Imperial College London

NOTES

IMPERIAL COLLEGE LONDON

DEPARTMENT OF COMPUTING

Quantum Information

Author:
Chen Huang

Email:
chen.huang23@imperial.ac.uk

Date: November 14, 2023

Contents

1 Elements of Quantum Mechanics and Quantum Information

1.1 Tools I from Quantum Mechanics

1.1.1 States and Operators

The harmonic oscillator

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right) \tag{1}$$

where the unit of $\hbar = 1$ has been applied and the zero-point energy $\omega/2$ has been ignored. With the common relations

$$\hat{a}\left|n\right\rangle = \sqrt{n}\left|n-1\right\rangle, \qquad \hat{a}^\dagger\left|n\right\rangle = \sqrt{n+1}\left|n+1\right\rangle \tag{2}$$

one can evaluate everything with any knowledge of the wave functions $\psi(x)$ in real space or any other representation.

We can express the operator a as

$$\hat{a} = \sum_{m,n=0}^{\infty}\left|m\right\rangle\left\langle m\right|\hat{a}\left|n\right\rangle\left\langle n\right| = \sum_{n=0}^{\infty}\sqrt{n+1}\left|n\right\rangle\left\langle n\right| \tag{3}$$

Similarly, we can express any operator for any quantum mechanical system as

$$\hat{A} = \sum_{i,j}\left\langle i\right|\hat{A}\left|j\right\rangle\left|i\right\rangle\left\langle j\right| \tag{4}$$

For a two-dimensional system, *i.e.* a qubit, the corresponding space of operators is in 2×2 matrix, and a common basis is given by the identity $\mathbb{1}$ and the three Pauli matrices.

$$\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \hat{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{5}$$

that implies the **commutator** and **anti-commutator** relation

$$[\hat{\sigma}_\alpha, \hat{\sigma}_\beta] = 2i\varepsilon_{\alpha\beta\gamma}\hat{\sigma}_\gamma, \qquad \{\hat{\sigma}_\alpha, \hat{\sigma}_\beta\} = 0 \tag{6}$$

1.1.2 Dynamics

The Schrödinger equation is written as $(\hbar = 1)$

$$i\frac{\mathrm{d}}{\mathrm{d}t}\left|\Psi(t)\right\rangle = \hat{H}\left|\Psi(t)\right\rangle \tag{7}$$

with a time-independent Hamiltonian, one obtains that

$$\left|\Psi(t)\right\rangle = \hat{U}(t,t_0)\left|\Psi(t_0)\right\rangle = \mathrm{e}^{-i\hat{H}(t-t_0)}\left|\Psi(t_0)\right\rangle \tag{8}$$

One may express this also in terms of the *time-evolution operator* or *propagator*

$$\hat{U}(t,t_0) = \mathrm{e}^{-i\hat{H}(t-t_0)} \tag{9}$$

which has several key properties:

- **The propagator $\hat{U}$ and $\hat{H}$ commute, and have the same eigenstates.** With the spectral decomposition $\hat{H} = \sum_j \omega_j |\Psi_j\rangle \langle\Psi_j|$, one obtains

$$\hat{U} = \hat{U} \sum_j |\Psi_j\rangle \langle\Psi_j| = \sum_j \mathrm{e}^{-i\omega_j(t-t_0)} |\Psi_j\rangle \langle\Psi_j| \tag{10}$$

- **The propagator is unitary**, *i.e.*

$$\hat{U}(t,t_0)\hat{U}^\dagger(t,t_0) = \hat{U}(t,t_0)^\dagger \hat{U}(t,t_0) = \mathbb{I} \tag{11}$$

  which guarantees conservation of norm of $|\Psi(t)\rangle$, and thus normalisation.

- **The propagator (as operator) satisfies the Schrödinger equation.** The basis states evolve as $|\Psi_j(t)\rangle = \hat{U}(t,t_0)|\Psi_j(t_0)\rangle$. That is, we can write the propagator as

$$\hat{U}(t,t_0) = \hat{U}(t,t_0)\sum_j |\Psi_j(t_0)\rangle \langle\Psi_j(t_0)| = \sum_j |\Psi_j(t)\rangle \langle\Psi_j(t_0)| \tag{12}$$

  We thus obtain

$$i\frac{\mathrm{d}}{\mathrm{d}t}\hat{U}(t,t_0) = \sum_j i\frac{\mathrm{d}}{\mathrm{d}t}|\Psi_j(t)\rangle \langle\Psi_j(t_0)| = \sum_j \hat{H}|\Psi_j(t)\rangle \langle\Psi_j(t_0)| = \hat{H}\hat{U}(t,t_0) \tag{13}$$

In quantum information, one often uses the term ‘quantum gate’ or simply ‘gate’ instead of propagator.

1.1.3 Measurement

Formally, a measurement is described in terms of projectors. Choose $\{|0\rangle, |1\rangle\}$ as the measurement basis, and the projectors are $\hat{P}_0 = |0\rangle\langle 0|$ and $\hat{P}_1 = |1\rangle\langle 1|$. The state reduction

$$\hat{P}_0|\psi\rangle = \hat{P}_0(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle \tag{14}$$

$$\hat{P}_1|\psi\rangle = \hat{P}_1(\alpha|0\rangle + \beta|1\rangle) = \beta|1\rangle \tag{15}$$

with probability

$$p_0 = \langle\psi|\hat{P}_0|\psi\rangle = |\alpha|^2, \quad p_1 = \langle\psi|\hat{P}_1|\psi\rangle = |\beta|^2 \tag{16}$$

The condition

$$\sum_i p_i = \langle\psi|\sum_i \hat{P}_i|\psi\rangle = 1 \tag{17}$$

must be required.

1.2 Quantum Key Distribution - BB84

Quantum Key Distribution (QKD) permits to share string of random numbers. One of the QKD protocol is *BB84*, which invented by Charles Bennett and Giles Brassard in 1984. Alice uses one qubit and prepares randomly one of the four states

$$|\mathrm{H}\rangle = |0\rangle\,, \quad |\mathrm{V}\rangle = |1\rangle\,, \quad |\mathrm{D}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\mathrm{A}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{18}$$

1. **Sending**: Alice randomly selects a string of bits and a string of basis ($+$ or $\times$) of equal length.
$$+ \to \{|\mathrm{H}\rangle\,, |\mathrm{V}\rangle\}, \qquad \times \to \{|\mathrm{D}\rangle\,, |\mathrm{A}\rangle\}$$
Then she transmits a photon for each bit with the corresponding polarization to Bob.

