Notes

Imperial College London

Department of Physics

# Quantum Information

*Author:*
Chen Huang

*Email:*
chen.huang23@imperial.ac.uk

Date: May 30, 2024

# Contents


**1 Elements of quantum mechanics and quantum information 3**
1.1 Tools from quantum mechanics (I) . . . 3
1.1.1 States and operators . . . 3
1.1.2 Dynamics . . . 3
1.1.3 Measurement . . . 4
1.2 Quantum key distribution - BB84 . . . 4
1.3 No-cloning theorem . . . 5
1.4 Tools from quantum mechanics (II) . . . 6
1.4.1 Bell's inequality . . . 6
1.4.2 Partial trace . . . 6

**2 Quantum algorithms 8**
2.1 Quantum interferometers . . . 8
2.2 Basic gate operations (I) . . . 8
2.3 Deutsch-Jozsa algorithm . . . 9
2.4 Basic gate operations (II) . . . 11
2.4.1 Controlled-$Z$ gate and controlled-unitary gate . . . 11
2.4.2 Three qubits - controlled-controlled-unitary gate . . . 11
2.4.3 NOT gate . . . 12
2.4.4 SWAP gate . . . 13
2.5 Grover's algorithm (quantum search algorithm) . . . 13
2.6 Quantum Fourier transform . . . 14
2.6.1 Properties of quantum Fourier transform . . . 15
2.6.2 Quantum circuit of quantum Fourier transform . . . 15

**3 Physical realisation - trapped ions 17**
3.1 DiVincenzo criteria . . . 17
3.2 Trapped-ion Hamiltonian . . . 17
3.3 Cirac-Zoller gate . . . 18

**4 Decoherence and quantum error correction 20**
4.1 Density matrices . . . 20
4.1.1 Reduced states . . . 20
4.1.2 Population and coherence . . . 21
4.1.3 Pure states and mixed states . . . 21
4.1.4 Expansion in operator basis . . . 22
4.2 Open quantum systems and decoherence . . . 22
4.2.1 System-environment interaction . . . 22
4.2.2 Quantum channels and open quantum dynamics . . . 23
4.2.3 Properties of quantum channels . . . 24
4.2.4 Exemplary quantum channels . . . 24
4.2.5 Generalised measurements . . . 26
4.3 Error correction . . . 27
4.3.1 Classical error correction . . . 27

4.3.2 Quantum error correction . . . . . 27
4.4 Stabiliser formalism . . . . . 29
4.4.1 Stabilisers . . . . . 29
4.4.2 Error measurements . . . . . 30
4.4.3 Preparation of eigenstates for a Pauli group operator . . . . . 30

**5 Properties and applications of entangled states** **32**
5.1 Definition and measures of entanglement . . . . . 32
5.1.1 Pure states . . . . . 32
5.1.2 Mixed state entanglement . . . . . 33
5.1.3 Multipartite entanglement . . . . . 34
5.2 Schmidt decomposition . . . . . 34
5.3 Quantum teleportation . . . . . 35
5.4 Super dense coding . . . . . 36
5.5 QKD example: Ekert 92 . . . . . 36
5.6 Bell measurements . . . . . 37
5.7 Entanglement distillation . . . . . 37

# 1 Elements of quantum mechanics and quantum information

## 1.1 Tools from quantum mechanics (I)

### 1.1.1 States and operators

The Hamiltonian for quantum harmonic oscillator

$$\hat{H} = \omega \hat{a}^\dagger \hat{a}, \tag{1}$$

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

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

we can express the operator $\hat{a}$ as

$$\hat{a} = \sum_{m,n} |m\rangle \langle m| \hat{a} |n\rangle \langle n| = \sum_{m,n} \sqrt{n} |m\rangle \langle m|n-1\rangle \langle n| = \sum_{n} \sqrt{n+1} |n\rangle \langle n+1|. \tag{3}$$

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

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

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

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

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

$$[\hat{\sigma}_\alpha, \hat{\sigma}_\beta] = 2i\varepsilon_{\alpha\beta\gamma}\hat{\sigma}_\gamma, \quad \{\hat{\sigma}_\alpha, \hat{\sigma}_\beta\} = \delta_{\alpha\beta}\mathbb{1}. \tag{6}$$

### 1.1.2 Dynamics

The Schrödinger equation can be written as

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

with a time-independent Hamiltonian, one obtains that

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

where $\hat{U}(t, t_0) = \exp\left[-i\hat{H}(t-t_0)\right]$ is called the **time-evolution operator** or **propagator**, which has several key properties:

1. **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

$$\hat{U} = \hat{U} \sum_j |\Psi_j\rangle \langle\Psi_j| = \sum_j \mathrm{e}^{-i\omega_j(t-t_0)} |\Psi_j\rangle \langle\Psi_j| . \tag{9}$$

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

$$\hat{U}(t,t_0)\hat{U}^\dagger(t,t_0) = \hat{U}^\dagger(t,t_0)\hat{U}(t,t_0) = \mathbb{1}, \tag{10}$$

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

3. **The propagator (as an 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

$$\hat{U}(t,t_0) = \hat{U}(t,t_0) \sum_j |\Psi_j(t_0)\rangle \langle\Psi_j(t_0)| = \sum_j |\Psi_j(t)\rangle \langle\Psi_j(t_0)| . \tag{11}$$

