Personal Notes on

Quantum Information

Jeffrey Ming Han Li

jeffreyli2288@Outlook.com

Abstract

This lecture notes are based on PHY365 Quantum information, Instructed by Professor Daniel James, also cross-referenced with Nielson & Chuang: Quantum Computation and Quantum Information.

Contents

1 Introduction

1.1 Quantum States

Quantum computer is built out of qubits that are either 0 or 1 state

Example 1: For a system of 4 qubits, here are some possible configurations.

$$|0\rangle_4, |0\rangle_3, |0\rangle_2, |0\rangle_1 = |0000\rangle$$
$$|0\rangle, |0\rangle, |0\rangle, |1\rangle = |0001\rangle$$
$$....$$

A generalized term is

$$|\psi\rangle = \bigotimes_{p=1}^{N} |x_p\rangle$$

- Any quantum state can be defined by
$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$
where the probability is normalized such that $\alpha^2 + \beta^2 = 1$. In matrix form, we can write in the $|0\rangle, |1\rangle$ basis.

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad \langle\psi| = (\alpha^*, \beta^*), \text{and } \langle\psi|\psi\rangle = 1$$

1.2 Quantum Operators

The operators are linear such that

$$\alpha' = U_{00}\alpha + U_{01}\beta$$
$$\beta' = U_{10}\alpha + U_{11}\beta$$

and

$$\hat{U} = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix}, \quad |\psi'\rangle = \hat{U}|\psi\rangle, \langle\psi'| = \langle\psi|\hat{U}^\dagger$$

The operators, to ensure the quantum state remained normalized, must be **Unitary** such that

$$\hat{U}^\dagger \hat{U} = \hat{I}$$

and the format of a quantum operator must also follow

$$\hat{U} = \begin{pmatrix} a & b \\ -b^* & a* \end{pmatrix}$$

Some common quantum operators include:

- Bit Flip(X gate): Flit the value from 0 to 1 and vice versa
$$\hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \hat{X}^\dagger$$

- Phase Flip(Z gate): Apply a phase shift to the $|1\rangle$ state
$$\hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Spin Half(Y gate):
$$\hat{Y} = \hat{Z}\hat{X} = i\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

- Hadamad Gate(H gate): A gate that is used to expand a single state into all possible states of the qubit

$$\hat{H} = \frac{1}{\sqrt{2}}(\hat{X} + \hat{Z}) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

such that

$$\hat{H}\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$\hat{H}\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

for N qubits, the transformation is

$$H^{\otimes N}\,|0\rangle = \sum_{x=0}^{2N-1} \frac{1}{\sqrt{2^N}}\,|x\rangle$$

where x stands for the decimal numbers that will be represented as binary numbers.

1.3 Quantum Measurement

Measuring the qubit destroys the randomness and left a definite state. Suppose we have two qubits in the system, measuring the first qubit as $|0\rangle$ would keep the states where the first qubit is$|0\rangle$

$$|\psi\rangle \to \frac{\hat{\Pi}_0\,|\psi\rangle}{\sqrt{P(0)}}$$

the non-unitary operator is called the projector operator, which is equivalent to the outer product of the states

$$\hat{\Pi}_0 = |0 \otimes 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix}$$

1.4 Two Qubit System

Applying a Unitary operator to qubit 1 only in a two qubit system is equivalent to

$$|\psi'\rangle = (\hat{U} \otimes \hat{I})\,|\psi\rangle$$

and two qubit state is expressed as

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$$

- **Concurrence**: it is a measurement of how entangled two qubits are, defined by

$$\boxed{C = 2|\alpha\delta - \beta\gamma|}$$

C = 1 means maximally entangled state.

1.5 Schmidt Decomposition

Definition: Let H_1 and H_2 be Hilbert spaces of dimensions n and m. Assume $n \geq m$. For any vector ω in the tensor product $H_1 \otimes H_2$, there exist orthonormal sets $\{u_1, ..., u_m\} \subset H_1, \{v_1, ..., v_n\} \subset H_2$. such that

$$\omega = \sum_{i=1}^{m} \lambda_i u_i \otimes v_i$$

where

$$\sum \lambda_i^2 = 1$$

[1]

In the context so far we can understand as any state $|\psi\rangle$ can be written as

$$\boxed{|\psi\rangle = \hat{U}_A \otimes \hat{U}_B(\lambda_0 |00\rangle + \lambda_1 |11\rangle)}$$

U_A and U_B are transforming the basis from $|0\rangle \, and \, |1\rangle$ into $|u_i\rangle \, and \, |v_i\rangle$.

Consider the unitary operators

$$\hat{U}_A = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix} \quad \text{and} \quad \hat{U}_B = \begin{pmatrix} c & d \\ -d^* & c^* \end{pmatrix}.$$

Therefore,

$$|\Psi\rangle = \lambda_0(a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) + \lambda_1(-b^*|0\rangle + a^*|1\rangle)(-d^*|0\rangle + c^*|1\rangle),$$
$$= (\lambda_0 ac + \lambda_1 b^* d^*)|00\rangle + (\lambda_0 ad - \lambda_1 b^* c^*)|01\rangle + (\lambda_0 bc - \lambda_1 a^* d^*)|10\rangle + (\lambda_0 bd + \lambda_1 a^* c^*)|11\rangle.$$

This looks very messy, but we can compute the concurrence (and after a length but straightforward computations), we get

$$\boxed{C = 2\lambda_0\lambda_1}$$

Using $\lambda_0^2 + \lambda_1^2 = 1$, we can obtain the quadratic equation

$$\lambda^4 - \lambda^2 + (C/2)^2 = 0,$$

so λ_0, λ_1 are determined by C. The maximum value of C is $C_{\max} = 1$, which occurs at $\lambda_{\text{crit}} = \dfrac{1}{\sqrt{2}}$

1.6 Control Gate

Control gate is a source of entanglement where the action on one qubit is controlled by the other qubit. Typically, it is defined such that only when the control qubit is $|1\rangle$ there will be an action on the target qubit.

$$|0\rangle \, 1$$
$$|0\rangle \, X$$

This is an example of CNOT(Control-X gate). The matrix format is

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

where the bottom right 2x2 matrix correspond to the cases when the first qubit is $|1\rangle$.

