Project Tenji:
Quantum Information Theory

Contents

Chapter 1

INTRODUCTION

1.1 Classical Information

The most basic piece of information is called a bit, and this basically represents a yes-no answer to a question.

To represent this <u>mathematically</u> we use binary numbers,a binary number can be 0 or 1.

Physically we can implement a bit with an electrical circuit $\begin{cases} \text{zero volts} \rightarrow \text{ binary } 0 \\ + \text{ five volts} \rightarrow \text{ binary } 1 \end{cases}$

The smallest number n of bits required to represent m different state :

$$2^n \geq m$$

n bits can store m different messages :

$$\log_2(m) = n$$

A byte is a string of eight bits linked together $(\log_2(256) = 8)$

1.2 Entropy and Shannon's information theory

To get a more accurate estimation of the information content in a signal, the key step taken by Shannon was that he asked:

How likely is it that we are going to see a given piece of information?

And that allows us to characterize how much information we actually gain from a signal.

- If a message has a very high probability of occurrence, then we don't gain all that much new information when we come across it.

- On the other hand, if a message has a low probability of occurrence, when we are made of aware of it, we gain a significant amount of information.

Shannon quantified this by taking the base 2 logarithm of the probability of a given message occurring. The information content of a message by I, and the probability of its occurrence by p, then :

$$I = -\log_2(p)$$

- A message that is unlikely to occur has a low probability and therefore has a large information content.

- A message that is very likely to occur has a high probability and therefore has a small information content.

Example :

Let's suppose that the probability of an earthquake not happening tomorrow is 0.995. The information content of this fact is
$I = -\log_2(0.995) = 0.0072$.
Now the probability that an earthquake does happen tomorrow is 0.005. The information content of this piece of information is
$I' = -\log_2(0.005) = 7.7.6439$

Now let X be a random variable characterized by a probability distribution $\vec{p}$, and suppose that it can assume one of the values $x_1, x_2, ..., x_n$ with probabilities $p_1, p_2, ..., p_n$
The Shannon entropy of X is defined as :

$$H(X) = -\sum_i p_i \log_2(p_i)$$

- If we are certain what the message is, the Shannon entropy is zero.

- The more uncertain we are as to what comes next, the higher the Shannon entropy.

Example :

Suppose that we have a signal that always transmits a "2", The probability of obtaining a 2 is 1,
So the entropy or disorder is : $H = -\log_2(1) = 0$
A signal that has all the same characters with no changes has no disorder and hence no entropy.

Chapter 2

QUBITS AND QUANTUM STATES

2.1 The Qubit

Qubit is the basic unit of information in quantum computing which is short for quantum bit.

A qubit can exist in the state $|0\rangle, |1\rangle$ or also in a superposition state $\begin{cases} |\psi\rangle = |0\rangle \\ |\psi\rangle = |1\rangle \\ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \end{cases}$

Where $|\alpha|^2$ and $|\beta|^2$ tells us the probability of finding $|\psi\rangle$ in state $|0\rangle$ and $|1\rangle$.
$|\alpha|^2 + |\beta|^2 = 1$
$|\alpha|^2 = (\alpha)(\alpha^*)$ and $|\beta|^2 = (\beta)(\beta^*)$
When a qubit is measured, it is only going to be found to be in the state $|0\rangle$ or the state $|1\rangle$.

2.2 Vector spaces

A vector space V is a nonempty set with elements u, v called vectors for which the following two operations are defined:

- Vector addition $,w \in V, w = u + v$

- Scalar multiplication,$\alpha \in \mathbb{C}, \alpha u \in V$

in addition :

- Associativity of addition : $(u + v) + w = u + (v + w)$

- zero vector such as : $u + 0 = 0 + u = u$

- additive inverse :$u + (-u) = (-u) + u = 0$

- addition of vectors is commutative : $u + v = v + u$

One particular vector space that is important in quantum computation is the vector space is $\mathbb{C}$.
we label the elements of $\mathbb{C}$ by $|a\rangle, |b\rangle, |c\rangle$.
we write down a vector as column vector :

$$|a\rangle = \begin{pmatrix} a_1 \\ a_2 \\ ... \\ a_n \end{pmatrix}$$

Multiplication of a vector by a scalar proceeds as :

$$\alpha \left|a\right\rangle = \alpha \begin{pmatrix} a_1 \\ a_2 \\ ... \\ a_n \end{pmatrix} = \begin{pmatrix} \alpha a_1 \\ \alpha a_2 \\ ... \\ \alpha a_n \end{pmatrix}$$

Vector addition :

$$\left|a\right\rangle + \left|b\right\rangle = \begin{pmatrix} a_1 \\ a_2 \\ ... \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ ... \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ ... \\ a_n + b_n \end{pmatrix}$$

2.3 Linear combinations of vectors

A linear combination of these vectors is given by

$$\alpha_1 \left|v_1\right\rangle + \alpha_2 \left|v_2\right\rangle + ... + \alpha_n \left|v_n\right\rangle = \sum_{i=1}^{n} \alpha_i \left|v_i\right\rangle$$

An arbitrary qubit can be writes as $\left|\psi\right\rangle = \alpha \left|0\right\rangle + \beta \left|1\right\rangle$

$$\left|\psi\right\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} \implies \text{ we identify } \left|0\right\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } \left|1\right\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Linear independence

if one vector of the set can be written as a linear combination of the other vectors in the set, then the set is linearly dependent.
a set of vectors is that of linear independence if:

$$\alpha_1 \left|v_1\right\rangle + \alpha_2 \left|v_2\right\rangle + ... + \alpha_n \left|v_n\right\rangle = 0$$

Note that :
    A spanning set of vectors for a given space V is not unique.

2.4 Basis and dimension

When a set of vectors is linearly independent and they span the space, the set is known as a basis.
We can express any vector in the space V in terms of a linear expansion on a basis set.
The dimension of a vector space V is equal to the number of elements in the basis set.
A quantum state $\left|\psi\right\rangle$ can be written as a linear combination of a basis set $\left|v_i\right\rangle$ with complex coefficients of expansion c_i as :

$$\left|\psi\right\rangle = \sum_{i=1}^{n} c_i \left|v_i\right\rangle = c_1 \left|v_1\right\rangle + c_2 \left|v_2\right\rangle + ... + c_n \left|v_n\right\rangle$$

The modulus squared of a given coefficient c_i gives the probability that measurement finds the system in the state $\left|v_i\right\rangle$.