   We thus obtain

$$i\frac{\mathrm{d}}{\mathrm{d}t}\hat{U} = \sum_j i\frac{\mathrm{d}}{\mathrm{d}t} |\Psi_j(t)\rangle \langle\Psi_j(t_0)| = \sum_j \hat{H} |\Psi_j(t)\rangle \langle\Psi_j(t_0)| = \hat{H}\hat{U}. \tag{12}$$

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

$$\hat{P}_0 |\psi\rangle = \hat{P}_0(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle , \tag{13}$$

$$\hat{P}_1 |\psi\rangle = \hat{P}_1(\alpha|0\rangle + \beta|1\rangle) = \beta|1\rangle , \tag{14}$$

with the probabilities

$$p_0 = \langle\psi| \hat{P}_0 |\psi\rangle = |\alpha|^2, \quad p_1 = \langle\psi| \hat{P}_1 |\psi\rangle = |\beta|^2. \tag{15}$$

The condition $\sum_i p_i = \langle\psi| \sum_i \hat{P}_i |\psi\rangle = 1$, or $\sum_i \hat{P}_i = \mathbb{1}$, 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. The four quantum states used in BB84 are:

- $|\mathrm{H}\rangle = |0\rangle$ and $|\mathrm{V}\rangle = |1\rangle$ in the rectilinear basis ($+$).
- $|\mathrm{D}\rangle = |+\rangle$ and $|\mathrm{A}\rangle = |-\rangle$ in the diagonal basis ($\times$).

1. **Sending**: Alice randomly selects a string of bits and a string of basis ($+$ or $\times$) of equal length and send photons.
2. **Receiving**: Bob randomly chooses a basis for each photon to measure its polarisation. 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 polarisation. If he doesn't guess correctly, he will get a random bit.
3. **Compare**: Bob tells Alice about the bases he used to measure each photon. Alice informs Bob of the bases that 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 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| Alice's encoding basis | $\times$ | $+$ | $\times$ | $+$ | $+$ | $+$ | $+$ | $+$ | $\times$ | $\times$ | $+$ | $\times$ | $\times$ |
| Photons Alice sends | D | V | A | H | V | V | H | H | A | D | V | A | D |
| Random measurement basis | $+$ | $\times$ | $\times$ | $+$ | $+$ | $\times$ | $\times$ | $+$ | $\times$ | $+$ | $\times$ | $\times$ | $\times$ |
| Bits received by Bob | H | A | A | H | V | D | A | H | A | H | D | A | D |
| The common basis | | | ✓ | ✓ | ✓ | | | ✓ | ✓ | | | ✓ | ✓ |
| Shifted key | | | 1 | 0 | 1 | | | 0 | 1 | | | 1 | 0 |

**Table 1:** The 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 exact state) and a second qubit in the $|0\rangle$ state. We would like to find a gate such that

$$\hat{U}\,|\Psi\rangle\,|0\rangle = |\Psi\rangle\,|\Psi\rangle\,, \quad \forall\,|\Psi\rangle\,. \tag{16}$$

This implies

$$\hat{U}\,|0\rangle\,|0\rangle = |0\rangle\,|0\rangle\,, \quad \hat{U}\,|1\rangle\,|0\rangle = |1\rangle\,|1\rangle\,. \tag{17}$$

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

$$\hat{U}\,(\alpha\,|0\rangle + \beta\,|1\rangle)\,|0\rangle = \alpha\,|0\rangle\,|0\rangle + \beta\,|1\rangle\,|1\rangle\,, \tag{18}$$

whereas we would have wanted to obtain

$$(\alpha\,|0\rangle + \beta\,|1\rangle)\,(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha^2\,|0\rangle\,|0\rangle + \alpha\beta(|0\rangle\,|1\rangle + |1\rangle\,|0\rangle) + \beta^2\,|1\rangle\,|1\rangle\,, \tag{19}$$

in a cloning process. In the above example, the cloning process works if either $\alpha$ or $\beta$ vanishes; that is, it only works for the two orthogonal basis states for which it is defined.

## 1.4 Tools from quantum mechanics (II)

In this section, we consider how to describe a quantum system of two subsystems – bipartite system.

### 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

$$A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 = 2, \tag{20}$$

and the average

$$\langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle \leq 2. \tag{21}$$

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,

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{22}$$

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

$$\begin{aligned}\langle \hat{A}_0 \otimes \hat{B}_0\rangle &= \langle\psi| \hat{A}_0 \otimes \hat{B}_0 |\psi\rangle \\ &= -\frac{1}{2\sqrt{2}}(\langle 01| - \langle 10|)\hat{\sigma}_z \otimes (\hat{\sigma}_x + \hat{\sigma}_z)(|01\rangle - |10\rangle) \\ &= -\frac{1}{2\sqrt{2}}(\langle 01| - \langle 10|)\,(|00\rangle - |01\rangle + |11\rangle + |10\rangle) = \frac{1}{\sqrt{2}}.\end{aligned} \tag{23}$$