1.7 Example: Quantum Teleportation

Suppose you have a qubit in some unknown state

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

and you want to transport this state to another qubit also with an unknown state. Therefore, in 1993 Bennett, Brassard, Crepeau, Josza, Peres, and Wootlers invented a protocol that can get this working with an intermediate qubit.

Unknown Qubit:

$\alpha \, |0\rangle + \beta \, |1\rangle$ 1 H c [vertical wire=c]2
Alice:$|0\rangle$ H 1 X c [vertical wire=c]1
Bob:$|0\rangle$ X X Z $|\psi_{\text{out}}\rangle$

mathematically we have that

$$\hat{I} \otimes \hat{H} \otimes \hat{I} \, |\psi\rangle \, |0\rangle \, |0\rangle = \frac{1}{\sqrt{2}} \, |\psi\rangle \, (|0\rangle + |1\rangle) \, |0\rangle$$

further taking a CNOT gate we have that

$$CNOT(|\psi_1\rangle) = |\psi_2\rangle = \frac{1}{\sqrt{2}}(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|100\rangle + \beta\,|111\rangle)$$

taking a Cnot to this state we also have

$$CNOT(\psi_2) = \frac{1}{\sqrt{2}}(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|110\rangle + \beta\,|101\rangle)$$

now we can have $|\psi_3\rangle$ after another hadamard gate at Qubit A

$$|\psi_3\rangle = \frac{1}{2}(|00\rangle\,|\psi_{in}\rangle + |01\rangle\,\hat{X}\,|\psi_{in}\rangle + |10\rangle\,\hat{Z}\,|\psi_{in}\rangle + |11\rangle\,\hat{X}\hat{Z}\,|\psi_{in}\rangle)$$

so now, based on the measured value of qubit 1 and 2 we are able to reconstruct the state at qubit 3. The X, Z gate on qubit 3 allows us to restore the state back into $|\psi_{in}\rangle$. Basically Alice can classically communicate with bob and informs him about the state measured, then Bob can do some transformation to his qubit to reconstruct the original unknown qubit state.

2 Algorithms

Quantum algorithms can do something similar to a classical computer, for instance communicating information from places to places(not quite in quantum teleportation case), so here we will go through some examples and some theories of how it is actually achieved.

2.1 Basic of Quantum computation

The main reasons that quantum computer can't construct a classical circuit, is because most of the quantum gates are *reversible* whereas it is not the case for most classical computers. However **Toffoli Gate** can make any classical circuit.

$$a2ab1bc$$

c $\oplus ab$

which can be used to simulate **NAND** gate by making $c = |1\rangle$

2.2 Quantum parallelism

suppose we have a function $f(x)$, quantum parallelism allows users to evaluate for many x simultaneously. Where any transformation is defined as

$$|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$$

, the first qubit is called the data register, and the second register is the target register.

$|0\rangle + |1\rangle \frac{}{\sqrt{2}}$ [2]U_f
$|0\rangle$

based on the schemetic above, the output state is

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

which carries information for both states of the function f(x). This procedure can be generalized by **Hadamard Transform**, which is just n Hadamard gates acting on n qubits(registers) simultaneously, namely $H^{\otimes n}$. The result of transformation on n qubit with initially all state $|0\rangle$ is

$$\frac{1}{\sqrt{2^n}} \sum_{x}^{2^N-1} |x\rangle$$

A more general Hadamard Transform of state $|x\rangle$ reads:

$$\frac{1}{\sqrt{2^n}} \sum_{y}^{2^N-1} (-1)^{xy} |y\rangle$$

suppose we have another qubit(the target register). Application of hadamard transform to the first n qubits will result in a final state of

$$\frac{1}{\sqrt{2^n}} \sum_{x}^{2^N-1} |x\rangle |f(x)\rangle$$

2.3 Deutsch's Algorithm

Lets say there is a function f(x) where it maps an input into binary output

$$\{0,1\} \to \{0,1\}$$

if the output f(0) = f(1), then it is constant, otherwise, balanced. The goal of this algorithm is to find whether the function is constant or balanced.

$|0\rangle$ H [2]U$_f$ H
$|1\rangle$ H

- $$|\psi_0\rangle = |01\rangle$$
- $$|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$
- $$|\psi_2\rangle = \begin{cases} \pm \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1) \end{cases}$$
- The final H gate on qubit 1 gives us

$$|\psi_3\rangle = \begin{cases} \pm |0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm |1\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1) \end{cases}$$

2.4 Deutsch-Jozsa Algorithm

A more general form of the Deutsch Algorithm is the Deutsch-Jozsa Algorithm for n arbitrary number of qubits. Similarly, it is to determine if a function f(x) is *constant* for all values of x or else f(x) is *balanced*, that is, equal to 1 for half of all the possible $x \in \{0, 2^n + 1\}$.