2.5   Inner Products

We write the inner product between two vectors $|u\rangle , |v\rangle$ with the notation $\langle u|v\rangle$.

The inner product is a complex number, the conjugate of this complex number satisfies : $\langle u|v\rangle^* = \langle v|u\rangle$. The norm of a vector u is : $||u|| = \sqrt{\langle u|u\rangle}$.

$$|u\rangle^\dagger = \langle u| \rightarrow \begin{pmatrix} a_1 \\ a_2 \\ ... \\ a_n \end{pmatrix}^\dagger = \begin{pmatrix} a_1^* & a_2^* & ...a_3^* \end{pmatrix}$$

2.6   Orthonormality

We say that $|u\rangle , |v\rangle$ are orthogonal when

$$\langle u|v\rangle = 0$$

When the norm of a vector is unity, we say that vector is normalized

$$\langle a|a\rangle = 1$$

If each element of a set of vectors is normalized and the elements are orthogonal with respect to each other, we say the set is orthonormal.

2.6.1   GRAM-SCHMIDT orthogonalisation

An orthonormal basis can be produced from an arbitrary basis by application of the Gram-Schmidt orthogonalisation process.
let $\{|v_1\rangle , |v_2\rangle , ..., |v_n\rangle\}$,be a basis for an inner product space V.
The Gram-Schmidt process constructs an orthogonal basis $|w_i\rangle$ as follows :
$|w_1\rangle = |v_1\rangle$
$|w_2\rangle = |v_2\rangle - \dfrac{\langle w_1|v_2\rangle}{\langle w_1|w_1\rangle} |w_1\rangle$
....
$|w_n\rangle = |v_n\rangle - \dfrac{\langle w_1|v_n\rangle}{\langle w_1|w_1\rangle} |w_1\rangle - \dfrac{\langle w_2|v_n\rangle}{\langle w_2|w_2\rangle} |w_2\rangle - ... - \dfrac{\langle w_{n-1}|v_n\rangle}{\langle w_{n-1}|w_{n-1}\rangle} |w_{n-1}\rangle$
To form an orthonormal set using the Gram-Schmidt procedure, divide each vector by its norm.

2.7   The Cauchy-Schwartz and triangle inequalities

The Cauchy-Schwarz inequality :
$$|\langle\psi|\phi\rangle|^2 \le \langle\psi|\psi\rangle \langle\phi|\phi\rangle$$

The triangle inequality :

$$\sqrt{\langle\psi + \phi|\psi + \phi\rangle} \le \sqrt{\langle\psi|\psi\rangle} + \sqrt{\langle\phi|\phi\rangle}$$

Chapter 3

MATRICES AND OPERATORS

An operator is a mathematical rule that can be applied to a function to transform it into another function. An operator $\hat{A}$ is a mathematical rule that transforms a ket $|\psi\rangle$ into another ket that we will call $|\phi\rangle$:

$$\hat{A}|\psi\rangle = |\phi\rangle$$

Operators can act also on bras:

$$\hat{A}\langle\mu| = \langle\nu|$$

We say that an operator is linear if :

$$\hat{A}(\alpha|\psi_1\rangle + \beta|\psi_2\rangle) = \alpha\hat{A}|\psi_1\rangle + \beta\hat{A}|\psi_2\rangle$$

The simplest operator is the identity operator $\hat{I}$:

$$\hat{I}|\psi\rangle = |\psi\rangle$$

The zero operator :

$$\hat{0}|\psi\rangle = 0$$

3.1 Outer Products

The product of a ket $|\psi\rangle$ with a bra $\langle\phi|$ which is written as $|\psi\rangle\langle\phi|$, this quantity is an operator.

$$(|\psi\rangle\langle\phi|)|\xi\rangle = |\psi\rangle\langle\phi|\xi\rangle = (\langle\phi|\phi|\xi\rangle)|\psi\rangle$$

3.2 The closure relation

$$\sum_{i=1}^{n} |u_i\rangle\langle u_i| = \hat{I}$$

The closure relation is often useful in manipulating expressions.
For example if $\langle u_i|\psi\rangle = c_i$, an arbitrary state $|\psi\rangle$ can be expanded in terms of the basis $\{|u_i\rangle\}$:

$$|\psi\rangle = \hat{I}|\psi\rangle = \left(\sum_{i=1}^{n}|u_i\rangle\langle u_i|\right)|\psi\rangle = \sum_{i=1}^{n}|u_i\rangle\langle u_i|\psi\rangle = \sum_{i=1}^{n}c_i|u_i\rangle$$

3.3 Representations of operators using matrices

We can find the matrix elements of the operator using the closure relation :

$$\hat{A} = \hat{I}\hat{A}\hat{I} = \left(\sum_i |u_i\rangle \langle u_i|\right) \hat{A} \left(\sum_j |u_j\rangle \langle u_j|\right) = \sum_{i,j} \langle u_i|\hat{A}|u_j\rangle |u_i\rangle \langle u_j|$$

$$\hat{A} = \begin{pmatrix} \langle u_1|\hat{A}|u_1\rangle & \langle u_1|\hat{A}|u_2\rangle & ... & \langle u_1|\hat{A}|u_n\rangle \\ \langle u_2|\hat{A}|u_1\rangle & \langle u_2|\hat{A}|u_2\rangle & ... & \langle u_2|\hat{A}|u_n\rangle \\ & & \ddots & \\ & & & \langle u_n|\hat{A}|u_n\rangle \end{pmatrix}$$

When the matrix representation of an operator is given, it is written with respect to a certain basis. in general :

$$\langle u_i|\hat{A}|u_j\rangle \neq \langle \nu_i|\hat{A}|\nu_j\rangle$$

3.4 Hermitian,Unitary, and Normal operators

An operator A is said to be normal if

$$AA^\dagger = A^\dagger A$$

An operator A is said to be unitary if

$$UU^\dagger = U^\dagger U = I$$

An operator $\hat{A}$ is said to be Hermitian if

$$\hat{A} = \hat{A}^\dagger$$

3.5 Observables

Observables are things we measure in order to characterize the quantum state of a particle