Similarly, we can find

$$\langle \hat{A}_0 \otimes \hat{B}_0\rangle = \langle \hat{A}_0 \otimes \hat{B}_1\rangle = \langle \hat{A}_1 \otimes \hat{B}_0\rangle = -\langle \hat{A}_1 \otimes \hat{B}_1\rangle = \frac{1}{\sqrt{2}}, \tag{24}$$

and the Bell's expectation value is

$$\langle \hat{A}_0 \otimes \hat{B}_0\rangle + \langle \hat{A}_0 \otimes \hat{B}_1\rangle + \langle \hat{A}_1 \otimes \hat{B}_0\rangle - \langle \hat{A}_1 \otimes \hat{B}_1\rangle = 2\sqrt{2}, \tag{25}$$

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

### 1.4.2 Partial trace

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

$$\mathrm{Tr}\,\hat{A} = \sum_i \langle i| \hat{A} |i\rangle\,, \tag{26}$$

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

$$\mathrm{Tr}_b \left( \hat{A} \otimes \hat{B} \right) = \hat{A} \,\mathrm{Tr}_b \,\hat{B}, \quad \mathrm{Tr}_a \left( \hat{A} \otimes \hat{B} \right) = \hat{B} \,\mathrm{Tr}_a \,\hat{A}. \tag{27}$$

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

$$\begin{aligned}
\mathrm{Tr}\left( \left( \hat{A} \otimes \mathbb{I} \right) \hat{C} \right) &= \sum_{ij} \langle i|_a \otimes \langle j|_b \left( \left( \hat{A} \otimes \mathbb{I} \right) \hat{C} \right) |i\rangle_a \otimes |j\rangle_b \\
&= \sum_{ij} \left( \langle i|_a \hat{A} \right) \otimes \langle j|_b \hat{C} \left( |i\rangle_a \otimes |j\rangle_b \right) \\
&= \sum_{i} \langle i|_a \hat{A} \left( \sum_{j} \langle j|_b \hat{C} \,|j\rangle_b \right) |i\rangle_a \\
&= \mathrm{Tr}_a \left( \hat{A} \,\mathrm{Tr}_b \,\hat{C} \right).
\end{aligned} \tag{28}$$

# 2 Quantum algorithms

## 2.1 Quantum interferometers

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

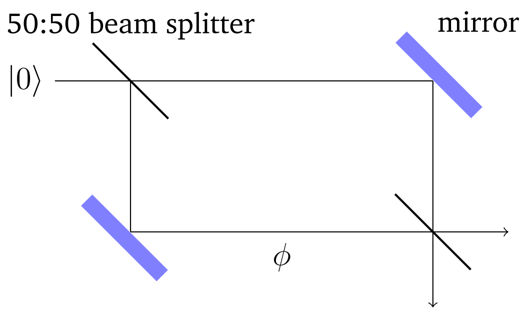



**Figure 1:** The Mach-Zehnder interferometer.

The Mach-Zehnder interferometer is described by

$$\underbrace{\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}}_{\text{2nd bs}}\underbrace{\begin{pmatrix}1 & 0\\ 0 & e^{i\phi}\end{pmatrix}}_{\text{phase shift}}\underbrace{\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}}_{\text{1st bs}}\underbrace{\begin{pmatrix}1\\ 0\end{pmatrix}}_{\text{input}} = e^{-i\frac{\pi}{4}\hat{\sigma}_y}\hat{R}_\phi e^{i\frac{\pi}{4}\hat{\sigma}_y}|0\rangle\,, \tag{29}$$

where the phase shift is described by the rotation

$$\hat{R}_\phi = \begin{pmatrix}1 & 0\\ 0 & e^{i\phi}\end{pmatrix} = e^{i\phi/2}\begin{pmatrix}e^{-i\phi/2} & 0\\ 0 & e^{i\phi/2}\end{pmatrix}, \tag{30}$$

and the beam splitter is described by

$$\hat{B} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix} = \frac{1}{\sqrt{2}}(\mathbb{1}+\hat{\sigma}_y) = e^{i\frac{\pi}{4}\hat{\sigma}_y}. \tag{31}$$

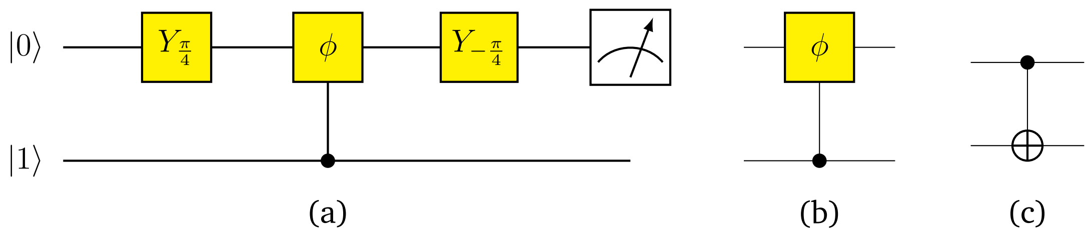



**Figure 2:** (a) For the input state $|0\rangle$, the quantum circuit for the Macj-Zehnder interferometer. (b) The controlled-phase gate. (c) The controlled-not (CNOT) gate.

