$

Dimension theorem states that any two sets of linearly independent vectors in a vector space V have the same cardinality.

Any vector space V has a basis with cardinality equal to the dimension of V which is n = 2 since V is $\mathbb{C}^2$.

However, the set of vectors (1,-1), (1,2) and (2,1) has cardinality equal to 3.

Therefore, (1,-1), (1,2) and (2,1) are linearly dependent.

## 3.5  Linear Operators and Matrices

A linear operator between two vector spaces V and W is a function $A : V \to W$ which is linear in its inputs,

$$A(\sum_i \alpha_i |\mathbf{v}_i\rangle) = \sum_i \alpha_i A(|\mathbf{v}_i\rangle) \tag{21}$$

Linear operator A is defined on a vector space V which menas that A is a linear operator from V to V.

We can say A maps V to V.

### 3.5.1  Identity Operator

The identity operator $I_V$ is defined as follows.

$$I_V(|\mathbf{v}\rangle) = |\mathbf{v}\rangle \tag{22}$$

for all vectors $|\mathbf{v}\rangle$ in V.

### 3.5.2  Zero Operator

The zero operator 0 is defined as follows.

$$0(|\mathbf{v}\rangle) = 0 \tag{23}$$

for all vectors $|\mathbf{v}\rangle$ in V.

This maps all vectors to the zero vector.

### 3.5.3  Operators

Say V, W, and X are vector spaces.

$A : V \to W$ and $B : W \to X$ are linear operators.

Then, $BA$ to denote the composition of $B$ and $A$ is defined as follows.

$$BA(|\mathbf{v}\rangle) = B(A(|\mathbf{v}\rangle)) \tag{24}$$

for all vectors $|\mathbf{v}\rangle$ in V.

Interengtingly, matrix representations can be used to represent linear operators.

### 3.5.4 Matrix Representation of Linear Operators

Connection can be explained as follows.

Imagine there is *m by n complex matrix A* with entries $a_{ij}$.

z Then, A can be used to represent a linear operator $A : \mathbb{C}^n \to \mathbb{C}^m$ as follows. More specifically, A maps $\mathbb{C}^n$ to $\mathbb{C}^m$.

$$A(\sum_{i=1}^{n} a_i|\mathbf{v}_i\rangle) = \sum_{i=1}^{n} a_i A(|\mathbf{v}_i\rangle) \tag{25}$$

As matrices can be given a linear operator, linear operators can be given a matrix representation.

Say that $A : V \to W$ is a linear operator between vector spaces V and W.

Suppose that $|\mathbf{v}_1\rangle, |\mathbf{v}_2\rangle, \ldots, |\mathbf{v}_m\rangle$ is a basis for V, and $|\mathbf{w}_1\rangle, |\mathbf{w}_2\rangle, \ldots, |\mathbf{w}_n\rangle$ is a basis for W.

Then for each $j$ in the range $1 \leq j \leq m$, there exist complex numbers $a_{1j}, a_{2j}, \ldots, a_{nj}$ such that

$$A(|\mathbf{v}_j\rangle) = \sum_{i=1}^{n} a_{ij}|\mathbf{w}_i\rangle \tag{26}$$

This is important to note that the matrix representation of a linear operator depends on the choice of basis.

Therefore, connection between matrices and linear operators, we must specify the imput and output basis states for the input and output vector spaces.

## 3.6 Exercise 2.2, 2.3 and 2.4

### 3.6.1 Exercise 2.2

Suppose V is a vector space with basis vectors $|0\rangle$ and $|1\rangle$, and A is a linear operator from V to V such that $A|0\rangle = |1\rangle$ and $A|1\rangle = |0\rangle$. Give a matrix representation for A, with respect to the input basis $|0\rangle$, $|1\rangle$, and the output basis $|0\rangle$, $|1\rangle$. Find input and output bases which give rise to a different matrix representation of A.