3.5.1 The Pauli operators

- $\sigma_0 |0\rangle = |0\rangle, \sigma_0 |1\rangle = |1\rangle$

$$\sigma_0 = \hat{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- $\sigma_1 |0\rangle = |1\rangle, \sigma_1 |1\rangle = |0\rangle$

$$\sigma_1 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- $\sigma_2 |0\rangle = -i |1\rangle, \sigma_2 |1\rangle = i |0\rangle$

$$\sigma_2 = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

- $\sigma_3 |0\rangle = |0\rangle, \sigma_3 |1\rangle = - |1\rangle$

$$\sigma_3 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

3.6 Eigenvalues and Eigenvectors

A given vector is said to be an eigenvector of an operator A if the following equation is satisfied

$$A \ket{\psi} = \lambda \ket{\psi}$$

The number λ is called an eigenvalue of the operator A.
A common problem in quantum mechanics is the following:
given an operator, find its eigenvalues and eigenvectors.
The first step in this process is to find the eigenvalues using what is known as the characteristic equation :

$$\det |A - \lambda I| = 0$$

3.7 Spectral Decomposition

An operator A belonging to some vector space that is normal and has a diagonal matrix representation with respect to some basis of that vector space.
$\hat{A}$ satisfies the spectral decomposition for the basis $\ket{u_i}$:

$$A = \sum_{i=1}^{n} a_i \ket{u_i} \bra{u_i}$$

Where a_i are the eigenvalues.

3.8 The trace of an operator

The trace of the operator is the sum of the diagonal elements.

$$Tr(A) = \sum_{i=1}^{n} \bra{u_i} A \ket{u_i}$$

Proprieties

- The trace is cyclic, $Tr(ABC) = Tr(CAB) = Tr(BCA)$

- The trace of an outer product is the inner product

$$Tr(\ket{\phi}\bra{\psi}) = \braket{\psi|\phi}$$

$$Tr(A\ket{\psi}\bra{\phi}) = \bra{\psi}A\ket{\phi}$$

- The trace is basis independent.
  let $\ket{u_i}$ and $\ket{\nu_i}$ be two bases for some Hilbert space, then $Tr(A) = \sum \bra{u_i}A\ket{u_i} = \sum \bra{\nu_i}A\ket{\nu_i}$

- The trace of an operator is equal to the sum of its eigenvalues.

- The trace is linear

$$Tr(\alpha A) = \alpha Tr(A), Tr(A + B) = Tr(A) + Tr(B)$$

3.9 The expectation value of an operator

The expectation value of an operator is the mean or average value of that operator with respect to a given quantum state.
if a quantum state $|\psi\rangle$ is prepared many times, and we measure a given operator A each time , the average of measurement result is the expectation value

$$\langle A \rangle = \langle \psi | A | \psi \rangle$$

3.10 Function of operators

The function of an operator can be found by calculating its Taylor expansion :

$$f(A) = \sum_{n=0}^{\infty} a_n A^n$$

If an operator A is normal and has a spectral expansion given by $A = \sum_i a_i |u_i\rangle \langle u_i|$ then

$$f(A) = \sum_i f(a_i) |u_i\rangle \langle u_i|$$

3.11 Unitary transformation

A method known as a unitary transformation can be used to transform the matrix representation of an operator in one basis to a representation of that operator in another basis.
The change of basis matrix from a basis $|u_i\rangle$ to a basis $|v_i\rangle$ is given by :

$$U = \begin{pmatrix} \langle \nu_1 | u_1 \rangle & \langle \nu_1 | u_2 \rangle \\ \langle \nu_2 | u_1 \rangle & \langle \nu_2 | u_2 \rangle \end{pmatrix}$$

We write a state vector $|\psi\rangle$ given in the $|u_i\rangle$ basis in terms of the new $|\nu_i\rangle$ basis as

$$|\psi'\rangle = U |\psi\rangle$$

3.12 Projection operators

A projection operator is an operator that can be formed by writing the outer product using a single ket

$$P = |\psi\rangle \langle \psi|$$

A projection operator is hermitian.
if the state $|\psi\rangle$ is normalized then a projection operator is equal to its own square :

$$P^2 = P$$

3.13 Commutator

The commutator of two operators A and B is defined as :

$$[A, B] = AB - BA$$

When $[A, B] = 0$, we say that the operators A and B commute.
The commutator is antisymmetric :
$$[A, B] = -[B, A]$$

The commutator is linear :
$$[A, B + C] = [A, B] + [A, C]$$

We can use the following rule of distributivity :

$$[A, BC] = [A, B]C + B[A, C]$$

3.14   Uncertainty

The uncertainty ΔA, is a statistical measure of the spread of measurements about the mean

$$\Delta A = \sqrt{\langle A^2 \rangle - \langle A \rangle^2}$$

Two operators A and B, it can be shown that the product of their uncertainties satisfies

$$\Delta A \Delta B \geq \frac{1}{2} |\langle [A, B] \rangle|$$

This is a generalization of the famous Heisenberg uncertainty principle

3.15   Singular Value Decomposition (SVD)

Every $m \times n$ matrix factors into

$$A = U \Sigma V^T$$

Where $\begin{cases} U \text{ is } m \times m \text{ orthogonal matrix} \\ \Sigma \text{ is } m \times n \text{ diagonal matrix} \\ V^T \text{ is } n \times n \text{ orthogonal matrix} \end{cases}$

$$A = \begin{pmatrix} u_1 & u_2 \end{pmatrix} \begin{pmatrix} \sigma_1 & 0 \\ 0 & \sigma_2 \end{pmatrix} \begin{pmatrix} v_1^T \\ v_2^T \end{pmatrix}$$

$\begin{cases} \sigma \text{ Are the singular values} \\ v \text{ Are the right singular vectors} \\ u \text{ Are the left singular vectors} \end{cases}$

What are U, Σ and V

$A^T A = (V \Sigma^T U^T) U \Sigma V^T = V \Sigma^T \Sigma V^T$, $\Sigma^T \Sigma$ is a diagonal matrix.
By the usual diagonalisation the eigenvalue λ for the matrix $A^T A$ are in $\Sigma^T \Sigma$ and the eigenvectors are in V .
Then λ for $A^T A$ are the singular value squared σ^2 for A.
Now we have Σ and V how we get hold of U
$A A^T = U \Sigma V^T V \Sigma^T U^T = U \Sigma \Sigma^T U^T$
So U is eigenvector matrix for $A A^T$, $A A^T$ and $A^T A$ have the same eigenvalues

Refference : MIT RES.18-009 Learn Differential Equations: Up Close with Gilbert Strang and Cleve Moler, Fall 2015

3.16 THE POSTULATES OF QUANTUM MECHANICS

3.16.1 Postulate 1 : The state of a System

- The state of a quantum system is a vector $|\psi(t)\rangle$ in a Hilbert space.

- The state $|\psi(t)\rangle$ contains all information that we can obtain about hte system.