## 2.2 Basic gate operations (I)

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

$$\hat{X} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \quad \hat{Y} = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}, \quad \hat{Z} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}. \tag{32}$$

- **Hadamard gate**
$$\hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} . \tag{33}$$

- **Controlled-phase gate**
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix} . \tag{34}$$

- **Controlled-NOT gate**
$$\begin{aligned} \hat{U}_c &= |00\rangle \langle 00| + |01\rangle \langle 01| + |10\rangle \langle 11| + |11\rangle \langle 10| \\ &= |0\rangle \langle 0| \otimes \mathbb{1} + |1\rangle \langle 1| \otimes \hat{\sigma}_x , \end{aligned} \tag{35}$$

  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

$$|i\rangle \otimes |j\rangle \to \hat{U}_0 |ij\rangle = |i\rangle \otimes |j \oplus f(i)\rangle , \tag{36}$$

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

$$\hat{U}_0 |00\rangle = |0 f(0)\rangle \,, \tag{37}$$
$$\hat{U}_0 |01\rangle = |0 \overline{f(0)}\rangle, \tag{38}$$
$$\hat{U}_0 |10\rangle = |1 f(1)\rangle \,, \tag{39}$$
$$\hat{U}_0 |11\rangle = |1 \overline{f(1)}\rangle. \tag{40}$$

With the initial state

$$|+\rangle \otimes |-\rangle = \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right), \tag{41}$$

one obtains

$$\hat{U}_0 |+\rangle \otimes |-\rangle = \frac{1}{2}\left(|0 f(0)\rangle - |0\overline{f(0)}\rangle + |1 f(1)\rangle - |1\overline{f(1)}\rangle\right) = |\Psi_0\rangle \,. \tag{42}$$

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

$$|\Psi_0\rangle = \frac{1}{2}\left[(|0\rangle + |1\rangle) \otimes |f(0)\rangle - (|0\rangle + |1\rangle) \otimes |\overline{f(0)}\rangle\right] = |+\rangle \otimes \frac{|f(0)\rangle - |\overline{f(0)}\rangle}{\sqrt{2}}. \tag{43}$$

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

$$|\Psi_0\rangle = \frac{1}{2}\left[(|0\rangle - |1\rangle) \otimes |f(0)\rangle - (|0\rangle - |1\rangle) \otimes |\overline{f(0)}\rangle\right] = |-\rangle \otimes \frac{|f(0)\rangle - |f(1)\rangle}{\sqrt{2}}. \tag{44}$$

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. Preparation 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 $\hat{H} \otimes \hat{H}\hat{\sigma}_x$)
$$\left[\exp\left(-i\frac{\pi}{4}\hat{\sigma}_y\right) \otimes \exp\left(i\frac{\pi}{4}\hat{\sigma}_y\right)\right] (|0\rangle \otimes |0\rangle) = |+\rangle \otimes |-\rangle \,. \tag{45}$$
3. Query to the oracle
   - If $f(0) = f(1)$, then the first qubit is in $|+\rangle$.
   - If $f(0) = \overline{f(1)}$, 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.

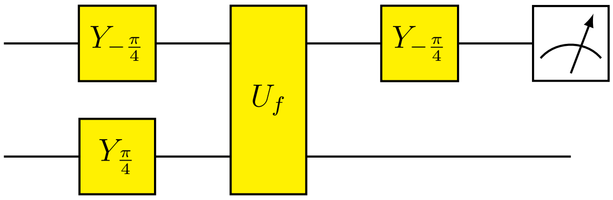



**Figure 3:** The quantum circuit of the Deutsch-Jozsa algorithm.

## 2.4 Basic gate operations (II)

### 2.4.1 Controlled-$Z$ gate and controlled-unitary gate

The Controlled-$Z$ gate

$$\hat{U}_{cz} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \hat{\sigma}_z, \tag{46}$$

which is similar to a CNOT gate which reads

$$\hat{U}_c = \hat{U}_{cx} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \hat{\sigma}_x. \tag{47}$$

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:

$$\begin{aligned}
\hat{U}_{cz} &= |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \exp\left(i\frac{\pi}{4}\hat{\sigma}_y\right)\hat{\sigma}_x \exp\left(-i\frac{\pi}{4}\hat{\sigma}_y\right) \\
&= \left[\mathbb{1} \otimes \exp\left(i\frac{\pi}{4}\hat{\sigma}_y\right)\right] \left(|0\rangle\langle 0| \otimes \mathbb{1}\right) \left[\mathbb{1} \otimes \exp\left(-i\frac{\pi}{4}\hat{\sigma}_y\right)\right] \\
&\quad + \left[\mathbb{1} \otimes \exp\left(i\frac{\pi}{4}\hat{\sigma}_y\right)\right] \left(|1\rangle\langle 1| \otimes \hat{\sigma}_x\right) \left[\mathbb{1} \otimes \exp\left(-i\frac{\pi}{4}\hat{\sigma}_y\right)\right] \\
&= \left[\mathbb{1} \otimes \exp\left(i\frac{\pi}{4}\hat{\sigma}_y\right)\right] \hat{U}_c \left[\mathbb{1} \otimes \exp\left(-i\frac{\pi}{4}\hat{\sigma}_y\right)\right].
\end{aligned} \tag{48}$$

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

$$\hat{U}_{cu} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \hat{U}. \tag{49}$$

**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 $\hat{U}_1 \otimes \hat{U}_2$.

### 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

$$\left(\mathbb{1} \otimes \mathbb{1} - |1\rangle\langle 1| \otimes |1\rangle\langle 1|\right) \otimes \mathbb{1} + |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes \hat{U}. \tag{50}$$