- Classically, an inquiry of $2^n/2 + 1$ times is needed to find whether it is balanced or constant. Whereas can be done at once by quantum communication.

$|0\rangle$ n H$^{\otimes n}$ [2]U_f $H^{\otimes n}$
$|1\rangle$ H

- $$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$$
- $$|\psi_1\rangle = \sum_x \frac{1}{\sqrt{2^n}} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$
- Next the function is evaluated $U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$ giving

$$|\psi_2\rangle = \sum_x \frac{1}{\sqrt{2^n}} (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

- Performing a Hadamard Transform to the upper n qubit for each state $|x\rangle$ yields:

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_z (-1)^{x\cdot z}|z\rangle,$$

which allows us to evaluate the combination of states for all the possible $|x\rangle$ state

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}}{2^n}|z\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right].$$

Noted that the amplitude of $|0\rangle^{\otimes n}$ is $\sum_x (-1)^{f(x)}/2^n$, meaning that if f(x) is constant the amplitude of $|0\rangle$ is either 1 or -1. Indicating if Alice measures $|0\rangle^{\otimes n}$ the function must be constant and otherwise, balanced.

2.5 Quantum Fourier Transform

For a discrete classical Fourier Transform, the function takes in a vector x of length N and outputs the transformed data,

$$y_k = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} x_j e^{2\pi jk/N}$$

Quantum Fourier transform is the same for an orthonormal basis$|0\rangle .... |N-1\rangle$

$$|j\rangle \to \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle.$$

Therefore, an arbitrary state may be written as

$$\sum_{j=0}^{N-1} x_j|j\rangle \to \sum_{k=0}^{N-1} y_k|k\rangle,$$

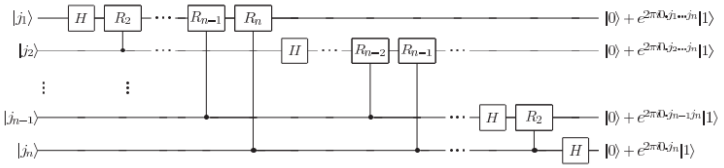
the product form of the fourier transform goes to

$$|j\rangle \to \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_1 j_2\cdots j_n}|1\rangle\right)}{2^{n/2}}$$

A unitary operator R can be used to achieve this

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$$

applying hadamard gate to circuit one gives



$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i 0.j_1}|1\rangle\right)|j_2\cdots j_n\rangle,$$

after transforming by R, we obtain

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle\right)|j_2\cdots j_n\rangle,$$

Doing this repetitively for all qubit we can obtain

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2\ldots j_n}|1\rangle\right)|j_2\cdots j_n\rangle,$$

which can then be transformed by Hadamard gate to the form

$$\frac{1}{2^{2/2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right)(|0\rangle + e^{2\pi 0.j_2}|1\rangle)|j_3 \cdots j_n\rangle,$$

which can be done repetitively to obtain the expression for the Fourier transform above. However the SWAP operation is omitted for clarity, but switching the state of the qubits give the final state as the equation denoted above.

2.5.1 Period Finding

One application of Quantum fourier transform is to find the period of a function. Suppose f is a periodic function f(x+r) = f(x) for some unknown $0 < r < 2^L$

$|0\rangle$ $\mathrm{H}^{\otimes n}[wires = 2]U_f U_{\mathrm{QFT}}$y
$|0\rangle$ $f(x_0)$

Right after the U_f gate the combined state is

- $$|\Psi_2\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\,|f(x)\rangle.$$

- Then we perform a measurement to the function register we can the state, $|f(x_0)\rangle$, and the argument register also collapse to the form where $x = x_0 + kr$ and $m = \dfrac{2^l}{r}$ = number of periods, and $2^n = mr + x_0$.

$$\begin{aligned}
|\Psi_2\rangle &= \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\,|f(x)\rangle \\
&= \frac{1}{\sqrt{2^n}}\big(|0\rangle\,|f(0)\rangle + |1\rangle\,|f(1)\rangle + \cdots + |r-1\rangle\,|f(r-1)\rangle \\
&\qquad + |r\rangle\,|f(0)\rangle + |r+1\rangle\,|f(1)\rangle + \cdots + |2^n-1\rangle\,|f(x)\rangle\big) \\
&= \frac{1}{\sqrt{2^n}}\sum_{k=0}^{m(x_0)-1}\big(|kr\rangle\,|f(0)\rangle + |kr+1\rangle\,|f(1)\rangle + \cdots + |kr+(r-1)\rangle\,|f(r-1)\rangle\big).
\end{aligned}$$

  Therefore, the only states left in the first register are

$$|\chi(x_0)\rangle = \frac{1}{\sqrt{m(x_0)}}\sum_{k=0}^{m(x_0)-1}|x_0 + kr\rangle$$