- We work with normalized states such that $\langle\psi|\psi\rangle = 1$.

3.16.2 Postulate 2: Observable quantities represented by operators

- To every dynamical variable A that is a physically measurable quantity, there corresponds an operator A.

- The operator A is Hermitian and its eigenvectors form a complete orthonormal basis of the vector space.

3.16.3 Postulate 3: Measurements

- The possible results of measurement of a dynamical variable A are the eigenvalues a_n of the operator A corresponding to that variable.

- $A = \sum_n a_n P_n$ where P_n is the projection operators $P_n = |u_n\rangle\langle u_n|$, The probability of obtaining measurement result a_n is given by :
$$Pr(a_n) = \langle\psi|P_n|\psi\rangle$$

- The probability amplitude $c_n = \langle u_n|\psi\rangle$ gives us the probability of obtaining measurement result a_n as
$$Pr(a_n) = \frac{|\langle u_n|\psi\rangle|^2}{\langle\psi|\psi\rangle} = \frac{|c_n|^2}{\langle\psi|\psi\rangle}$$

- A measurement result a_n causes the collapse of the wave-function,meaning that the system is left in state $|u_n\rangle$

3.16.4 Postulate 4: Time evolution of the system

- The time evolution oa a closed quantum system is governed by the Schrodinger equation:

$$i\hbar\frac{\partial}{\partial t}|\psi\rangle = H|\psi\rangle$$

Where H is the Hamiltonian

- The state of the system at a later time t is given by

$$|\psi(t)\rangle = e^{-i\frac{Ht}{\hbar}}|\psi(0)\rangle$$

Therefore the time evolution of a quantum state is governed by the unitary operator

$$U = e^{-i\frac{Ht}{\hbar}}$$

Chapter 4

TENSOR PRODUCTS

In the context of quantum information processing, it is necessary to work with multi particles states.
Suppose that H_1 and H_2 are two Hilbert spaces of dimension N_1 and N_2.
We can put these two Hilbert spaces together to construct a larger Hilbert space H

$$H = H_1 \otimes H_2$$

The dimension of H : $\dim(H) = N_1 N_2$

Let $|\phi\rangle \in H_1$ and $|\xi\rangle \in H_2$, we can construct a vector $|\psi\rangle \in H$:

$$|\psi\rangle = |\phi\rangle \otimes |\xi\rangle$$

- The tensor product of two vectors is linear.

$$|\phi\rangle \otimes [|\xi_1\rangle + |\xi_2\rangle] = |\phi\rangle \otimes |\xi_1\rangle + |\phi\rangle \otimes |\xi_2\rangle$$
$$[|\phi_1\rangle + |\phi_2\rangle] \otimes |\xi\rangle = |\phi_1\rangle \otimes |\xi\rangle + |\phi_2\rangle \otimes |\xi\rangle$$

- Tensor product is linear with respect to scalars

$$|\phi\rangle \otimes (\alpha |\xi\rangle) = \alpha |\phi\rangle \otimes |\xi\rangle$$

- The order of the tensor product is not relevant

$$|\phi\rangle \otimes |\xi\rangle = |\xi\rangle \otimes |\phi\rangle$$

4.1   Inner product

Suppose $\begin{cases} |\psi_1\rangle = |\phi_1\rangle \otimes |\xi_1\rangle \\ |\psi_2\rangle = |\phi_2\rangle \otimes |\xi_2\rangle \end{cases}$

$$\langle\psi_1|\psi_2\rangle = ((\langle\phi_1| \langle\xi_1|)(|\phi_2\rangle |\xi_2\rangle)) = \langle\phi_1|\phi_2\rangle \langle\xi_1|\xi_2\rangle$$

4.2   Matrix Representation

$$|\phi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \text{ and } |\xi\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$$

The tensor product :

$$|\phi\rangle \otimes |\xi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

4.3 Operators and tensor product

Let A be an operator that acts on vectors $|\phi\rangle$, and B act on vectors $|\xi\rangle$

$$(A \otimes B)|\psi\rangle = (A \otimes B)(|\phi\rangle \otimes |\xi\rangle) = (A|\phi\rangle) \otimes (B|\xi\rangle)$$

4.4 Tensor Products of matrices

Let

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

The matrix representation of the tensor product $A \otimes B$ is

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}$$

4.5 Note

Not all states can be written as product of states, this is what will be called later entanglement.

Chapter 5

THE DENSITY OPERATOR

5.1   The density operator for a pure state

When a system is in a definite state, we say the system is in a pure state.
The density operator is an average operator that will allow us to describe a statistical mixture.
The density operator for a state $|\psi\rangle$ is given by :

$$\rho = |\psi\rangle \langle\psi| = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \end{pmatrix} \begin{pmatrix} a_1{}^* & a_2{}^* & \dots \end{pmatrix} = \begin{pmatrix} |a_1|^2 & a_1 a_2{}^* & \dots \\ a_2 a_1{}^* & |a_2|^2 & \dots \\ & & \ddots \end{pmatrix}$$

Then, diagonal elements are probabilities of being in the state $|u_i\rangle$:

$$p_i = |a_i|^2 = \langle u_i|\psi\rangle \langle\psi|u_i\rangle = \langle u_i|\rho|u_i\rangle$$

Due to the conservation of probability the trace of the density operator is always 1

$$Tr(\rho) = \sum_j \langle u_j|\rho|u_j\rangle = \sum_j \langle u_j|\psi\rangle \langle\psi|u_j\rangle = \sum_j c_j c_j{}^* = \sum_j |c_j|^2 = 1$$

5.1.1   Properties of a density operator

- The density operator is Hermitian

- $Tr(\rho) = 1$

- ρ is a positive operator, meaning $\langle u|\rho|u\rangle \geq 0$ for any state vector $|u\rangle$

If a system is in a pure state $|\psi\rangle$ then :

$$\rho^2 = \rho$$

$$Tr(\rho^2) = 1$$

5.2 Using the density operator to find the expectation value

The expectation value of an operator A can be written in terms of the density operator as:

$$\langle A \rangle = \sum_{k,l=1}^{n} \langle u_l|\rho|u_k\rangle \langle u_k|A|u_l\rangle$$
$$= \sum_{l=1}^{n} \langle u_l|\rho(\sum_{k=1}^{n} |u_k\rangle \langle u_k|)A|u_l\rangle$$
$$= \sum_{l=1}^{n} \langle u_l|\rho A|u_l\rangle$$
$$= Tr(\rho A)$$

5.3 Time evolution

$$i\hbar\frac{d\rho}{dt} = [H,\rho]$$

For a closed system the time evolution of the density operator can also be written in terms of a unitary operator U

$$\rho(t) = U\rho(t_0)U^{\dagger}$$

A pure state will always be a pure state if the system is "isolated" or closed.