2. **Receiving**: Bob randomly chooses a basis for each photon to measure its polarization. If Bob selects the same basis as Alice for a particular photon, he will correctly find the bit Alice wanted to share as he measured the same polarization. If he doesn't guess correctly, he will get a random bit.

3. **Compare**: Bob tells Alice the bases he used to measure each photon. Alice informs Bob of the bases he guessed correctly to measure the encoded bits. After that, Alice and Bob remove the encoded and measured bits on different bases. Now, Alice and Bob have an identical bit-string, the s**hifted key**.

Alice's random bits	1	0	0	1	1	0	1	0	0	1
Alice's encoding basis	$+$	$\times$	$\times$	$+$	$\times$	$+$	$+$	$+$	$+$	$+$
Photons Alice sends	V	D	D	V	A	H	V	H	H	V
Random measurement basis	$+$	$+$	$\times$	$+$	$+$	$\times$	$+$	$+$	$+$	$\times$
Bits as received by Bob	V	V	D	V	H	A	V	H	H	D
Reveal the sequence of their basis	✓		✓	✓			✓	✓	✓	
Shifted Key	1		0	1			1	0	0	

Table 1: BB84 protocol

1.3 No-Cloning Theorem

Let's assume we have a qubit in a given state $|\Psi\rangle$ (but we don't know the state) and a second qubit in the $|0\rangle$ state. We would like to find a gate such that

$$\hat{U}\,|\Psi\rangle\,|0\rangle = |\Psi\rangle\,|\Psi\rangle \tag{19}$$

for any state $|\Psi\rangle$, so we have

$$\hat{U}\,|0\rangle\,|0\rangle = |0\rangle\,|0\rangle \tag{20}$$

$$\hat{U}\,|1\rangle\,|0\rangle = |1\rangle\,|1\rangle \tag{21}$$

For a general state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, this implies that

$$\hat{U}(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \tag{22}$$

whereas we would have wanted to obtain

$$(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) = \alpha^2|0\rangle|0\rangle + \alpha\beta(|0\rangle|1\rangle + |1\rangle|0\rangle) + \beta^2|1\rangle|1\rangle \tag{23}$$

In the above example, the cloning process works if either α or β vanishes; that is, it works for the two orthogonal basis states for which it is defined.

1.4 Tools II from Quantum Mechanics

1.4.1 Bell's Inequality

Assume that Alice has two cards A_0, A_1 having their value either $+1$ or -1 and Bob has his cards B_0 and B_1 also having their values $+1$ or -1. If all the cards bear the value $+1$, i.e. $A_0 = A_1 = B_0 = B_1 = 1$, then

$$A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 = 2 \tag{24}$$

The average

$$\boxed{\langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle \leq 2} \tag{25}$$

This is called *Bell's inequality* which is obtained for **classical** physics based on local realism.

However, we can prove that a quantum-mechanically correlated state can violate Bell's inequality. Let us assume the singlet state,

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{26}$$

and the observables $\hat{A}_0 = \hat{\sigma}_z$, $\hat{A}_1 = \hat{\sigma}_x$, $\hat{B}_0 = -\frac{1}{\sqrt{2}}(\hat{\sigma}_x + \hat{\sigma}_z)$, $\hat{B}_1 = \frac{1}{\sqrt{2}}(\hat{\sigma}_x - \hat{\sigma}_z)$. Then we find that

$$\begin{aligned}\langle \hat{A}_0 \otimes \hat{B}_0\rangle &= \langle\psi|\, \hat{A}_0 \otimes \hat{B}_0\, |\psi\rangle \\ &= -\frac{1}{2\sqrt{2}}((\langle 01| - \langle 10|)\hat{\sigma}_z \otimes (\hat{\sigma}_x + \hat{\sigma}_z)(|01\rangle - |10\rangle) \\ &= -\frac{1}{2\sqrt{2}}((\langle 01| - \langle 10|)(|00\rangle - |01\rangle + |11\rangle + |10\rangle) = \frac{1}{\sqrt{2}}\end{aligned} \tag{27}$$

Similarly, we can find

$$\langle \hat{A}_0 \otimes \hat{B}_0\rangle = \langle \hat{A}_0 \otimes \hat{B}_1\rangle = \langle \hat{A}_1 \otimes \hat{B}_0\rangle = -\langle \hat{A}_1 \otimes \hat{B}_1\rangle = \frac{1}{\sqrt{2}} \tag{28}$$

and the Bell's expectation value is

$$\langle \hat{A}_0 \otimes \hat{B}_0\rangle + \langle \hat{A}_0 \otimes \hat{B}_1\rangle + \langle \hat{A}_1 \otimes \hat{B}_0\rangle - \langle \hat{A}_1 \otimes \hat{B}_1\rangle = 2\sqrt{2} \tag{29}$$

which clearly **violates** Bell's inequality.