- Applying Quantum Fourier Transform to the first qubit only

$$|\psi_3\rangle = U_{QFT}\,|\chi(x_0)\rangle \otimes |f(x_0)\rangle$$

  and

$$U_{\mathrm{QFT}}\,|\chi(x_0)\rangle = \frac{1}{\sqrt{m}}\sum_{k=0}^{m-1}U_{\mathrm{QFT}}\,|x_0 + k\,r\rangle = \frac{1}{\sqrt{m}}\sum_{k=0}^{m-1}\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}e^{\frac{2\pi i\,(x_0+k\,r)\,y}{2^n}}\,|y\rangle$$

$$= \frac{1}{\sqrt{2^n\,m}}\sum_{y=0}^{2^n-1}\Big(e^{\frac{2\pi i\,x_0\,y}{2^n}}\underbrace{\sum_{k=0}^{m-1}e^{\frac{2\pi i\,k\,r\,y}{2^n}}}_{\gamma(y)}\Big)\,|y\rangle\ .$$

The inner sum

$$\gamma(y) = \sum_{k=0}^{m-1} e^{2\pi i\, k\,(r\,y/2^n)}$$

is a geometric series. For large m it exhibits sharp peaks when

$$\exp\!\big(2\pi i\, r\, y/2^n\big) = 1,$$

i.e. whenever y is (approximately) a multiple of $2^n/r$. One finds

$$\gamma(y) \;\approx\; \begin{cases} m, & y \approx 0,\ 2^n/r,\ 2\cdot 2^n/r,\ \ldots, \\ 0, & \text{otherwise.} \end{cases}$$

Hence $U_{\mathrm{QFT}}\,|\chi(x_0)\rangle$ becomes (up to normalization) a superposition of basis states $|y\rangle$ with $y \approx p\,2^n/r$, exposing the hidden period r.

2.5.2 Public Key Cryptography and RSA Cryptosystem

By public key, it means a channel for anyone to transmit information in, but only a particular party can receive the information through a *secret Key*. This mean that any cryptosystem must have at least 2 keys: *public key* and *secret key*. The most widely used system is the RSA cryptosystem, it follows the following procedures to create the public key and the secret key.

1. Select two large prime numbers, p and q
2. Compute the product n = pq
3. Select at random a small odd integer, e, that is relatively prime to

$$\varphi(n) = (p-1)(q-1)$$

4. Compute

$$d = e^{-1} \mod \varphi(n)$$

5. The RSA *public key* is the pair P = (e,n). The RSA secret key is the pair S = (d,n)

When encrypting the information, suppose Bob has a message M has only [log n] bits, the encrypted version of the message M is

$$E(M) = M^e (\text{mod } n)$$

When decrypting the message, simply raise the encrypted message to the dth power

$$E(M) \to D(E(M)) = E(M)^d (\text{mod n}) = M (\text{mod n})$$

By Fermat's Little theorem, which makes two scenarios,

- When M is not co-prime to n:
  such that one or both of p and q divide M, lets consider p divides M.

  $$M = 0 (\text{mod p})$$

  where

  $$M^{ed} = M (\text{mod n})$$

  which provides the message to ed-th power.

However, there are two issues for RSA to be implemented.

1. The generation of public and private keys(or the p and q prime numbers). Requiring $O(L^4)$ operations through the Miller-Rabin test of Primality, and the prime number theorem.
2. Efficiency of the encryption and decryption transformations. These are modular exponentiation which is done using $O(L^3)$ operations.

Therefore, these efficiency limits the complexity ofthe keys leaving to potential breaking of RSA, there are two methods RSA be broken.

1. Order-finding:
   Suppose Eve receives a message M^e(mod n). She can find the order of the message by the smallest integer r such that $(M^e)^r$(mod n). Even if M^e is not co-prime to n, an Euclid's Algorithm can be used to find this power. Then since r divides $\varphi(n)$, and since e is co-prime to $\varphi(n)$, it must also be co-prime to r, so $ed' = 1 + kr$ for some integer k, obtained from the equation $ed = 1 + \varphi(n)k$.
   Then Eve can recover the original message M by raising the message to the d'th power

$$\begin{aligned} \left(M^e\right)^{d'} \bmod n &= M^{1+k\,r} \bmod n \\ &= M \cdot M^{k\,r} \bmod n \\ &= M \bmod n. \end{aligned}$$

2. Factor Method: If Eve could factor n = pq, extracting possible values for p and q, then she can find the encrypted message easily.

3 Quantum Computer Realization

So how do we build an actual quantum computer. There are 5 criteria that quantum computer must follows so called **Divincento Criteria**

1. A lot of Qubits(Scalable) must be used around $10^5 - 10^7$ qubits must be used to do useful computation.
2. Initiating the Qubits to $|0\rangle^{\otimes n}$.
3. Reliable Qubits with long coherence time.
4. Must be able to perform gate operations: Unitary gates + CNOT gates
5. Must be able to measure individual qubit

There are a few types of quantum computers

- Two level & Multi level Systems Quantum Computers: Something like electron spins, nucleus spins, or magnetic field (2level). Also atoms or ions used for multi level systems.
- Fabricated Qubits: Somehting like superconducting circuits(LCR and Capacitor at low temperature), Quantum dots(Artificial atoms in semiconductors; trap single electrons or holes using Cryogenic cooling and precise nanofabrication), Topological Anyons(Quasiparticles in 2D, theoretically immune to local noise)
- Photonic Qubits: Photons at optical or microwave frequencies, Naturally quantum but weak interactions make two-qubit gates difficult. Excellent for communication and interfacing distant nodes. It operate at the single-photon level. It can be nonlinear crystals, linear-optics interferometry, and the main challenge is photonic interaction.