5.4 The density operator for a mixed state

For a state $|\psi_i\rangle$,denote the probability that a member of the ensemble has been prepared in the state $|\psi_i\rangle$ as p_i,then the density operator for the entire system is :

$$\rho = \sum_{i=1}^{n} p_i\rho_i = \sum_{i=1}^{n} p_i |\psi_i\rangle \langle\psi_i|$$

5.5 Probability of obtaining a given measurement result

The probability of obtaining a_n can be calculated using the density operator

$$p(a_n) = \langle u_n|\rho|u_n\rangle$$

5.6 Characterizing mixed states

The coherence is the capability of different components of a state to interfere with one another.

- A mixed state is a classical statistical mixture of two or more states.
  The state has no coherence.
  Therefore the off-diagonal terms of the density operator are zero.

- A pure state will have nonzero off-diagonal terms.

$Tr(\rho^2) = 1$ for a pure state .The same is not true in the case of mixed state.

- $Tr(\rho^2) < 1$ for a mixed state.

- $Tr(\rho^2) = 1$ for a pure state.

5.7   Completely mixed states

In a completely mixed state the probability for the system to be in each given state is identical.
In that case the density operator is a constant multiple of the identity matrix.
If the state space has n dimensions, then

$$\rho = \frac{1}{n}I$$

So for a completely mixed state we have

$$Tr(\rho^2) = Tr(\frac{1}{n^2}I) = \frac{1}{n^2}Tr(I) = \frac{1}{n}$$

5.8   Bloch representation

We can write any matrix as a linear combination of the sigma matrices.
Arbitrary density matrix :

$$\rho = \frac{a_0 + \vec{a}.\vec{\sigma}}{2}$$

With $\begin{cases} a_x = Tr(\sigma_x\rho) \\ a_y = Tr(\sigma_y\rho) \\ a_z = Tr(\sigma_z\rho) \end{cases}$
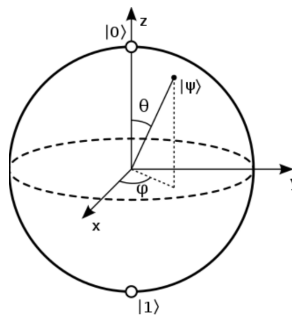
5.9   Partial Trace

Given bipartite system in a state ρ_{AB}
We can be interested in one of the two subsystems,we can then trace out the other one.
Reduced density matrix :

$$\rho_A = Tr_B(\rho_{AB}) = \langle 0_B|\rho_{AB}|0_B\rangle + \langle 1_B|\rho_{AB}|1_B\rangle$$

$$\rho_B = Tr_A(\rho_{AB}) = \langle 0_A|\rho_{AB}|0_A\rangle + \langle 1_A|\rho_{AB}|1_A\rangle$$

A reduced density matrix is that of a pure system if and only if the initial state is a pure and it is a product of states.

Chapter 6

QUANTUM MEASUREMENT THEORY

6.1   Distinguishing quantum states and measurement

An act of measurement disturbs a quantum system in a fundamental way.
The measurement of a quantum system involves some type of interaction or coupling of that system with a measuring device.
That device can be thought of as part of the larger environment which the quantum system is a part of.

If the system is initially described by some density operator ρ_0,then the state of the system at time t will be

$$\rho_t = U\rho_0 U^\dagger$$

The dynamics of a quantum system is trace-preserving $(Tr(\rho_0) = Tr(\rho_t))$.
While time evolution is trace-preserving, measurement is described by trace-decreasing quantum operations.
A quantum operation involving measurement, described by a measurement operator that we will denote by M_m, transforms a density operator ρ according to $\rho' = M_m\rho M_m{}^\dagger$.
In this case $Tr(\rho') \leq 1$

6.2   Projective Measurements

The idea of making a projective measurement is based on the following notion:

Given a set of mutually exclusive possible states, what state is the system is in?

6.2.1   Properties

- A projection operator P is Hermitian and equal to its own square

$$P = P^\dagger, P^2 = P$$

- P_1 and P_2 orthogonal if

$$P_1 P_2 \left|\psi\right\rangle = 0$$

- A complete set of orthogonal projection operators is one

$$\sum_i P_i = I$$

- The number of projection operators is determined by the dimension of the Hilbert space that describes the system.
  If the dimension of the Hilbert space is d and there are m projection operators

$$m \leq d$$

- If two projection operators commute, then their product is also a projection operator.

- The probability of finding the ith outcome when a measurement is made is

$$Pr(i) = |P_i \, |\psi\rangle \, |^2 = (P_i \, |\psi\rangle)^\dagger (P_i \, |\psi\rangle) = \langle\psi|P_i^2|\psi\rangle = \langle\psi|P_i|\psi\rangle$$

- The probability of obtaining measurement result a_i can be written as

$$Pr(i) = \langle\psi|P_i|\psi\rangle = Tr(P_i \, |\psi\rangle \, \langle\psi|)$$

6.2.2 Collapse of the wave function

while the state of the system prior to measurement could be a superposition of basis states after measurement the system collapses to the basis state that corresponds to the measurement result that was obtained.

$$|\psi'\rangle = \frac{P_i \, |\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}}$$

6.3 Generalized measurements

We denote a measurement operator by M_m, he probability that we find measurement result m is

$$Pr(m) \, \langle\psi|M_m{}^\dagger M_m|\psi\rangle$$

After a measurement the state of the system is

$$|\psi'\rangle = \frac{M_m \, |\psi\rangle}{\sqrt{\langle\psi|M_m{}^\dagger M_m|\psi\rangle}}$$

Measurements when a system is described by a density operator.
If a quantum system is described by a density operator ρ , the probability of finding measurement result m is

$$Pr(m) = Tr(M_m{}^\dagger M_m \rho)$$

If the measurement is described by a set of orthogonal projection operators $P_i = |u_i\rangle \, \langle u_i|$ corresponding to measurement result i then the probability of finding that measurement result is

$$Pr(i) = Tr(P_i{}^\dagger P_i \rho) = Tr(|u_i\rangle \, \langle u_i| \, \rho) = \langle u_i|\rho|u_i\rangle$$

6.4 Positive operator-valued measures

Known as POVM, A POVM consists of a set of positive operators commonly denoted by E_m.
The probability of obtaining measurement result m in this case is given by

$$Pr(m) = \langle\psi|E_m|\psi\rangle$$

The POVM allows us to construct a more general type of measurement operator to describe measurements where projective measurements do not apply in the real world.
A POVM allows us to describe measurements on the system without regard to the post measurement state.