1.4.2 Partial Trace

The trace of the operator $\hat{A}$ reads

$$\operatorname{tr} \hat{A} = \sum_i \langle i| \hat{A} |i\rangle \tag{30}$$

for any orthonormal basis $\{|i\rangle\}$. For an operator $\hat{A} \otimes \hat{B}$ (on $\mathcal{H}_a \otimes \mathcal{H}_b$) we can define the partial traces

$$\hat{A} \operatorname{tr}_b \hat{B} = \operatorname{tr}_b \left(\hat{A} \otimes \hat{B}\right) \tag{31}$$

$$\hat{B} \operatorname{tr}_a \hat{A} = \operatorname{tr}_a \left(\hat{A} \otimes \hat{B}\right) \tag{32}$$

The partial trace naturally appears in expressions of the form $\operatorname{tr}\left(\left(\hat{A} \otimes \mathbb{I}\right) \hat{C}\right)$, where $\hat{A}$ acts on $\mathcal{H}_a$, $\mathbb{I}$ acts on $\mathcal{H}_b$ and $\mathbb{C}$ acts on $\mathcal{H}_a \otimes \mathcal{H}_b$.

$$\begin{aligned}
\operatorname{tr}\left(\left(\hat{A} \otimes \mathbb{I}\right) \hat{C}\right) &= \sum_{ij} \langle i|_a \otimes \langle j|_b \left(\left(\hat{A} \otimes \mathbb{I}\right) \hat{C}\right) |i\rangle_a \otimes |j\rangle_b \\
&= \sum_{ij} \left(\langle i|_a \hat{A}\right) \otimes \langle j|_b \hat{C} \left(|i\rangle_a \otimes |j\rangle_b\right) \\
&= \sum_i \langle i|_a \hat{A} \left(\sum_j \langle j|_b \hat{C} |j\rangle_b\right) |i\rangle_a \\
&= \operatorname{tr}_a \left(\hat{A} \operatorname{tr}_b \hat{C}\right)
\end{aligned} \tag{33}$$

2 Quantum Algorithms

2.1 Quantum Interferometers

Let's take the Mach-Zehnder interferometer as an example.

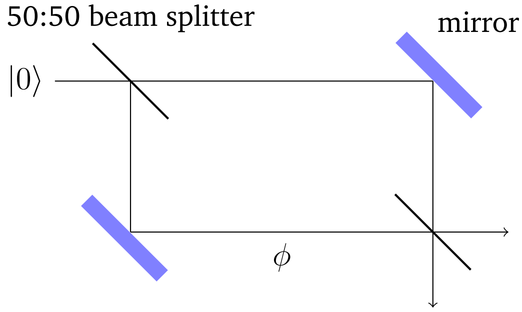

Figure 1: The Mach-Zehnder interferometer.

The Mach-Zehnder interferometer is described by

$$\begin{aligned}\underbrace{\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}}_{\text{2nd bs}}\underbrace{\begin{pmatrix}1 & 0\\ 0 & e^{i\phi}\end{pmatrix}}_{\text{phase shift}}\underbrace{\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}}_{\text{1st bs}}\underbrace{\begin{pmatrix}1\\ 0\end{pmatrix}}_{\text{input}} &= \frac{1}{2}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & e^{i\phi}\end{pmatrix}\begin{pmatrix}1\\ -1\end{pmatrix}\\ &= \frac{1}{2}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1\\ -e^{i\phi}\end{pmatrix}\\ &= \frac{1}{2}e^{i\phi/2}\begin{pmatrix}e^{-i\phi/2}+e^{i\phi/2}\\ e^{-i\phi/2}-e^{i\phi/2}\end{pmatrix}\\ &= e^{i\phi/2}\begin{pmatrix}\cos\phi/2\\ -i\sin\phi/2\end{pmatrix}\end{aligned} \tag{34}$$

where phase shift is described by the rotation

$$\hat{R}_\phi = \begin{pmatrix}1 & 0\\ 0 & e^{i\phi}\end{pmatrix} = e^{i\phi/2}\begin{pmatrix}e^{-i\phi/2} & 0\\ 0 & e^{i\phi/2}\end{pmatrix} \tag{35}$$

and the beam splitter is described by

$$\hat{B} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix} = \frac{1}{\sqrt{2}}(\mathbb{1}+\hat{\sigma}_y) = e^{i\pi\hat{\sigma}_y/4} \tag{36}$$

2.2 Basic Gate Operators

- **Pauli** X, Y, Z **gates** - single qubit gates

$$\hat{X} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \qquad \hat{Y} = \begin{pmatrix}0 & i\\ -i & 0\end{pmatrix}, \qquad \hat{Z} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \tag{37}$$

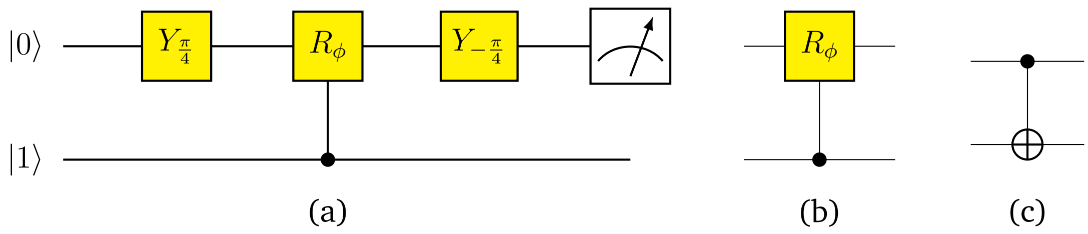

Figure 2: (a) For the input state $|0\rangle$, the quantum circuit for the Macj-Zehnder interferometer. (b) The controlled-phase gate. (c) The Controlled-NOT gate.

- **Controlled-phase gate**

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix} \tag{38}$$

- **Controlled-NOT gate**

$$\begin{aligned} \hat{U}_c &= |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10| \\ &= |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \hat{\sigma}_x \end{aligned} \tag{39}$$

which generates

input		output	
control	target	control	target
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Table 2: Controlled-NOT gate.

Compare with the XOR gate (for conventional computer)

input		output
0	0	0
0	1	1
1	0	1
1	1	0

Table 3: The XOR gate in conventional computer.

NOTE: Any unitary on a system with several qubits as a sequence of *single qubit gates* and *CNOT* gates. A general single qubit unitary gate and two-qubit controlled-gate are called a *universal* quantum gate.