**Solution**

First of all, as $|0\rangle$ and $|1\rangle$ can be written as follows,

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{27}$$

And, we have

$$A = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} \tag{28}$$

As $A|0\rangle = |1\rangle$ and $A|1\rangle = |0\rangle$, we have

$$A|0\rangle = 0|0\rangle + 1|1\rangle = 0\begin{bmatrix}1\\0\end{bmatrix} + 1\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix} \rightarrow \tag{29}$$

$$A|0\rangle = \begin{bmatrix}a_{00} & a_{01}\\a_{10} & a_{11}\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} \rightarrow \begin{bmatrix}a_{00}\\a_{10}\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix} \tag{30}$$

This demonstrates that $a_{00} = 0$ and $a_{01} = 1$.
Similarly, we have

$$A|1\rangle = 1|0\rangle + 0|1\rangle = \begin{bmatrix}a_{00} & a_{01}\\a_{10} & a_{11}\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} \tag{31}$$

This demonstrates that $a_{10} = 1$ and $a_{11} = 0$.
The matrix representation of A is as follows.

$$A = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix} \tag{32}$$

as the input basis is $|0\rangle$ and $|1\rangle$, and the output basis is $|0\rangle$ and $|1\rangle$.
Now, we find input and output bases which give rise to a different matrix representation of A.
Let's say that the input basis is . . . .

### 3.6.2   Exercise 2.3

Suppose A is a linear operator from vector space V to vector space W , and B is a linear operator from vector space W to vector space X. Let $|vi\rangle, |wj\rangle$, and $|xk\rangle$ be bases for the vector spaces V,W, and X, respectively. Show that the matrix representation for the linear transformation BA is the matrix product of the matrix representations for B and A, with respect to the appropriate bases.

   **Solution**

### 3.6.3   Exercise 2.4

Show that the identity operator on a vector space V has a matrix representation which is one along the diagonal and zero everywhere else, if the matrix representation is taken with respect to the same input and output bases. This matrix is known as the identity matrix.

## 3.7   The Pauli Matrices

The *Pauli matrices* are a set of three 2 by 2 complex matrices.
Following are the *Pauli matrices*.

10

$$\sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \tag{33}$$

$$\sigma_1 = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X \tag{34}$$

$$\sigma_2 = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = Y \tag{35}$$

$$\sigma_3 = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z \tag{36}$$

## 3.8    Inner Products

*Inner product* is a function that maps two vectors to a complex number as output.

Stand quantum mechanical notation for inner product is as follows.

$$\langle \mathbf{v} | \mathbf{w} \rangle \tag{37}$$

where $\mathbf{v}$ and $\mathbf{w}$ are vectors in the inner product space.

And, notation $\langle \mathbf{v} |$ is used for dual vector to the vector $| \mathbf{v} \rangle$.

Dual is a linear map from the vector space to the field of complex numbers.

This is defined as follows.

$$\langle \mathbf{v} | (| \mathbf{w} \rangle) = \langle \mathbf{v} | \mathbf{w} \rangle = (| \mathbf{v} \rangle, | \mathbf{w} \rangle) \tag{38}$$

Matrix representation of dual vectors is just a row vector.

A function (.,.) from V X V to $\mathbb{C}$ is an inner product if it satisfies the following properties.

Function (.,.) is notation for inner product for now.

(1) (.,.) is linear in the second argument.

$$\left( | \mathbf{v} \rangle, \sum_i \lambda_i | \mathbf{w}_i \rangle \right) = \sum_i \lambda_i (| \mathbf{v} \rangle, | \mathbf{w}_i \rangle) \tag{39}$$

(2) $(| \mathbf{v} \rangle, | \mathbf{w} \rangle) = (| \mathbf{w} \rangle, | \mathbf{v} \rangle)^*$

(3) $(| \mathbf{v} \rangle, | \mathbf{w} \rangle) \geq 0$ with equality if and only if $| \mathbf{v} \rangle = 0$

For instance, inner product of two vectors in $\mathbb{C}^n$ is as follows.

$((y_1, y_2, \ldots, y_n), (z_1, z_2, \ldots, z_n)) = \sum_i y_i^* z_i$

$$= $$

$$\begin{bmatrix} y_1^* & y_2^* & \cdots & y_n^* \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} \tag{40}$$

Vector space equipped with an inner product is called an *inner product space*.