Chapter 7

ENTANGLEMENT

One of the most unusual and fascinating aspects of quantum mechanics is the fact that particles or systems can become entangled.

For the simplest two quantum systems case we denote the systems A and B.

If these systems are entangled, this means that the values of certain properties of system A are correlated with the values that those properties will assume for system B.

When a system is entangled, this means that the individual component systems are really linked together as a single entity.

Any measurement that measures a part of the system is really a measurement on the entire system.

If two systems are entangled, the description of each system has to be made with reference to the state of the other system, even if the component systems are spatially separated and non interacting.

7.1 BELL STATE

They are known as the four maximally entangled two-qubit Bell states and they form a maximally entangled basis

- $|\beta_{00}\rangle = \dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$

- $|\beta_{01}\rangle = \dfrac{|01\rangle + |10\rangle}{\sqrt{2}}$

- $|\beta_{10}\rangle = \dfrac{|00\rangle - |11\rangle}{\sqrt{2}}$

- $|\beta_{11}\rangle = \dfrac{|01\rangle - |10\rangle}{\sqrt{2}}$

7.2 When is a state entangled

Not all states $|\psi\rangle \in H_A \otimes H_B$ are entangled.

When two systems are entangled, the state of each composite system can only be described with reference to the other state.

If two states are not entangled, we say that they are a product state or separable.

If $|\psi\rangle \in H_A$ and $|\phi\rangle \in H_B$ and $|\xi\rangle = |\psi\rangle \otimes |\phi\rangle$, then $|\xi\rangle$ is a product state

7.3 Entanglement fidelity

Consider a density operator for a single qubit that is diagonal with respect to the computational basis

$$\rho = f \left|0\right\rangle \left\langle 0\right| + (1 - f) \left|1\right\rangle \left\langle 1\right|$$

The parameter f is known as the entanglement fidelity.

Chapter 8

Quantum noise and error correction

In the treatment of quantum theory we've used so far we have been looking at closed systems.
These are quantum systems that do not interact with the outside world.That is, an idealized model.
In reality, quantum systems interact with the outside environment.
The problem if that interactions with the environment can introduce noise and cause errors.

We are going to have to develop a mathematical formalism to describe quantum systems that interact with the environment.
We refer to systems of this type as open systems.

8.1 Single-Qubit errors

The ability to work with superposition states is what gives quantum computers their power.
When a quantum system interacts with the environment superposition can be lost,we call this process decoherence.
Quantum noise acts on qubits via the application of one of the operators I, X, Y, Z.

8.1.1 Bit flip errors

We have $|0\rangle \rightarrow |1\rangle$ and $|1\rangle \rightarrow |0\rangle$
This type of error is described by the X operator.

8.1.2 Phase flip errors

We have $|x\rangle \rightarrow (-1)^x |x\rangle$
This type of error is described by the Z operator.

The Y operators is related to a phase flip followed by a bit flip

8.2 Quantum operations and Krauss operators

The system density operator ρ.
$\Phi(\rho)$ is a quantum operation,it is a mapping that describes the evolution of the system.
The new system density operator ρ'

$$\Phi(\rho) = \rho'$$

Unitary evolution : $\Phi(\rho) = U\rho U^*$
Measurement : $\Phi(\rho) = M_m \rho M_m^*$

If we have a set of operators A_k that aren't necessarily unitary:

$$\Phi(\rho) = \sum_{k=1}^{n} A_k \rho A_k^*$$

The A_k, which are known as operation elements, cas satisfy a completeness relation

$$\sum_{k=1}^{n} A_k A_k^* = I$$

To Calculate A_k we define :

- ρ is the density operator for the system.

- We denote the basis states of the environment by $|e_k\rangle$.

- $|e_0\rangle$ is the environment state

- σ is the density operator for the environment.

$$A_k = \langle e_k | U | e_0 \rangle$$

8.3 Some channels

8.3.1 Depolarization channel

Quantum noise is often described in terms of channels.
The depolarization channel is known as when p is a probability that the principal system evolves into a completely mixed state.
and $(1-p)$ is the probability that the system stays the same.

$$\Phi(\rho) = (1-p)\rho + p\frac{1}{2}I$$

8.3.2 Bit flip and phase flip channel

There is a probability p that nothing happens to the qubit, While there is a probability $(1-p)$ that there is a bit flip error.
$$\Phi(\rho) = p\rho + (1-p)X\rho X$$

There is a probability p that nothing happens to the qubit, while there is a probability $(1-p)$ that there is a phase flip error.
$$\Phi(\rho) = p\rho + (1-p)Z\rho Z$$

8.4 Amplitude damping

Real physical systems lose energy. When describing a quantum system undergoing energy dissipation because of some type of interaction with the environment, we apply a quantum operation known as amplitude damping.

8.5   Phase damping

Phase damping is a quantum process that involves information loss, but unlike amplitude damping, it does not involve energy loss. Specifically phase damping involves the loss of information about relative phases in a quantum state.

Chapter 9

TOOLS OF QIT

9.1 The no-Cloning theorem

The remarkable power of a quantum computer comes from the fact a qubit can exist in a superposition.
Given this fact, can we make an exact copy of an arbitrary qubit?
It turns out the answer is no
Proof :
Consider two pure states $|\psi\rangle$ and $|\phi\rangle$, and suppose that there exists a unitary operator U such that

$$U(|\psi\rangle \otimes |\xi\rangle) = |\psi\rangle \otimes |\psi\rangle$$

$$U(|\phi\rangle \otimes |\xi\rangle) = |\phi\rangle \otimes |\phi\rangle$$

We take the inner product of the left hand side

$$(\langle\psi| \otimes \langle\xi| \, |U^\dagger)(U \, |\phi\rangle \otimes |\xi\rangle) = \langle\psi|\phi\rangle \langle\xi|\xi\rangle = \langle\psi|\phi\rangle$$

We take the inner product of the right hand side

$$(\langle\psi| \otimes \langle\psi|)(|\phi\rangle \otimes |\phi\rangle) = \langle\psi|\phi\rangle^2$$

Then we get the equation

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2$$

The equation is true if $\langle\psi|\phi\rangle = 0$ in which case the states are orthogonal, or if $|\phi\rangle = |\psi\rangle$.