2.3 Deutsch Jozsa Algorithm

The task of this algorithm is to probe whether a function $f : \{0,1\} \to \{1,0\}$ is constant. *i.e.* if $f(0) = f(1)$, or if it is balanced, *i.e.* if $f(0) \neq f(1)$. The function f can be implemented in terms of a two qubit gate

$$|i\rangle \otimes |j\rangle \to \hat{U}_o |ij\rangle = |i\rangle \otimes |j \oplus f(i)\rangle \tag{40}$$

where '$\oplus$' denotes the addition modulo 2, *i.e.* $0 \oplus A = A$ and $1 \oplus A = \bar{A}$, where $\bar{A}$ denotes '*not* A'.

$$\hat{U}_0 |00\rangle = |0f(0)\rangle \tag{41}$$

$$\hat{U}_0 |01\rangle = \left|0\overline{f(0)}\right\rangle \tag{42}$$

$$\hat{U}_0 |10\rangle = |1f(1)\rangle \tag{43}$$

$$\hat{U}_0 |11\rangle = \left|1\overline{f(1)}\right\rangle \tag{44}$$

With the initial state

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right) \tag{45}$$

one obtains

$$\hat{U}_0 \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{2}\left(|0f(0)\rangle - \left|0\overline{f(0)}\right\rangle + |1f(1)\rangle - \left|1\overline{f(1)}\right\rangle\right) = |\Psi_0\rangle \tag{46}$$

If $f(0) = f(1)$, this reduces to

$$\begin{aligned} |\Psi_0\rangle =& \frac{1}{2}\left[(|0\rangle + |1\rangle) \otimes |f(0)\rangle - (|0\rangle + |1\rangle) \otimes \left|\overline{f(0)}\right\rangle\right] \\ =& \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - \left|\overline{f(0)}\right\rangle}{\sqrt{2}} = |+\rangle \otimes \frac{|0\rangle - \left|\overline{f(0)}\right\rangle}{\sqrt{2}} \end{aligned} \tag{47}$$

If $f(0) = \overline{f(1)}$, this reduces to

$$\begin{aligned} |\Psi_0\rangle =& \frac{1}{2}\left[(|0\rangle - |1\rangle) \otimes |f(0)\rangle - (|0\rangle - |1\rangle) \otimes \left|\overline{f(0)}\right\rangle\right] \\ =& \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |f(1)\rangle}{\sqrt{2}} = |-\rangle \otimes \frac{|0\rangle - |f(1)\rangle}{\sqrt{2}} \end{aligned} \tag{48}$$

A measurement on the first qubit in the $\hat{\sigma}_x$-basis permits to distinguish between these two cases.

In practice, the algorithm would be broken down in the elementary steps:

1. Prepare of the initial state $|0\rangle \otimes |0\rangle$.

2. Application of the gate $\mathrm{e}^{-i\frac{\pi}{4}\hat{\sigma}_y} \otimes \mathrm{e}^{i\frac{\pi}{4}\hat{\sigma}_y}$ (if we want to use the Hadamard gate $\hat{H} \otimes \hat{H}\hat{\sigma}_x$)

$$\left[\exp\left(-i\frac{\pi}{4}\hat{\sigma}_y\right) \otimes \exp\left(i\frac{\pi}{4}\hat{\sigma}_y\right)\right] (|0\rangle \otimes |0\rangle) = |+\rangle \otimes |-\rangle \tag{49}$$

3. Query to the oracle
   - If $f(0) = f(1)$, then the first qubit is in $|+\rangle$.
   - If $f(0) = f(1)$, then the first qubit is in $|-\rangle$.

4. Application of the gate $\exp\left(-i\frac{\pi}{4}\hat{\sigma}_y\right) \otimes \mathbb{1}$, which will bring $|+\rangle$ to $|1\rangle$ and $|-\rangle$ to $|0\rangle$.

5. Measurement on the first qubit in the $\hat{\sigma}_z$-basis.

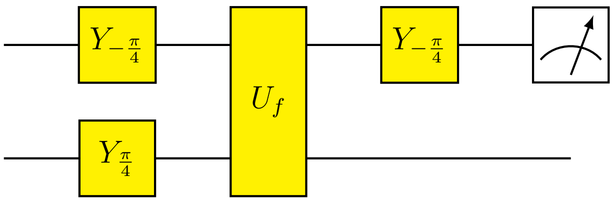

Figure 3: The quantum circuit of the Deutsch-Jozsa algorithm.

2.4 Basic Gate Operation II

2.4.1 Controlled-Z Gate and Controlled-Unitary Gate

$$\hat{U}_{cz} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \hat{\sigma}_z \tag{50}$$

similar to a CNOT gate which reads

$$\hat{U}_c = \hat{U}_{cx} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \hat{\sigma}_x \tag{51}$$

With $\hat{\sigma}_z = \exp\left(i\frac{\pi}{4}\hat{\sigma}_y\right)\hat{\sigma}_x \exp\left(-i\frac{\pi}{4}\hat{\sigma}_y\right)$ one can see that $\hat{U}_{cz}$ can be realise as the gate sequence

$$\begin{aligned}
\hat{U}_{cz} &= |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \exp\left(i\frac{\pi}{4}\hat{\sigma}_y\right)\hat{\sigma}_x \exp\left(-i\frac{\pi}{4}\hat{\sigma}_y\right) \\
&= \left[\mathbb{1} \otimes \exp\left(i\frac{\pi}{4}\hat{\sigma}_y\right)\right] (|0\rangle\langle 0| \otimes \mathbb{1}) \left[\mathbb{1} \otimes \exp\left(-i\frac{\pi}{4}\hat{\sigma}_y\right)\right] \\
&\quad + \left[\mathbb{1} \otimes \exp\left(i\frac{\pi}{4}\hat{\sigma}_y\right)\right] (|1\rangle\langle 1| \otimes \hat{\sigma}_x) \left[\mathbb{1} \otimes \exp\left(-i\frac{\pi}{4}\hat{\sigma}_y\right)\right] \\
&= \left[\mathbb{1} \otimes \exp\left(i\frac{\pi}{4}\hat{\sigma}_y\right)\right] \hat{U}_c \left[\mathbb{1} \otimes \exp\left(-i\frac{\pi}{4}\hat{\sigma}_y\right)\right]
\end{aligned} \tag{52}$$

so we have

$$\hat{U}_{cz}|00\rangle = |00\rangle\,, \quad \hat{U}_{cz}|01\rangle = |01\rangle\,, \quad \hat{U}_{cz}|10\rangle = |10\rangle\,, \quad \hat{U}_{cz}|11\rangle = -|11\rangle \tag{53}$$