### 3.9 Exercise 2.5, 2.6

#### 3.9.1 Exercise 2.5

Verify that $(.,.)$ just defined is an inner product on $\mathbb{C}^n$.

**Solution**

On $\mathbb{C}^n$, $(.,.)$ is defined as follows.

$((y_1, y_2, \ldots, y_n), (z_1, z_2, \ldots, z_n)) = \sum_i y_i^* z_i$

$$
= \begin{bmatrix} y_1^* & y_2^* & \cdots & y_n^* \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} \tag{41}
$$

Also, there are three conditions should be qualified to be considered as an inner product.

(1) $(.,.)$ is linear in the second argument.

$$
(|\mathbf{v}\rangle, \sum_i \lambda_i |\mathbf{w}_i\rangle) = \sum_i \lambda_i (|\mathbf{v}\rangle, |\mathbf{w}_i\rangle) \tag{42}
$$

(2) $(|\mathbf{v}\rangle, |\mathbf{w}\rangle) = (|\mathbf{w}\rangle, |\mathbf{v}\rangle)^*$

(3) $(|\mathbf{v}\rangle, |\mathbf{w}\rangle) \geq 0$ with equality if and only if $|\mathbf{v}\rangle = 0$

Now, we verify that $(.,.)$: $\mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ satisfies the three conditions.

Prove (1):

....

Prove (2):

As $((y_1, y_2, \ldots, y_n), (z_1, z_2, \ldots, z_n)) = \sum_i y_i^* z_i,$

$= (\sum_i y_i z_i^*)^*$

$= (\sum_i z_i^* y_i)^*$

$= ((z_1, z_2, \ldots, z_n), (y_1, y_2, \ldots, y_n))^*$

Therefore, this satisfies (2).

Prove (3):

$(\mathbf{0}, \mathbf{0}) = \sum_i 0 * 0 = 0$

When $\mathbf{v} = (v_1, v_2, \ldots, v_n) \neq \mathbf{0}$,

there is at least one $v_i \neq 0$.

Therefore, $((v_1, v_2, \ldots, v_n), (v_1, v_2, \ldots, v_n)) = \sum_i v_i^* v_i = \sum_i |v_i|^2 \geq |v_j|^2 > 0$

### 3.10 Exercise 2.6

Show that any inner product $(.,.)$ is conjugate-linear in the first argument.

$((\sum_i \lambda_i |\mathbf{v}_i\rangle), |\mathbf{w}\rangle) = \sum_i \lambda_i^* (|\mathbf{v}_i\rangle, |\mathbf{w}\rangle)$

**Solution**

$$((\sum_i \lambda_i |\mathbf{v}_i\rangle), |\mathbf{w}\rangle) = (|\mathbf{w}\rangle, (\sum_i \lambda_i |\mathbf{v}_i\rangle))^* \tag{43}$$

$$= (\sum_i \lambda_i (|\mathbf{w}_i\rangle, |\mathbf{v}_i\rangle))^* \tag{44}$$

$$= \sum_i \lambda_i^* (|\mathbf{w}_i\rangle, |\mathbf{v}_i\rangle)^* \tag{45}$$

$$= \sum_i \lambda_i^* (|\mathbf{v}_i\rangle, |\mathbf{w}\rangle) \tag{46}$$

## 3.11    Hilbert Spaces

Hilbert Space is same as inner product space in quantum computation, and quantum information.
There are things to note.
When inner product is zero, vectors are orthogonal.
For instance, $|\mathbf{v}\rangle = (1,0)$ and $|\mathbf{w}\rangle = (0,1)$ are orthogonal.
There is a notion of *norm* of a vector.
Norm of a vector is defined as follows.

$$||\mathbf{v}|| = \sqrt{\langle \mathbf{v}|\mathbf{v}\rangle} \tag{47}$$

*Unit Vector* is a vector with norm 1 which is defined as follows.

$$||\mathbf{v}|| = 1 \tag{48}$$

We sometimes called unit vector as *normalized vector*.
For any non-zero vector $|\mathbf{v}\rangle \in V$, we can normalize vector by dividing by its norm.

$$|\mathbf{v}\rangle' = \frac{1}{||\mathbf{v}||} |\mathbf{v}\rangle \tag{49}$$

where $|\mathbf{v}\rangle'$ is a normalized vector.