The controlled-not gate operation can be written in

$$|i\rangle|j\rangle \to |i\rangle|i \oplus j\rangle, \quad \text{or} \quad \text{target} \to \text{target} \oplus \text{control}. \tag{51}$$

The controlled-unitary gate operation can be written in

$$|i\rangle|j\rangle \to |i\rangle\hat{U}^i|j\rangle. \tag{52}$$

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

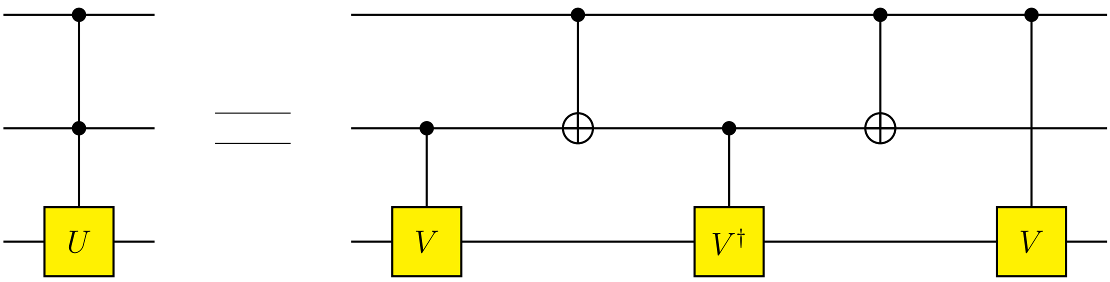



**Figure 4:** A controlled-controlled-$U$ operation can be realised in terms of CNOT and controlled-$V$ operations for $\hat{U} = \hat{V}^2$

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

$$\hat{U}\,|00\rangle\otimes|\phi\rangle = |00\rangle\otimes|\phi\rangle\,, \tag{53}$$
$$\hat{U}\,|01\rangle\otimes|\phi\rangle = |01\rangle\otimes|\phi\rangle\,, \tag{54}$$
$$\hat{U}\,|10\rangle\otimes|\phi\rangle = |10\rangle\otimes|\phi\rangle\,, \tag{55}$$
$$\hat{U}\,|11\rangle\otimes|\phi\rangle = |11\rangle\otimes\hat{U}\,|\phi\rangle\,. \tag{56}$$

### 2.4.3 NOT gate

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

$$\hat{\sigma}_x\,|0\rangle = |1\rangle\,,\quad \hat{\sigma}_x\,|1\rangle = |0\rangle\,. \tag{57}$$

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

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{58}$$

then

$$\mathrm{NOT}\,|\Psi\rangle = \alpha\,|1\rangle + \beta\,|0\rangle = |\Psi'\rangle\,. \tag{59}$$

As

$$\langle\Psi'|\Psi\rangle = (\alpha^*\,\langle 1| + \beta^*\,\langle 0|)\,(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha^*\beta + \beta^*\alpha \neq 0, \tag{60}$$

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.
We can also define $\sqrt{\mathrm{NOT}}$ to satisfy $\sqrt{\mathrm{NOT}}\sqrt{\mathrm{NOT}} = \mathrm{NOT}$:

$$\sqrt{\mathrm{NOT}} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}. \tag{61}$$

### 2.4.4 SWAP gate

The SWAP gate is to swap two qubits

$$\text{SWAP}\,|\Psi\rangle\,|\Phi\rangle = |\Phi\rangle\,|\Psi\rangle\,, \tag{62}$$

with

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{63}$$

and

$$\sqrt{\text{SWAP}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1+i) & \frac{1}{2}(1-i) & 0 \\ 0 & \frac{1}{2}(1-i) & \frac{1}{2}(1+i) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{64}$$

## 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 $|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle = |0\rangle^{\otimes n}$.

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

$$|s\rangle = \hat{H}\,|0\rangle \otimes \cdots \otimes \hat{H}\,|0\rangle \otimes \hat{H}\,|0\rangle = |+\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle\,. \tag{65}$$

3. Apply $\hat{U} = \mathbb{1} - 2\,|q\rangle\,\langle q|$ to distinguish the basis state $|q\rangle$ from all other $N-1$ basis states $|i\rangle$

$$\hat{U}\,|s\rangle = (\mathbb{1} - 2\,|q\rangle\,\langle q|)\,|s\rangle = |s\rangle - 2\,|q\rangle\,\langle q|\,\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle = |s\rangle - \frac{2}{\sqrt{N}}\,|q\rangle\,. \tag{66}$$

4. Apply $\hat{V} = 2\,|s\rangle\,\langle s| - \mathbb{1}$

$$\begin{aligned} \hat{V}\hat{U}\,|s\rangle =& (2\,|s\rangle\,\langle s| - \mathbb{1})\left(|s\rangle - \frac{2}{\sqrt{N}}\,|q\rangle\right) \\ =& 2\,|s\rangle - |s\rangle - \frac{4}{\sqrt{N}}\,|s\rangle\,\langle s|q\rangle + \frac{2}{\sqrt{N}}\,|q\rangle \\ =& |s\rangle - \frac{4}{\sqrt{N}}\,|s\rangle\,\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \langle i|q\rangle + \frac{2}{\sqrt{N}}\,|q\rangle \\ =& \frac{N-4}{N}\,|s\rangle + \frac{2}{\sqrt{N}}\,|q\rangle \\ =& \frac{N-4}{N\sqrt{N}} \sum_{i\neq q}^{N-1} |i\rangle + \left(\frac{N-4}{N\sqrt{N}} + \frac{2}{\sqrt{N}}\right)|q\rangle\,. \end{aligned} \tag{67}$$