3.1 Two-level Single Qubit Hamiltonian

Use two energy levels as the states: $|0\rangle, |1\rangle$ with energies E_0, E_1. However, by the boltzmann ratio

$$\frac{p_1}{p_0} = \exp\left(-\frac{\Delta E}{k_B T}\right)$$

In order to cool a qubit to a definite $|0\rangle$ state, $\Delta E \gg k_B T$. By definition, for the orthogonal basis, $|0\rangle, |1\rangle$, the Hamiltonian is written as

$$\hat{H} = \begin{pmatrix} E_0 & 0 \\ 0 & E_1 \end{pmatrix} = \left(\frac{E_0 + E_1}{2}\right)\hat{I} + \left(\frac{E_0 - E_1}{2}\right)\hat{Z}$$

The first term is adding a global phase to the quantum state, which is not doing anything, so the second term is what actually drives the quantum simulation. The dynamical behavior of quantum systems is governed by Schrodinger Equation:

$$i\hbar\frac{\partial|\psi\rangle}{\partial t} = \hat{H}|\psi\rangle = i\hbar(\dot{A}|0\rangle + \dot{B}|1\rangle) = \frac{\hbar\omega}{2}A|0\rangle - \frac{\hbar\omega}{2}B|1\rangle$$

Where $A(t) = A(0)e^{-i\omega t/2}$, $B(t) = B(0)e^{i\omega t/2}$, and any state is defined as

$$|\psi(t)\rangle = \exp\left(-i\,\frac{E_1 + E_2}{2}\,t\right)\left[A(0)\,e^{-i\omega t/2}\,|\psi_1\rangle \;+\; B(0)\,e^{+i\omega t/2}\,|\psi_2\rangle\right].$$

3.1.1 Time Dependent Quantum Operation

The Hamiltonian is a Hermitian operator, therefore it has a spectral decomposition

$$H = \sum_E E\,|E\rangle\langle E|$$

which states the energy E of the state $|E\rangle$, the evolution of state $|E\rangle$ is simple. Like a simple quantum infinite boundary model(or in any time-dependent quantum model actually)

$$|E\rangle \to \exp(-iEt/\hbar)\,|E\rangle = \exp\left(-i\hat{H}_0 t/\hbar\right) = \exp(-i\hat{\omega}t\sigma_z/2)$$

and the exponential of a Pauli Matrix is

$$e^{-i\theta\sigma_z} = \cos\theta\,\mathbb{I} - i\sin\theta\,\sigma_z = c\mathbb{I} - is\sigma_z \rightarrow U_0 = \cos\frac{\omega t}{2}\hat{I} + i\sin\frac{\omega t}{2}\sigma_z$$

this also tells the evolution of arbitrary gates, for instance X gate in the Heisenberg Picture:

$$X(t) = U_0(t)\sigma_x U_0^\dagger(t)$$

multiplying step by step using the expression of $U_0(t)$

$$X(t) = (c^2 - s^2)\sigma_x + acs\sigma_y = cos(\omega t)\sigma_x + sin(\omega t)\sigma_y = \begin{pmatrix} 0 & e^{i\omega t} \\ e^{-i\omega t} & 0 \end{pmatrix}$$

what this physically mean is that to implement a true X rotation at time t, the control pulse must generate $X(t)$

- Y gate

$$\begin{pmatrix} 0 & -ie^{i\omega t} \\ ie^{-i\omega t} & 0 \end{pmatrix}$$

- Z gate:

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

Therefore, the total Hamiltonian reads

$$\hat{H}(t) = \hat{H}_0 - \hat{r}\cdot f(t)$$

physically, r would be the dipole operator , and f(t) would be the classical driving field(magnetic or electric field). Plugging this expression into the Schrodinger's Equation

$$i\hbar\left[\dot{A}(t)\,|0\rangle + \dot{B}(t)\,|1\rangle\right] = \left[\hat{H}_0 - \hat{\mathbf{r}}\cdot\mathbf{f}(t)\right]\left[A\,|0\rangle + B\,|1\rangle\right].$$

to isolate A we can project the equation to $\langle 0|$ then we will obtain the form

$$\boxed{i\hbar\dot{A} = E_0 A - B\left(\mathbf{d}\cdot\mathbf{f}(t)\right) = E_0 A - B\left(\langle 0|\,\hat{r}\,|1\rangle\cdot\mathbf{f}(t)\right),}$$

and same for B

$$\boxed{i\hbar\dot{B} = E_1 B - A\left(\mathbf{d}^*\cdot\mathbf{f}^*(t)\right),}$$

In our case we consider a Harmonic Drive field

$$f(t) = f_0\cos(\omega t + \phi) \rightarrow \hat{H}_{int} = -\hat{r}\cdot f(t)$$

from which we can project the influence of the matrix on $|1\rangle$ onto $|0\rangle$ using $\langle 0|$. Additionally we define the influence of the field component(aka the strength of transition between $|1\rangle$ and $|0\rangle$) using the Rabi Frequency

$$\Omega = \langle 0|\,\hat{r}\,|1\rangle\cdot f_0/\hbar \rightarrow \langle 0|\,\hat{H}(t)\,|1\rangle = -\hbar\Omega\cos(\omega t + \phi)$$

when the frequency of the field is on resonance to the two level system, the populations of $|A|^2$ and $|B|^2$ will oscillate at rate Ω so called the Rabi Oscillations.

$$A(t) = \alpha(t)e^{i\omega t/2}$$
$$B(t) = \beta(t)e^{-i\omega t/2}$$

plugging it into the original equation for the derivative of A we can get

$$i\hbar\dot{A}(t) = -\frac{\hbar\Omega}{2}e^{i\omega_0 t}B(t) \rightarrow i\dot{\alpha} = \Omega\cos(\omega t + \phi)e^{-i\omega t}\beta \approx \frac{\Omega}{2}e^{i\phi}\beta$$