We can generalize two qubit operations to the controlled-unitary operation:

$$\hat{U}_{cu} = |0\rangle\langle 0| \times \mathbb{1} + |1\rangle\langle 1| \otimes \hat{U} \tag{54}$$

NOTE: In a controlled gate operation, the action on one qubit is dependent on the state of another qubit. So they cannot be written in

$$\hat{U}_1 \otimes \hat{U}_2 \tag{55}$$

2.4.2 Three Qubits - Controlled-Controlled-Unitary Gate

A generalisation of the controlled-unitary gate to a system of three qubits is a controlled-controlled-unitary gate

$$(\mathbb{1} \otimes \mathbb{1} - |1\rangle\langle 1| \otimes |1\rangle\langle 1|) \otimes \mathbb{1} + |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \hat{U} \tag{56}$$

The controlled-not gate operation can be written in

$$|i\rangle|j\rangle \rightarrow |i\rangle|i \oplus j\rangle \tag{57}$$

The controlled-unitary gate operation can be written in

$$|i\rangle|j\rangle \rightarrow |i\rangle \hat{U}^i|j\rangle \tag{58}$$

The three qubits gate can be decomposed into single and two-qubit gates as depicted in the quantum circuit Fig.(4)

1. $|i\rangle|j\rangle \hat{V}^j|k\rangle$
2. $|i\rangle|i \oplus j\rangle \hat{V}^j|k\rangle$
3. $|i\rangle|i \oplus j\rangle (\hat{V}^\dagger)^{i\oplus j}\hat{V}^j|k\rangle$
4. $|i\rangle|i \oplus (i \oplus j)\rangle (\hat{V}^\dagger)^{i\oplus j}\hat{V}^j|k\rangle = |i\rangle|j\rangle (\hat{V}^\dagger)^{i\oplus j}\hat{V}^j|k\rangle$
5. $|i\rangle|j\rangle \hat{V}^i(\hat{V}^\dagger)^{i\oplus j}\hat{V}^j|k\rangle$

So we have

$$\begin{aligned}
\hat{U}|00\rangle \otimes |\phi\rangle &= |00\rangle \otimes |\phi\rangle \\
\hat{U}|01\rangle \otimes |\phi\rangle &= |01\rangle \otimes |\phi\rangle \\
\hat{U}|10\rangle \otimes |\phi\rangle &= |10\rangle \otimes |\phi\rangle \\
\hat{U}|11\rangle \otimes |\phi\rangle &= |11\rangle \otimes \hat{U}|\phi\rangle
\end{aligned} \tag{59}$$

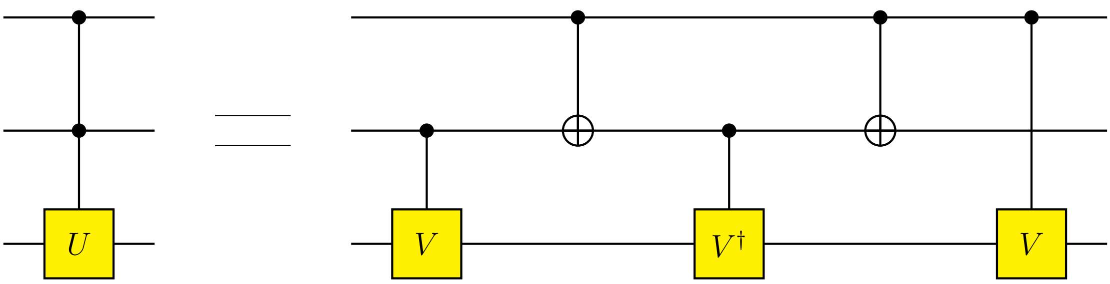

Figure 4: A controlled-controlled-U operation can be realised in terms of CNOT and controlled-V operations for $\hat{U} = \hat{V}^2$

2.4.3 NOT Gate

The Pauli $\hat{\sigma}_x$ operator is also called as the NOT gate as it switches

$$\hat{\sigma}_x |0\rangle = |1\rangle , \qquad \hat{\sigma}_x |1\rangle = |0\rangle \tag{60}$$

In quantum mechanics, do we have a universal-NOT gate? Let's consider an arbitrary state

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{61}$$

then

$$\text{NOT} |\Psi\rangle = \alpha |1\rangle + \beta |0\rangle = |\Psi'\rangle \tag{62}$$

as

$$\langle\Psi'|\Psi\rangle = (\alpha^* \langle 1| + \beta^* \langle 0|) (\alpha |0\rangle + \beta |1\rangle) = \alpha^*\beta + \beta^*\alpha \neq 0 \tag{63}$$

NOT operation cannot to bring the initial state $|\psi\rangle$ to its orthogonal state $|\Psi^\perp\rangle$ ($\langle\Psi^\perp|\Psi\rangle = 0$), *i.e.* we don't have a universal-NOT gate in quantum mechanics.

2.4.4 SWAP Gate

The SWAP gate is to swap two qubits

$$\text{SWAP} |\Psi\rangle |\Phi\rangle = |\Phi\rangle |\Psi\rangle \tag{64}$$

with

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{65}$$

2.5 Grover's Algorithm (Quantum Search Algorithm)

The goal of the algorithm is to find a solution to the search problem. Let's consider a system with n qubits; that is, we are working in an $N = 2^n$ dimensional Hilbert space. The Grover's algorithm follows the following steps:

1) The system begins with the initial state $|0\rangle |0\rangle \cdots |0\rangle = |0\rangle^{\otimes n}$

2) Apply Hadamard transform $\hat{H}^{\otimes n}$

$$|s\rangle = \hat{H} |0\rangle \ldots \hat{H} |0\rangle \hat{H} |0\rangle = |+\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \tag{66}$$

3) Apply $\hat{U} = \mathbb{1} - 2 |q\rangle \langle q|$

$$\begin{aligned} |\Psi\rangle =& \hat{U} |s\rangle = (\mathbb{1} - 2 |q\rangle \langle q|) |s\rangle \\ =& |s\rangle - 2 |q\rangle \langle q| \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \\ =& |s\rangle - \frac{2}{\sqrt{N}} |q\rangle \end{aligned} \tag{67}$$