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

$$\left(\frac{N-4}{N\sqrt{N}} + \frac{2}{\sqrt{N}}\right)^2 > \frac{1}{N}, \quad \text{for } N > 2. \tag{68}$$

5. Repeat the process 3 and 4 to increase the probability of finding the system in $|q\rangle$.

## 2.6 Quantum Fourier transform

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

$$\boxed{\mathcal{QF}\,|\Phi_p\rangle = \frac{1}{\sqrt{N}}\sum_{q=0}^{N-1} \mathrm{e}^{\frac{2\pi i}{N}pq}\,|\Phi_q\rangle\,.} \tag{69}$$

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

- **A single qubit**

$$\mathcal{QF}\,|p\rangle = \frac{1}{\sqrt{2}}\sum_{q=0}^{1} \mathrm{e}^{\frac{2\pi i}{N}pq}\,|q\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + \mathrm{e}^{i\pi p}\,|1\rangle\big)\,. \tag{70}$$

This is also know as Hadamard gate, with

$$\mathcal{QF}\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle\,, \tag{71}$$

$$\mathcal{QF}\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle\,. \tag{72}$$

- **Many qubits**

$$\mathcal{QF}_N = \frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix}, \tag{73}$$

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

$$\begin{aligned} |\Psi\rangle =& a_0\,|0\rangle + a_1\,|1\rangle + \cdots + a_{N-1}\,|N-1\rangle \\ =& a_0\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix} + a_1\begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix} + \cdots + a_{N-1}\begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix} = \begin{pmatrix}a_0\\a_1\\\vdots\\a_{N-1}\end{pmatrix}. \end{aligned} \tag{74}$$

- **Two qubits**

$$\mathcal{QF}_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}. \tag{75}$$

We have some examples

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

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

### 2.6.1 Properties of quantum Fourier transform

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

$$\frac{1}{N}\sum_{n=0}^{N-1} \omega^{ni}\omega^{nj*} = \frac{1}{N}\sum_{n=0}^{N-1} (\omega^{i-j})^n = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases} \tag{76}$$

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

3. **Period / wave length relationship**.

### 2.6.2 Quantum circuit of quantum Fourier transform

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

1. The part I of the circuit reads

$$\hat{H} \otimes \mathbb{1} = \frac{1}{\sqrt{2}}\begin{pmatrix} \mathbb{1} & \mathbb{1} \\ \mathbb{1} & -\mathbb{1} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}. \tag{77}$$

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

$$\mathbb{1} \otimes |0\rangle\langle 0| + (|0\rangle\langle 0| + \mathrm{e}^{2\pi i/2^k}\,|1\rangle\langle 1|) \otimes |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mathrm{e}^{2\pi i/2^k} \end{pmatrix}. \tag{78}$$

3. The part III reads

$$\mathbb{1} \otimes \hat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}. \tag{79}$$

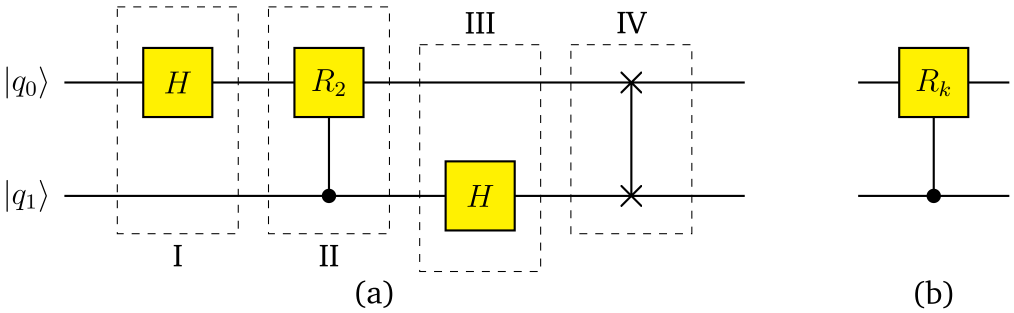



**Figure 5:** (a) The quantum circuit for quantum Fourier transform. (b) Part II of circuit (a).

4. The part IV reads

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{80}$$

In general QFT can be decomposed as:

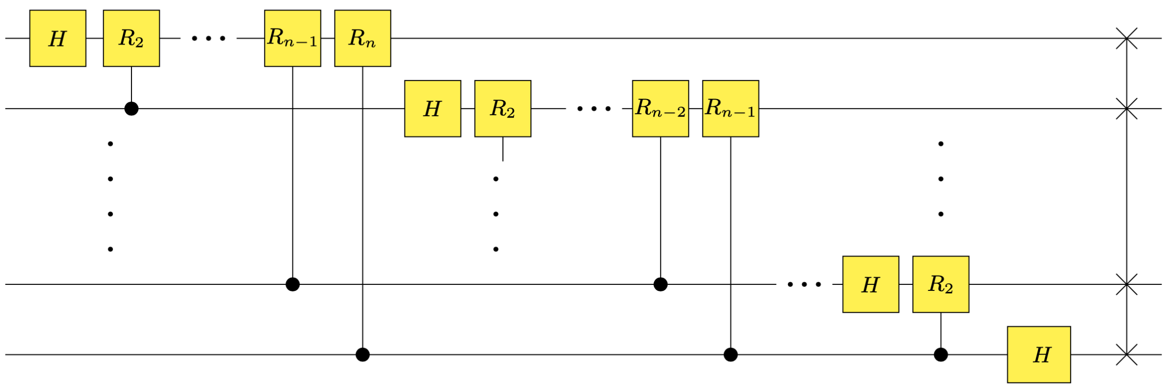



**Figure 6:** The general QFT circuits.

# 3 Physical realisation - trapped ions

## 3.1 DiVincenzo criteria

DiVincenzo wrote that in order to realise a quantum computer a physical system has to satisfy the following conditions:

1. Well-defined qubits.
2. Initialisation $|0\rangle |0\rangle \cdots |0\rangle$.
3. Universal set of quantum gates.
4. Measurements of each qubit.
5. Sufficiently long coherence times.

## 3.2 Trapped-ion Hamiltonian

The free Hamiltonian is composed of

$$\hat{H}_0 = \underbrace{\frac{\omega_0}{2}\hat{\sigma}_z}_{\text{atomic internal energy}} + \underbrace{\omega_t \hat{a}^\dagger \hat{a}}_{\text{trapped motion energy}}, \tag{81}$$

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

$$\hat{H}_I = \Omega_R \hat{\sigma}_x \cos(\omega t - k\hat{x} + \phi), \tag{82}$$

where $\Omega_R$ is the coupling strength between the ion and laser, $\omega$ 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]

$$\hat{H} = \hat{U}_0^\dagger \hat{H}_I \hat{U}_0 = \frac{1}{2}\left(\hat{\sigma}_- \mathrm{e}^{-i\omega_0 t} + \hat{\sigma}_+ \mathrm{e}^{i\omega_0 t}\right)\left(\Omega_R \mathrm{e}^{i\phi} \mathrm{e}^{i\left(\omega t - \eta\left(\hat{a}\mathrm{e}^{-i\omega_t t} + \hat{a}^\dagger \mathrm{e}^{i\omega_t t}\right)\right)} + \text{h.c.}\right). \tag{83}$$

Here we introduce the **Lamb-Dicke parameter**

$$\boxed{\eta = k\sqrt{\frac{\hbar}{2m\omega_t}} = \frac{\hbar k}{\sqrt{2m\hbar\omega_t}} = \frac{p_{\text{photon}}}{p_{\text{phonon}}}.} \tag{84}$$

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

$$\hat{H} \simeq \frac{\Omega_R}{2}\left(\hat{\sigma}_- \mathrm{e}^{-i\omega_0 t} + \hat{\sigma}_+ \mathrm{e}^{-\omega_0 t}\right)\left[\mathrm{e}^{i\omega t}\left(\mathbb{1} - i\eta\left(\hat{a}\mathrm{e}^{-i\omega_t t} + \hat{a}^\dagger \mathrm{e}^{i\omega_t t}\right)\right) + \text{h.c.}\right], \tag{85}$$

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

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

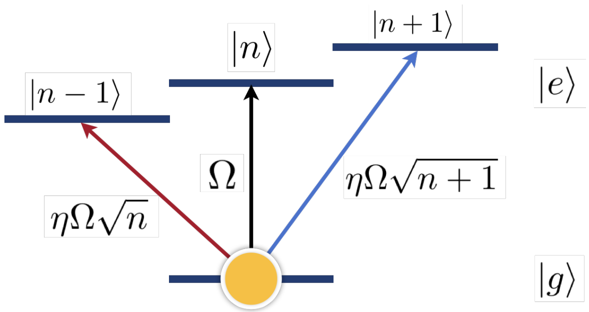



**Figure 7:** Trapped ion transitions.

- Carrier transition $\omega = \omega_0$

$$\hat{H} \simeq \hat{H}_\mathrm{c} = \frac{\Omega_R}{2}\left(\hat{\sigma}_+ + \hat{\sigma}_-\right) = \frac{\Omega_R}{2}\hat{\sigma}_x. \tag{86}$$

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

$$\hat{H} \simeq \hat{H}_\mathrm{r} = -i\eta\frac{\Omega_R}{2}\left(\hat{\sigma}_-\hat{a}^\dagger - \hat{\sigma}_+\hat{a}\right). \tag{87}$$

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

$$\hat{H} \simeq \hat{H}_\mathrm{b} = -i\eta\frac{\Omega_R}{2}\left(\hat{\sigma}_-\hat{a} - \hat{\sigma}_+\hat{a}^\dagger\right). \tag{88}$$

$\hat{H}$ 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 $\lambda = -i\eta\frac{\Omega_R}{2}e^{i\phi}$ and $\phi = \pi/2$, then

$$\hat{H}_\mathrm{r} = \lambda\left(\hat{\sigma}_-\hat{a}^\dagger + \hat{\sigma}_+\hat{a}\right). \tag{89}$$