We used rotating Wave Approximation (RWA) assuming $\omega \gg \Omega$ ignoring the high frequency term. Differentiating the obtained expression we can solve the ODE and finding that

$$\frac{d\alpha^2}{dt^2} = -(\frac{\Omega}{2})^2\alpha$$

where $\beta(0) = \beta_0 = \alpha_0$

$$\boxed{\alpha(t) = \cos\left(\frac{\Omega t}{2}\right)\alpha(0) - i\sin\left(\frac{\Omega t}{2}\right)e^{i\phi}\beta(0)}$$

$$\boxed{\beta(t) = \cos\left(\frac{\Omega t}{2}\right)\beta(0) - i\sin\left(\frac{\Omega t}{2}\right)e^{-i\phi}\alpha(0)}$$

in matrix form it reads

$$\begin{pmatrix}\alpha(t)\\ \beta(t)\end{pmatrix} = \underbrace{\begin{pmatrix}\cos\left(\frac{\Omega t}{2}\right) & -ie^{i\phi}\sin\left(\frac{\Omega t}{2}\right)\\ -ie^{-i\phi}\sin\left(\frac{\Omega t}{2}\right) & \cos\left(\frac{\Omega t}{2}\right)\end{pmatrix}}_{U_1(\Omega t)}\begin{pmatrix}\alpha_0\\ \beta_0\end{pmatrix}.$$

where we can also see that

$$U_1(\theta) = \cos\left(\frac{\theta}{2}\right)\mathbb{I} - i\sin\left(\frac{\theta}{2}\right)\left[\cos\phi\,\sigma_x + \sin\phi\,\sigma_y\right], \quad \theta \equiv \Omega t.$$

this is precisely a rotation by angle θ about the Bloch-sphere axis $\cos\phi\hat{x} + \sin\phi\hat{y}$ From which we can see 3 special cases

- $\pi - pulse(\theta = \Omega t = \pi)$ gives
$$U_1(\pi) = -i\left[\cos\phi\,\sigma_x + \sin\phi\,\sigma_y\right]$$
which is a direct flip from $|0\rangle \to |1\rangle$ around the Bloch Sphere axis
- $\pi/2 - pulse(\theta = \Omega t = \pi/2)$
$$U_1\left(\frac{\pi}{2}\right) = \frac{1}{\sqrt{2}}\left(\mathbb{I} - i\left[\cos\phi\,\sigma_x + \sin\phi\,\sigma_y\right]\right),$$
which is a 90 degree rotation to the equator(XY plane) defined by the initial phase. Interestingly if the phase is 0 then this is a Hadamard Gate
- $2\pi - pulse(\theta = \Omega t = 2\pi)$ The operator returns the qubit to itself
$$U_1(2\pi, \phi) = -I$$

3.2 Two-Qubit Hamiltonian

In lab frame, a two qubit system only has a different energy comparing to a single qubit because of a coupling term V

$$i\hbar\frac{d}{dt}|\Psi(t)\rangle = \left(\hat{H}_0 + \hat{V}\right)|\Psi(t)\rangle \tag{1}$$

Recall that for a single qubit the time propagation equation is

$$U_0(t) = e^{-i\left(\frac{\hbar\omega}{2}\right)\sigma_z t/\hbar} = \cos\left(\frac{\omega t}{2}\right)\mathbb{I} - i\sin\left(\frac{\omega t}{2}\right)\sigma_z = \begin{pmatrix}e^{-i\omega t/2} & 0\\ 0 & e^{+i\omega t/2}\end{pmatrix}$$

Therefore for two qubits, the total time propagation is simply

$$\left|\tilde{\Psi}\right\rangle = \left(U_0^A(t)\otimes U_0^B(t)\right)|\psi\rangle$$

Also recall that the free Hamiltonian of the two qubit system is

$$\hat{H}_0 = \frac{\hbar\omega}{2}(\sigma_z\otimes I + I\otimes\sigma_z)$$

Assuming that both of them undergoes the same propagation we can sub in this representation into equation 1, we can obtain the form

$$i\hbar\frac{d}{dt}\left|\psi_{AB}\right\rangle = \left(\hat{U}_0^\dagger \otimes \hat{U}_0^\dagger\right)\hat{V}\left(\hat{U}_0 \otimes \hat{U}_0\right)\left|\psi_{AB}\right\rangle$$

How is it going to look like in matrix form? For each element of $\tilde{V}(t)$, the projection onto each of the state is

$$\tilde{V}_{ij}(t) = \langle i|\left(\hat{U}_0^\dagger \otimes \hat{U}_0^\dagger\right)\hat{V}\left(\hat{U}_0 \otimes \hat{U}_0\right)|j\rangle$$

but there is a simpler expression, in matrix form

$$\left(\hat{U}_0^\dagger \otimes \hat{U}_0^\dagger\right)\hat{V}\left(\hat{U}_0 \otimes \hat{U}_0\right) = \begin{pmatrix} e^{-i\omega t} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{+i\omega t} \end{pmatrix}\begin{pmatrix} V_{00,00} & V_{00,01} & V_{00,10} & V_{00,11} \\ V_{01,00} & V_{01,01} & V_{01,10} & V_{01,11} \\ V_{10,00} & V_{10,01} & V_{10,10} & V_{10,11} \\ V_{11,00} & V_{11,01} & V_{11,10} & V_{11,11} \end{pmatrix}\begin{pmatrix} e^{i\omega t} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{-i\omega t} \end{pmatrix} =$$