4) Apply $\hat{V} = 2\left|s\right\rangle\left\langle s\right| - \mathbb{1}$

$$\begin{aligned}\hat{V}\left|\Psi\right\rangle =&(2\left|s\right\rangle\left\langle s\right| - \mathbb{1})(\left|s\right\rangle - \frac{2}{\sqrt{N}}\left|q\right\rangle) \\ =&2\left|s\right\rangle - \left|s\right\rangle - \frac{4}{\sqrt{N}}\left|s\right\rangle\left\langle s|q\right\rangle + \frac{2}{\sqrt{N}}\left|q\right\rangle \\ =&\left|s\right\rangle - \frac{4}{N}\left|s\right\rangle\sum_{i=0}^{N-1}\left\langle i|q\right\rangle + \frac{2}{\sqrt{N}}\left|q\right\rangle \\ =&\frac{N-4}{N}\left|s\right\rangle + \frac{2}{\sqrt{N}}\left|q\right\rangle \\ =&\frac{N-4}{N\sqrt{N}}\sum_{i\neq q}^{N-1}\left|i\right\rangle + \left(\frac{N-4}{N\sqrt{N}} + \frac{2}{\sqrt{N}}\right)\left|q\right\rangle\end{aligned} \tag{68}$$

We find that the probability of finding $\left|q\right\rangle$

$$\left(\frac{N-4}{N\sqrt{N}} + \frac{2}{\sqrt{N}}\right)^2 > \frac{1}{N} \tag{69}$$

when $N > 2$.

5) Repeat the process 2) and 3) to increase the probability of finding the system in $\left|q\right\rangle$.

2.6 Quantum Fourier Transform

The quantum Fourier transform $\mathcal{QF}$ for an N-dimensional system is defined as

$$\boxed{\mathcal{QF}\left|\Phi_p\right\rangle = \frac{1}{\sqrt{N}}\sum_{q=0}^{N-1} \mathrm{e}^{\frac{2\pi i}{N}pq}\left|\Phi_q\right\rangle} \tag{70}$$

For $N = 2^n$ one can realise it with n qubits.

- **A single qubit**

$$\mathcal{QF}\left|p\right\rangle = \frac{1}{\sqrt{2}}\sum_{q=0}^{1} \mathrm{e}^{\frac{2\pi i}{N}pq}\left|q\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \mathrm{e}^{i\pi p}\left|1\right\rangle\right) \tag{71}$$

  This is also know as Hadamard gate, with

$$\mathcal{QF}\left|0\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle) = \left|+\right\rangle \tag{72}$$

$$\mathcal{QF}\left|1\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) = \left|-\right\rangle \tag{73}$$

- **Many qubits**

$$\mathcal{QF}_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix} \tag{74}$$

where $\omega = \exp(2\pi i/N)$ is the N^{th} root of unity. The state for n qubits can be written in

$$\begin{aligned} |\Psi\rangle =& a_0 |0\rangle + a_1 |1\rangle + \cdots + a_{N-1} |N-1\rangle \\ =& a_0 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + a_1 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + a_{N-1} \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{N-1} \end{pmatrix} \end{aligned} \tag{75}$$

- **Two qubits**

$$\mathcal{QF}_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \tag{76}$$

We have some examples

i) $|f\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle) \quad \Rightarrow \quad \left|\tilde{f}\right\rangle = \mathcal{QF}_4 |f\rangle = |0\rangle$

ii) $|g\rangle = |0\rangle \quad \Rightarrow \quad |\tilde{g}\rangle = \mathcal{QF}_4 |g\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$

iii) $|h\rangle = |1\rangle \quad \Rightarrow \quad \left|\tilde{h}\right\rangle = \mathcal{QF}_4 |h\rangle = \frac{1}{2}(|0\rangle + i\,|1\rangle - |2\rangle - i\,|3\rangle)$

2.6.1 Properties of Quantum Fourier Transform

1. **QFT is unitary**
   Proof: an operator is unitary if its columns are orthonormal.

$$\frac{1}{N}\sum_{n=0}^{N-1} \omega^{ni}\omega^{nj*} = \frac{1}{N}\sum_{n=0}^{N-1} (\omega^{i-j})^n = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \tag{77}$$

2. **Linear shift** as shown in the example above $|\tilde{g}\rangle$ and $\left|\tilde{h}\right\rangle$.

3. **Period/wave length relationship**

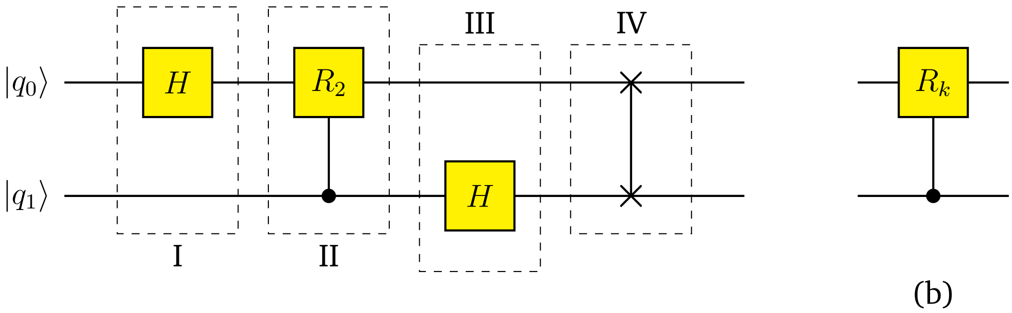

Figure 5: (a) The quantum circuit for quantum Fourier transform. (b) The part II in the circuit (a).

2.6.2 Quantum Circuit of Quantum Fourier Transform

The quantum circuit for the two-qubit QFT see in Fig.5(a).