> Thats mean that there is no unitary operator U can be used to clone arbitrary quantum states

9.2 Trace Distance

The trace distance can be used to determine how similar two states are.
Let ρ and σ be two density matrices. The trace distance $\delta(\rho, \sigma)$ is defined to be

$$\delta(\rho, \sigma) = \frac{1}{2} Tr|\rho - \sigma|$$

The trace distance acts like a metric on the Hilbert space.
The trace distance is nonnegative

$$0 \leq \delta(\rho, \sigma)$$

The trace distance is symmetric :

$$\delta(\rho, \sigma) = \delta(\sigma, \rho)$$

The trace distance satisfies the triangle inequality

$$\delta(\rho, \sigma) \leq \delta(\rho, \vartheta) + \delta(\vartheta, \sigma)$$

If $\rho = |\psi\rangle \langle\psi|$ is a pure state, then $\delta(\rho, \sigma)$ is given by

$$\delta(\rho, \sigma) = \sqrt{1 - \langle\psi|\sigma|\psi\rangle}$$

If $[\rho, \sigma] = 0$, and they are both diagonal with respect to some basis $\{|u_i\rangle\}$ such that the eigenvalues of ρ are r_i and the eigenvalues of σ are s_i then

$$\delta\rho, \sigma = \frac{1}{2}Tr|\sigma_i(r_i - s_i)|u_i\rangle \langle u_i||$$

9.3   Fidelity

The Fidelity can be used to determine how close one state is to another.
Let ρ and σ be two density operators.

$$F(\rho, \sigma) = Tr(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})$$

If $\rho = |\psi\rangle \langle\psi|$ and $\sigma = |\phi\rangle \langle\phi|$, and $|\psi\rangle$ and $|\phi\rangle$ are two pure state,Then

$$F(\rho, \sigma) = |\langle\phi|\psi\rangle|$$

Fidelity is a number that ranges between 0 and 1 .
The fidelity of two pure states is symmetric.
The fidelity is invariant under unitary operations:

$$F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma)$$

Suppose that $\rho = \sum_i r_i |u_i\rangle \langle u_i|$ and $\sigma = \sum_i s_i |u_i\rangle \langle u_i|$, Then

$$F(\rho, \sigma) = \sum_i \sqrt{r_i s_i}$$

9.4   Entanglement of formation and concurrence

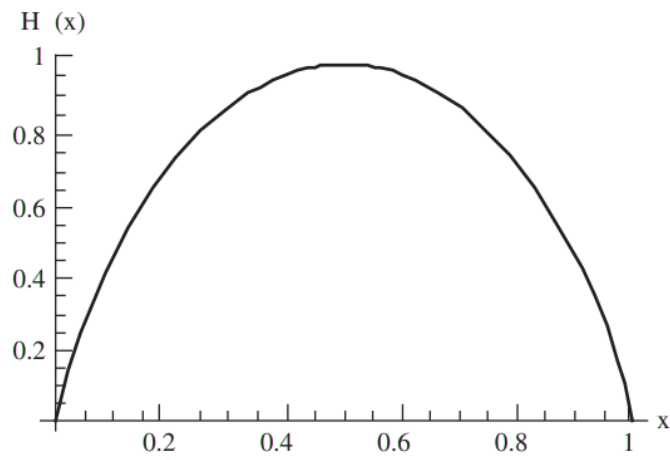The concurrence is just the amount of overlap between a state $|\psi\rangle$ and a state $|\psi\rangle$

$$C(\psi) = |\langle\psi|\tilde{\psi}\rangle|$$

9.5   Information content and entropy

Entropy is a way to quantify the information content in a signal.
The Shannon entropy H is given by

$$H_2(x) = -x \log(x) - (1 - x) \log(1 - x)$$

If we are completely uncertain then $H(x) = 1$

The general rule is that the larger the entropy, the more ignorance you have about the outcome.

The entropy of a quantum state with density operator is given by

$$S(\rho) = -Tr(\rho \log_2(\rho))$$

Chapter 10

QUANTUM GATES

In a classical computer, at the most fundamental level there are two basic tasks that we can use when manipulating information.
We can move it from one place to another, or we can do some type of basic processing on the information using a logic gate.
Sets of logic gates can be connected together to construct digital circuits.

10.1   Classical Logic Gates

The basic purpose of a logic gate is to manipulate or process information at the bit level in some way.

10.1.1   NOT gate

INPUT	OUTPUT
0	1
1	0

10.1.2   OR gate

A	B	A OR B
0	0	0
0	1	1
1	0	1
1	1	1

10.1.3   AND gate

A	B	A AND B
0	0	0
0	1	0
1	0	0
1	1	1

10.1.4 XOR gate

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

10.1.5 NAND gate

A	B	A NAND B
0	0	1
0	1	1
1	0	1
1	1	0

This gate has the interesting property of being universal. That is, all computing operations can be completed using only NAND gates.
In fact you can construct an entire computer using nothing but NAND gates.
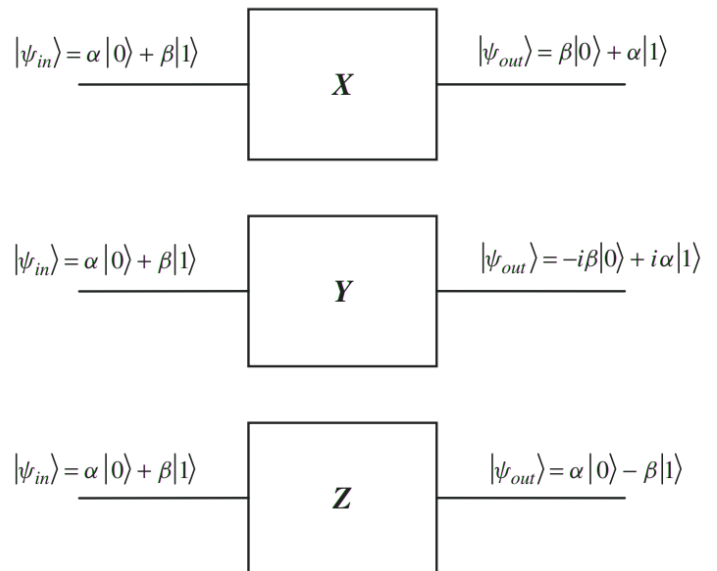
10.2 Single-qubit gates

A gate can be thought of as an abstraction that represents information processing.
In a quantum computer the "gates" are unitary operations.