$$\begin{pmatrix} V_{00,00} & V_{00,01}e^{-i\omega t} & V_{00,10}e^{-i\omega t} & V_{00,11}e^{-i2\omega t} \\ V_{01,00}e^{+i\omega t} & V_{01,01} & V_{01,10} & V_{01,11}e^{-i\omega t} \\ V_{10,00}e^{+i\omega t} & V_{10,01} & V_{10,10} & V_{10,11}e^{-i\omega t} \\ V_{11,00}e^{+i2\omega t} & V_{11,01}e^{+i\omega t} & V_{11,10}e^{+i\omega t} & V_{11,11} \end{pmatrix}$$

neglecting all the high frequency term by RWA we can obtain the final approximated transoformation.

$$\tilde{V}(t) \approx \begin{pmatrix} V_{00,00} & 0 & 0 & 0 \\ 0 & V_{01,01} & V_{01,10} & 0 \\ 0 & V_{10,01} & V_{10,10} & 0 \\ 0 & 0 & 0 & V_{11,11} \end{pmatrix}$$

Example 2: A common two qubit coupling is the **Heisenberg Exchange**

$$\hat{V} = J\left(\vec{\sigma}^A \cdot \vec{\sigma}^B\right) = J\left(\sigma_x^A\sigma_x^B + \sigma_y^A\sigma_y^B + \sigma_z^A\sigma_z^B\right) = J\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

which is a $\sqrt{SWAP}$ gate, this indicates that

- Any two-qubit interaction that has conservation of energy can be used to build $\sqrt{SWAP}$ gate
- This gate plus arbitrary single qubit rotations is universal

Note that J is the exchange coupling strength, having the unit of energy, setting how fast the transition happens

3.3 Ionic Trap

so how do we actually trap ions for quantum computing? One solution is the RF(Paul) Trap introduced by Wolfgang Paul. The reason was because of Earnshaw's Theorem that electric potential can't really trap an ion. The main idea is to drive a electric field at Radio frequency, the time-averaged force is a restoring force in all directions.

1. Apply $V\cos(\Omega_{RF}t)$ to one pair of opposite electrodes and $-V\cos(\Omega_{RF}t)$ to the other pair.
2. one of the axis will be a saddle point.
3. If the frequency is fast enough, then the particle experiences a trapping force, with a time-averaged potential

$$U_{eff} \propto \frac{q^2V^2}{m\Omega_{RF}^2}(x^2+y^2+z^2)$$

This can be used to create a three-step Cirac-Zoller gate where you use shared motion of two trapped ions to enact a CZ gate between their internal qubit level. The state of a qubit is defined as

$$|q_Aq_B, n\rangle, \quad q_A \in \{0,1\} : \text{Internal States}$$

and n is the phonon(Motional Fock number), saying if it is in motion or not.

1. Starting with no motion in ground state

$$|\Psi(0)\rangle = \alpha\,|00,0\rangle + \beta\,|01,0\rangle + \gamma\,|10,0\rangle + \delta\,|11,0\rangle\,.$$

2. Apply a $\pi - pulse$ on Ion A such that

$$|1,n=0\rangle_A \leftrightarrow |0,n=1\rangle_A$$

and the state is

$$|\Psi_1\rangle = \alpha\,|00,0\rangle + \beta\,|01,0\rangle + \gamma\,|00,1\rangle + \delta\,|01,1\rangle$$

3. Apply a $2\pi - pulse$ on Ion B which do a rotation $|0\rangle \leftrightarrow |1\rangle$ state transition only if the phonon is present and adding a -1 global phase.

$$|\Psi_2\rangle = \alpha\,|00,0\rangle + \beta\,|01,0\rangle + \gamma\,|00,1\rangle - \delta\,|01,1\rangle$$

4. Apply a $\pi - pulse$ again on Ion A:

$$|\Psi_2\rangle = \alpha\,|00,0\rangle + \beta\,|01,0\rangle + \gamma\,|10,1\rangle - \delta\,|11,1\rangle$$

Now we have a CZ gate as demanded.

4 Quantum Error Correction

There are many form of noise, but in most case we talk about decoherence causes by random frequency noise

4.1 Dephasing

recall that the time-dependent state is defined as

$$|\psi(t)\rangle = A(0)e^{-i\omega t/2}|0\rangle + B(0)e^{i\omega t/2}|1\rangle = U_0(t)|\psi(0)\rangle$$

we can write the overlap of the evolved state with itself(how much hasn't changed yet)

$$\langle\psi(0)|U_0(t)|\psi(0)\rangle = \cos\frac{\omega t}{2}\hat{I} - i\sin\frac{\omega t}{2}\sigma_z$$

what if $\omega \to \omega + \delta\omega(t)$ for an instance so the total phase accured is

$$\phi(t) = \int_0^t \omega + \delta\omega(t)dt = \omega t + \int_0^t \delta\omega(t)dt$$

the second term ϵ is called **Random Phase** there are few properties about this noise