I. The part I of the circuit reads

$$\hat{H} \otimes \mathbb{1} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbb{1} & \mathbb{1} \\ \mathbb{1} & -\mathbb{1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \tag{78}$$

II. The part II (see Fig.5(b)) reads

$$\mathbb{1} \otimes |0\rangle\langle 0| + (|0\rangle\langle 0| + \mathrm{e}^{2\pi i/2^k} |1\rangle\langle 1|) \otimes |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mathrm{e}^{2\pi i/2^k} \end{pmatrix} \tag{79}$$

III. The part III reads

$$\mathbb{1} \otimes \hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \tag{80}$$

IV. The part IV reads

$$\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{81}$$

In general, the QFT acts on a quantum state $\left|q^{(2)}\right\rangle$

$$\mathcal{QF}\,|p\rangle = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \mathrm{e}^{\frac{2\pi i}{N} pq} \left|q^{(2)}\right\rangle \tag{82}$$

$q^{(2)}$ is the binary basis of q, which satisfies the following relationship

$$q = \sum_{i=0}^{n-1} q_i^{(2)} 2^i \tag{83}$$

For example, $(1, 0, 1) = 1 \times 2^0 + 0 \times 2^1 + 1 \times 2^2 = 5$. So we can expand

$$\begin{aligned}
\mathcal{QF} \left|p\right\rangle =& \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \exp\left[\frac{2\pi i}{N} p \left(\sum_{i=0}^{n-1} q_i^{(2)} 2^i\right)\right] \left|q^{(2)}\right\rangle \\
=& \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \exp\left[\frac{2\pi i}{N} p \left(q_0^{(2)} + \sum_{i=1}^{n-1} q_i^{(2)} 2^i\right)\right] \left|q^{(2)}\right\rangle \\
=& \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \exp\left[\frac{2\pi i}{N} p \left(0 \times 1 + 2\sum_{i=0}^{n-2} q_i'^{(2)} 2^i\right)\right] \left(\left|0\right\rangle \otimes \left|q'^{(2)}\right\rangle\right) \\
&+ \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \exp\left[\frac{2\pi i}{N} p \left(1 \times 1 + 2\sum_{i=0}^{n-2} q_i'^{(2)} 2^{i-1}\right)\right] \left(\left|1\right\rangle \otimes \left|q'^{(2)}\right\rangle\right) \\
=& \frac{1}{\sqrt{N}} \left(\left|0\right\rangle + \mathrm{e}^{\frac{2\pi i}{N} p \times 1} \left|1\right\rangle\right) \otimes \sum_{q=0}^{N'-1} \mathrm{e}^{\frac{2\pi i}{N'} p q'} \left|q'^{(2)}\right\rangle
\end{aligned} \tag{84}$$

where $N' = 2^{n-1}$. Thus, by performing the same procedure, we obtain the following separable state

$$\frac{1}{\sqrt{N}} \left(\left|0\right\rangle + \mathrm{e}^{\frac{2\pi i}{2^n} p} \left|1\right\rangle\right) \otimes \left(\left|0\right\rangle + \mathrm{e}^{\frac{2\pi i}{2^{n-1}} p} \left|1\right\rangle\right) \otimes \cdots \otimes \left(\left|0\right\rangle + \mathrm{e}^{\pi i p} \left|1\right\rangle\right) \tag{85}$$

and $(\left|0\right\rangle + \mathrm{e}^{\pi i p} \left|1\right\rangle)$ can be achieved by Hadamard gate

$$H \left|p\right\rangle = \frac{1}{\sqrt{2}} (\left|0\right\rangle + \mathrm{e}^{\pi i p} \left|1\right\rangle) \tag{86}$$

The idea of QFT is thus to perform the following actions

1. Initial states: $\left|p_{n-1}\right\rangle \otimes \left|p_{n-2}\right\rangle \otimes \cdots \otimes \left|p_0\right\rangle$
2. Apply Hadamard gate H on p_0: $\left|p_{n-1}\right\rangle \otimes \left|p_{n-2}\right\rangle \otimes \cdots \otimes (\left|0\right\rangle + \mathrm{e}^{\pi i p} \left|1\right\rangle)$

3 Physical Realisation - Trapped Ions

3.1 Di-Vincenzo Criteria

i) Well-defined qubits

ii) Initialisation $|0\rangle|0\rangle\cdots|0\rangle$

iii) Universal set of quantum gates

iv) Measurements of each qubit

v) Sufficiently long coherence times

3.2 Trapped Ion Hamiltonian

The free Hamiltonian is composed of

$$\hat{H}_0 = \underbrace{\frac{\omega_0}{2}\hat{\sigma}_z}_{\text{atomic internal energy}} + \underbrace{\omega_t \hat{a}^\dagger \hat{a}}_{\text{trapped motion energy}} \tag{87}$$

where ω_t is the trap frequency. The interaction between the ion and a laser can be expressed as

$$\hat{H}_I = \Omega_R \hat{\sigma}_x \cos(\omega t - k\hat{x} + \phi) \tag{88}$$

where Ω_R is the coupling strength between the ion and laser, ω is the laser frequency, and $\hat{x} = \sqrt{\hbar/2m\omega_t}(\hat{a} + \hat{a}^\dagger)$ is the position of ion. In the interaction picture[1]

$$\begin{aligned}\hat{H} =& \mathrm{e}^{i\hat{H}_0 t}\hat{H}_I \mathrm{e}^{-i\hat{H}_0 t} \\ =& \frac{1}{2}\left(\hat{\sigma}_- \mathrm{e}^{-i\omega_0 t} + \hat{\sigma}_+ \mathrm{e}^{i\omega_0 t}\right) \\ &\times \left[\Omega_R \mathrm{e}^{i\phi} \exp\left(i\left(\omega t - k\sqrt{\frac{\hbar}{2m\omega_t}}\left(\hat{a}\mathrm{e}^{-i\omega_t t} + \hat{a}^\dagger \mathrm{e}^{i\omega_t t}\right)\right)\right) + \text{h.c.}\right]\end{aligned} \tag{89}$$

Here we introduce the *Lamb-Dicke parameter*

$$\boxed{\eta = k\sqrt{\frac{\hbar}{2m\omega_t}} = \frac{\hbar k}{\sqrt{2m\hbar\omega_t}} = \frac{p_{\text{photon}}}{p_{\text{phonon}}}} \tag{90}$$

Assume $\eta \ll 1$ (which is typically of the order of $1/10$), then

$$\hat{H} \approx \frac{\Omega_R}{2}\left(\hat{\sigma}_- \mathrm{e}^{-i\omega_0 t} + \hat{\sigma}_+ \mathrm{e}^{-\omega_0 t}\right)\left[\mathrm{e}^{-i\omega t}\left(\mathbb{1} - i\eta\left(\hat{a}\mathrm{e}^{-i\omega_t t} + \hat{a}^\dagger \mathrm{e}^{i\omega_t t}\right)\right) + \text{h.c.}\right] \tag{91}$$

for $\phi = 0$. For sufficiently weak driving, after rotating wave approximation (RWA), one obtains the following approximations

[1] $\mathrm{e}^{i\hat{A}\theta}\hat{B}\mathrm{e}^{-i\hat{A}\theta} = \hat{B} + \theta[\hat{A},\hat{B}] + \frac{\theta^2}{2}[\hat{A},[\hat{A},\hat{B}]] + \cdots$.