Set $|\mathbf{i}\rangle$ of vectors with index $i$ is orthonormal if each vector is a unit vectorm and distinct vectors are orthogonal.
Which means,

$$\langle \mathbf{i}|\mathbf{j}\rangle = \delta_{ij} \tag{50}$$

where $i$ and $j$ are chosen from the same index set.

## 3.12   Exercise 2.7

Verify that $|\mathbf{w}\rangle = (1, 1)$ and $|\mathbf{v}\rangle = (1, -1)$ are orthogonal.
What are the normalized forms of these vectors?

**Solution**
When $|\mathbf{v}\rangle$, $|\mathbf{w}\rangle$ are orthogonal, if $\langle \mathbf{v}|\mathbf{w}\rangle = 0$.
And the norm of $|\mathbf{v}\rangle$ is $\sqrt{\langle \mathbf{v}|\mathbf{v}\rangle}$.
Therefore, we have to shows that $\langle \mathbf{w}|\mathbf{v}\rangle = 0$.

$$\langle \mathbf{w}|\mathbf{v}\rangle = (1, 1)(1, -1) = 1 * 1 + 1 * (-1) = 0 \tag{51}$$

Norms of $|\mathbf{v}\rangle$ and $|\mathbf{w}\rangle$ are as follows.

$$||\mathbf{v}|| = \sqrt{\langle \mathbf{v}|\mathbf{v}\rangle} = \sqrt{(1, -1)(1, -1)} = \sqrt{1 * 1 + (-1) * (-1)} = \sqrt{2} \tag{52}$$

$$||\mathbf{w}|| = \sqrt{\langle \mathbf{w}|\mathbf{w}\rangle} = \sqrt{(1, 1)(1, 1)} = \sqrt{1 * 1 + 1 * 1} = \sqrt{2} \tag{53}$$

Therefore, normalized forms of $|\mathbf{v}\rangle$ and $|\mathbf{w}\rangle$ are as follows.

$$|\mathbf{v}\rangle' = \frac{1}{||\mathbf{v}||}|\mathbf{v}\rangle = \frac{1}{\sqrt{2}}(1, -1) \tag{54}$$

$$|\mathbf{w}\rangle' = \frac{1}{||\mathbf{w}||}|\mathbf{w}\rangle = \frac{1}{\sqrt{2}}(1, 1) \tag{55}$$

In matrix form,

$$|\mathbf{v}\rangle' = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix}, |\mathbf{w}\rangle' = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \tag{56}$$

## 3.13   Gram-Schmidt procedure

Suppose that $|\mathbf{w}_1\rangle$, $|\mathbf{w}_2\rangle$, ..., $|\mathbf{w}_d\rangle$ is a basis set for some vector space V with an inner product.
Using the *Gram-Schmidt procedure*, which can be used to construct an orthonormal basis set $|\mathbf{v}_1\rangle$, $|\mathbf{v}_2\rangle$, ..., $|\mathbf{v}_d\rangle$ for V.
Define $|\mathbf{v}_1\rangle$ as follows.

$$|\mathbf{v}_1\rangle = \frac{1}{||\mathbf{w}_1||}|\mathbf{w}_1\rangle \tag{57}$$

and for $1 \leq k \leq d - 1$, define $|\mathbf{v}_{k+1}\rangle$ as follows.

$$|\mathbf{v}_{k+1}\rangle = \frac{|\mathbf{w}_{k+1}\rangle - \sum_{i=1}^{k}\langle vi|w_{k+1}\rangle|vi\rangle}{||\,|\mathbf{w}_{k+1}\rangle - \sum_{i=1}^{k}\langle vi|w_{k+1}\rangle|vi\rangle||} \tag{58}$$

Any infinite dimensinal vector space of dimension d has an orthonormal basis $|\mathbf{v}_1\rangle$, $|\mathbf{v}_2\rangle$, ..., $|\mathbf{v}_d\rangle$.

## 3.14   Hilbert Space with convenient matrix representation