- Assume $\overline{\delta\omega(t)} = 0$ this is called the **White Noise** and

$$\overline{\delta\omega(t) * \delta\omega(t')} \propto \delta(t - t')$$

- **Variance:** follows the equation

$$\sigma^2 = \overline{\epsilon^2} = \int_0^t \int_0^t \delta\omega(t) * \delta\omega(t')dtdt' \approx \int_0^t Cdt = Ct$$

  where C is a constant set by the noise power spectral density and we define T = 1/C st. $\sigma^2 = t/T$

Therefore, the time evolution of quantum state with phase noise follows

$$|\psi(t)\rangle = A(0)e^{-(i\omega t/2 + i\epsilon/2)}|0\rangle + B(0)e^{(i\omega t/2 + i\epsilon/2)}|1\rangle$$

4.1.1 Fidelity

Fidelity is a metric for finding the time-average overlap between the ideal state and the noisy state.

$$F(t) = |\langle\psi(t)|U_\Phi(t)|\psi(0)\rangle|^2 =$$

undoing the ideal rotation U_0 gives

$$|\langle\psi(0)|U_0^\dagger U_\Phi(t)|\psi(0)\rangle|^2 = \begin{pmatrix} A^*e^{+i\omega t/2} & B^*e^{-i\omega t/2} \end{pmatrix} \begin{pmatrix} e^{-i\epsilon/2} & 0 \\ 0 & e^{+i\epsilon/2} \end{pmatrix} \begin{pmatrix} Ae^{-i\omega t/2} \\ Be^{+i\omega t/2} \end{pmatrix}.$$

which collapses to

$$= ||A|^2e^{-i\epsilon/2} + |B|^2e^{i\epsilon/2}|^2 = |A|^4 + |B|^4 + 2|A|^2|B|^2\overline{\cos}(\epsilon) = |A|^4 + |B|^4 + 2|A|^2|B|^2(e^{-\epsilon/2T} - 1)$$

st.

$$\boxed{F(\epsilon) = 1 + 2|A|^2|B|^2(e^{-\epsilon/2T} - 1)}$$

4.2 Bit-Flip Error

One common error is if Bit-Flip doesn't occur correctly, this can be fixed by the bit flip code. Suppose we encode the single qubit state $a|0\rangle + b|1\rangle$ as $a|000\rangle + b|111\rangle$ or $a|0_L\rangle + b|1_L\rangle$ so called the *logical* $|0\rangle$ and *logical* $|1\rangle$ states. A circuit performing such an encoding is

$|\psi\rangle$ 1 2
$|0\rangle$
$|0\rangle$

Suppose a bit flip occurred on one or fewer of the qubits, there is a simple two stage error-correction procedure which can be used to recover the correct quantum state:

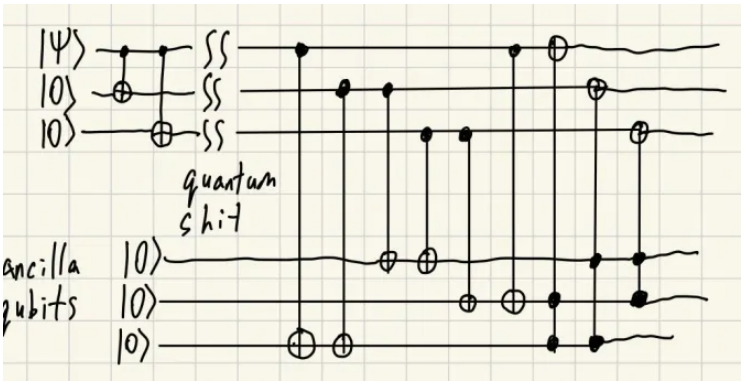
- Error Detection(error syndrome measurement):
  first use 4 different projection operators

$$\begin{aligned} P_0 &\equiv |000\rangle\langle 000| + |111\rangle\langle 111| && \text{no error} \\ P_1 &\equiv |100\rangle\langle 100| + |011\rangle\langle 011| && \text{bit flip on qubit one} \\ P_2 &\equiv |010\rangle\langle 010| + |101\rangle\langle 101| && \text{bit flip on qubit two} \\ P_3 &\equiv |001\rangle\langle 001| + |110\rangle\langle 110| && \text{bit flip on qubit three.} \end{aligned}$$

  Note that syndrome measurement doesn't change the state of the qubit, because it only tells us about the information of the error not the entire qubit.

- Recovery: Based on the error we flip the qubit that is having error. Suppose the change of error on each qubit is p then the the probability of having bit flip on one or fewer of the three qubits is $1 - 3p^2 + 2p^3$

The following is the full Detection and Correction Circuits: The ancilla Qubits stores information about the com-



parison between qubit 2 vs 3, 1 vs 3, 1 vs 2. If there is any disparity bewteen the states then the ancilla qubit that has state $|1\rangle$ at the end of the detection tells you which qubit to flip

$$(1, 0, 0)$$

tells you that data 1 has been flipped(needs to be flipped to recover)

4.3 Phase Error

Phase flip error can be understood as a Z gate applying on $|1\rangle$ or $|0\rangle$ with a probability of p. The solution is simple, change the basis of the state! Suppose we use Bell State instead of classical $|0\rangle$ *and* $|1\rangle$ flipping the bell state is the same as flipping the phase = bit flip error.

$|\psi\rangle$ 1 2 H
$|0\rangle$ H
$|0\rangle$ H

to prepare the circuit in Bell States, then run the 3 qubit bit-flip code and apply a Hadamard Gate again to return to the computational basis.

References

[1] Wikipedia contributors. Schmidt decomposition — Wikipedia, the free encyclopedia, 2025. [Online; accessed 13-March-2025].