- Carrier transition $\omega = \omega_0$

$$\hat{H}_{\mathrm{c}} = \frac{\Omega_R}{2}\left(\hat{\sigma}_+ + \hat{\sigma}_-\right) = \frac{\Omega_R}{2}\hat{\sigma}_x \tag{92}$$

- Red sideband $\omega = \omega_0 - \omega_t$

$$\hat{H}_{\mathrm{r}} = -i\eta\frac{\Omega_R}{2}\left(\hat{\sigma}_-\hat{a}^\dagger - \hat{\sigma}_+\hat{a}\right) \tag{93}$$

- Blue sideband $\omega = \omega_0 + \omega_t$

$$\hat{H}_{\mathrm{b}} = -i\eta\frac{\Omega_R}{2}\left(\hat{\sigma}_-\hat{a} - \hat{\sigma}_+\hat{a}^\dagger\right) \tag{94}$$

$\hat{H}$ induces single qubit gates; $\hat{H}_{\mathrm{r}}$ and $\hat{H}_{\mathrm{b}}$ affect the ion and oscillation jointly.

3.3 Cirac-Zoller Gate

Taking $\lambda = -i\eta\Omega\mathrm{e}^{i\phi/2}/2$ and $\phi = \pi/2$, then

$$\hat{H}_{\mathrm{r}} = \lambda\left(\hat{\sigma}_-\hat{a}^\dagger + \hat{\sigma}_+\hat{a}\right) \tag{95}$$

Solving the dynamic equation

$$|g,n\rangle \to \cos\lambda\sqrt{n}t\,|g,n\rangle - i\sin\lambda\sqrt{n}t\,|e,n-1\rangle \tag{96}$$

$$|e,n-1\rangle \to \cos\lambda\sqrt{n}t\,|e,n-1\rangle - i\sin\lambda\sqrt{n}t\,|g,n\rangle \tag{97}$$

where $|g\rangle, |e\rangle$ are ground and excited state and $|n\rangle$ is the n phonon number (trap state).

Lets consider two inonic states and phononic state

i) A laser shining on ion 1 for $\lambda t = \pi/2$.

ii) Another laser shining on ion 2 for $\lambda t = \pi$.

iii) A laser shining on ion 1 for $\lambda t = \pi/2$.

$$\begin{array}{ccccccc}
 & \hat{U}_1 & & \hat{U}_2 & & \hat{U}_1 & \\
|g,g,0\rangle & \to & |g,g,0\rangle & \to & |g,g,0\rangle & \to & |g,g,0\rangle \\
|g,e,0\rangle & \to & |g,e,0\rangle & \to & |g,e,0\rangle & \to & |g,e,0\rangle \\
|e,g,0\rangle & \to & -i\,|g,g,1\rangle & \to & i\,|g,g,1\rangle & \to & |e,g,0\rangle \\
|e,e,0\rangle & \to & -i\,|g,e,1\rangle & \to & -i\,|g,e,1\rangle & \to & -\,|e,e,0\rangle
\end{array}$$

Table 4: Cirac-Zoller Gate

Now we discuss the ground state motion. The average excitation within thermal equilibrium is that

$$\bar{n} = \frac{1}{\mathrm{e}^{\hbar\omega/k_BT} - 1} \tag{98}$$

The frequency $\omega \sim$MHz, and the room temperature $T \sim 300$K, so the average excitation in room temperature $\bar{n} \sim 10^7$. So we need to cool the ions down to $T \sim 10^{-5}$K.

4 Decoherence and Quantum Error Correction

4.1 Density Matrices

If a pure state $|\Psi_j\rangle$ is prepared with probability p_j, an expectation value of an observable $\hat{A}$ can be calculated

$$\begin{aligned}
\langle\hat{A}\rangle &= \sum_j p_j \langle\Psi_j|\,\hat{A}\,|\Psi_j\rangle \\
&= \sum_{j,k} p_j \langle\Psi_j|\,\hat{A}\,|k\rangle\langle k|\Psi_j\rangle \qquad \left(\text{when } \sum_k |k\rangle\langle k| = \mathbb{1}\right) \\
&= \sum_{j,k} p_j \langle k|\Psi_j\rangle\langle\Psi_j|\,\hat{A}\,|k\rangle \\
&= \sum_k \langle k| \sum_j p_j |\Psi_j\rangle\langle\Psi_j|\,\hat{A}\,|k\rangle \\
&= \mathrm{Tr}\left(\hat{\rho}\hat{A}\right)
\end{aligned} \tag{99}$$

with the density matrix

$$\hat{\rho} = \sum_j p_j |\Psi_j\rangle\langle\Psi_j| \tag{100}$$

The properties of density matrix

1. $\hat{\rho}$ is hermitian: $\hat{\rho} = \hat{\rho}^\dagger$
2. $\hat{\rho}$ has unit trace: $\mathrm{Tr}\,\hat{\rho} = 1$ $(\sum_j p_j = 1)$
3. $\hat{\rho}$ is positive semi-definite

$$\langle\phi|\,\hat{\rho}\,|\phi\rangle = \sum_j p_j \langle\phi|\Psi_j\rangle\langle\Psi_j|\phi\rangle = \sum_j p_j |\langle\phi|\Psi_j\rangle|^2 \geq 0 \tag{101}$$

4.1.1 Reduced States