10.2.1 Pauli operators

- X-GATE it is a NOT-GATE : $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

- Y-GATE it is a bit flip: $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

- Z-GATE it is a phase shift: $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$|\psi_{in}\rangle = \alpha|0\rangle + \beta|1\rangle$ $\quad$ **X** $\quad$ $|\psi_{out}\rangle = \beta|0\rangle + \alpha|1\rangle$

$|\psi_{in}\rangle = \alpha|0\rangle + \beta|1\rangle$ $\quad$ **Y** $\quad$ $|\psi_{out}\rangle = -i\beta|0\rangle + i\alpha|1\rangle$

$|\psi_{in}\rangle = \alpha|0\rangle + \beta|1\rangle$ $\quad$ **Z** $\quad$ $|\psi_{out}\rangle = \alpha|0\rangle - \beta|1\rangle$

10.2.2 Other operators

- H-Gate (Hadamard Gate) :
  The Hadamard gates are used to create superposition states.
  $$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{cases} H|0\rangle = |+\rangle \\ H|1\rangle = |-\rangle \end{cases} \text{, with } |\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$
  Two Hadamard gates in serries act to reverse the operation and give back the original input.

- P-Phase it is a phase shift : $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \begin{cases} P\,|0\rangle = |0\rangle \\ P\,|1\rangle = e^{i\theta}\,|1\rangle \end{cases}$

10.3 The Z-Y decomposition

We can use arbitrary unitary gate with simple geometrical interpretation in the Bloch sphere

$$U = e^{i\alpha} R_y(...) R_z(...) R_y(...)$$

R_y : rotation around the y axis. R_z : rotation around the z axis.
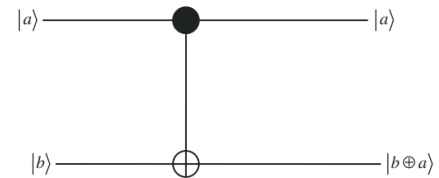
10.4 Two-qubit gates

We include a control bit C.
If C = 0, then the gate does nothing, but if C = 1, then the gate performs some specified action.

10.4.1 The controlled NOT or CNOT gate.

If the control qubit is $|0\rangle$, then nothing happens to the target qubit.
If the control qubit is $|1\rangle$, then the NOT or X matrix is applied to the target qubit.

$$CNOT = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$
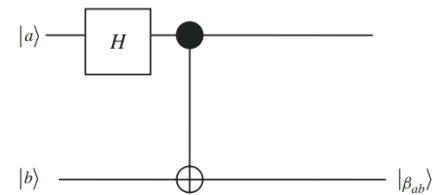

10.4.2 The controlled-Hadamard or CH gate.

If the control qubit is $|0\rangle$, then nothing happens to the target qubit.
If the control qubit is $|1\rangle$, then we apply a Hadamard gate to the target qubit.

$$CNOT = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \dfrac{1}{\sqrt{2}} & \dfrac{1}{\sqrt{2}} \\ 0 & 0 & \dfrac{1}{\sqrt{2}} & \dfrac{-1}{\sqrt{2}} \end{pmatrix}$$

10.5 Gate decomposition

A large part of working with quantum circuits is decomposing an arbitrary controlled unitary operation U into a series of single-qubit operations and controlled NOT gates.
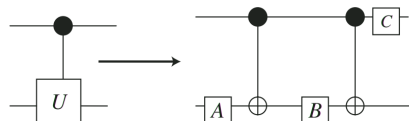
Chapter 11

QUANTUM ALGORITHMS

An algorithm is a set of instructions used to perform some well-defined task on a computer.
The nature of quantum systems—captured in superposition and interference of qubits—often allows a quantum system to compute in a parallel way that is not possible even, in principle, with a classical computer. However, since measurement finds a qubit in one state or the other— frustratingly we find that if we give a quantum computer n inputs we only get n outputs.

11.1 Matrix representation of serial and parallel operations

The matrix representation of this sequence of operations is written down by multiplying the matrices in reverse order.

$$ZHP(\theta)$$
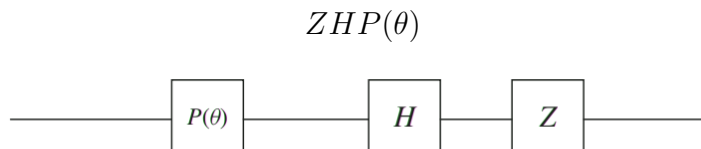
When quantum operations are performed in parallel,we compute the tensor product.

11.2 Quantum Interference

The application of a Hadamard gate to an arbitrary qubit is an example of quantum interference.
There are two types of interference, positive interference in which probability amplitudes add constructively to increase or negative interference in which probability amplitudes add destructively to decrease.
Quantum interference allows us to gain information about a function f (x) that depends on evaluating the function at many values of x.
Interference allows us to deduce certain global properties of the function.

11.3 Deutsch's algorithm

consider a very simple function, one that accepts a single bit as input and produces a single bit as output. For example we could have :

- The identity function
$$f(x) = \begin{cases} 0 \text{ if } x = 0 \\ 1 \text{ if } x = 1 \end{cases}$$

- constant functions
  $f(x) = 0, f(x) = 1$

- Bit flip function
  $$f(x) = \begin{cases} 1 \text{ if } x = 0 \\ 0 \text{ if } x = 1 \end{cases}$$

The identity and bit flip functions are called balanced because the outputs are opposite for half the inputs.

Deutsch's algorithm will let us put together a state that has all of the output values of the function associated with each input value in a superposition state.
Then we will use quantum interference to find out if the given function is constant or balanced.

Deutsch's algorithm is implemented by the following steps:

- Apply Hadamard gates to the input state $|0\rangle |1\rangle$ to produce a product state of two superpositions.

- Apply U_f to that product state where U_f is a unitary operation that acts on two qubits.
  It leaves the first qubit alone and produces the exclusive or (denoted by $\otimes$) of the second qubit with the function f evaluated with the first qubit as argument.

$$U_f |x, y\rangle = |x, y \otimes f(x)\rangle$$

$$U_f \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) |0\rangle = \frac{1}{\sqrt{2}} (U_f |00\rangle + U_f |01\rangle) = \frac{|0, 0 \otimes f(0)\rangle + |1, 0 \otimes f(1)\rangle}{\sqrt{2}}$$

- Apply a Hadamard gate to the first qubit leaving the second qubit alone.