Solving the dynamic equation under the Hamiltonian above

$$|g,n\rangle \to \cos\lambda\sqrt{n}t\,|g,n\rangle - i\sin\lambda\sqrt{n}t\,|e,n-1\rangle\,, \tag{90}$$
$$|e,n-1\rangle \to \cos\lambda\sqrt{n}t\,|e,n-1\rangle - i\sin\lambda\sqrt{n}t\,|g,n\rangle\,, \tag{91}$$

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

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

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

**Table 4:** Cirac-Zoller Gate

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

$$\bar{n} = \frac{1}{\mathrm{e}^{\hbar\omega/k_B T} - 1}. \tag{92}$$

The frequency $\omega$ ~MHz, and the room temperature $T \sim 300$K, so the average excitation in room temperature $\bar{n} \sim 10^7$. 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

$$\begin{aligned}\langle\hat{A}\rangle &= \sum_j p_j \langle\Psi_j|\,\hat{A}\,|\Psi_j\rangle = \sum_{j,k} p_j \langle\Psi_j|\,\hat{A}\,|k\rangle\langle k|\Psi_j\rangle = \sum_{j,k} p_j \langle k|\Psi_j\rangle\langle\Psi_j|\,\hat{A}\,|k\rangle \\ &= \sum_k \langle k|\left(\sum_j p_j\,|\Psi_j\rangle\langle\Psi_j|\right)\hat{A}\,|k\rangle = \mathrm{Tr}\Big(\hat{\rho}\hat{A}\Big),\end{aligned} \tag{93}$$

with the density matrix

$$\hat{\rho} = \sum_j p_j\,|\Psi_j\rangle\langle\Psi_j|\,. \tag{94}$$

The properties of density matrix are

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:

$$\langle\phi|\,\hat{\rho}\,|\phi\rangle = \sum_j p_j\langle\phi|\Psi_j\rangle\langle\Psi_j|\phi\rangle = \sum_j p_j|\,\langle\phi|\Psi_j\rangle\,|^2 \geq 0. \tag{95}$$

### 4.1.1 Reduced states

Let's consider a two-body system

$$|\Psi\rangle = \sum_{ij}\Psi_{ij}\,|\varphi_i\rangle\otimes|\phi_j\rangle\,. \tag{96}$$

For the observable $\hat{A} = \hat{O}\otimes\mathbb{1}$, the expectation value can be calculated

$$\langle\hat{A}\rangle = \langle\Psi|\,\hat{O}\otimes\mathbb{1}\,|\Psi\rangle = \mathrm{Tr}\Big(\hat{O}\otimes\mathbb{1}\,|\Psi\rangle\langle\Psi|\Big) = \mathrm{Tr}\Big(\hat{O}\,\mathrm{Tr}_2\,|\Psi\rangle\langle\Psi|\Big) = \mathrm{Tr}\Big(\hat{O}\hat{\rho}_1\Big), \tag{97}$$

where the $\hat{\rho}_1$ is the **reduced density matrix** for system 1

$$\hat{\rho}_1 = \mathrm{Tr}_2\,|\Psi\rangle\langle\Psi| = \sum_p\langle\phi_p|\Psi\rangle\langle\Psi|\phi_p\rangle = \sum_{ijp}\Psi_{ip}\Psi^*_{jp}\,|\psi_i\rangle\langle\psi_j|\,. \tag{98}$$

The reduced density matrix is (i) Hermitian, (ii) positive semi-definite, and (3) has unit trace $\mathrm{Tr}\,\hat{\rho} = 1$.

### 4.1.2 Population and coherence

Consider the initial state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, the density matrix is

$$\hat{\rho}(0) = |+\rangle\langle+| = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + |0\rangle\langle 1| + |1\rangle\langle 0|). \tag{99}$$

The measurements on $\{|0\rangle, |1\rangle\}$ basis show

$$\langle 0|\hat{\rho}(0)|0\rangle = \frac{1}{2}, \quad \langle 1|\hat{\rho}(0)|1\rangle = \frac{1}{2}. \tag{100}$$

Recall the dynamics $\hat{U}|+\rangle$ with $\hat{U} = \mathrm{e}^{-i\omega\hat{\sigma}_z t/2}$ from the Ramsey scheme, the density operator becomes

$$\begin{aligned}\rho(t) = \hat{U}\hat{\rho}(0)\hat{U}^\dagger =& \frac{1}{2}\left(\hat{U}|0\rangle\langle 0|\hat{U}^\dagger + \hat{U}|1\rangle\langle 1|\hat{U}^\dagger + \hat{U}|0\rangle\langle 1|\hat{U}^\dagger + \hat{U}|1\rangle\langle 0|\hat{U}^\dagger\right)\\ =& \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1| + \mathrm{e}^{-i\omega t}|0\rangle\langle 1| + \mathrm{e}^{i\omega t}|1\rangle\langle 0|\right).\end{aligned} \tag{101}$$

The probability to project on the state $|+\rangle$ is

$$\langle +|\hat{\rho}(t)|+\rangle = \frac{1}{2}(1 + \cos\omega t). \tag{102}$$

Now we consider the initial state

$$\hat{\rho}_\eta(0) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + \eta|0\rangle\langle 1| + \eta|1\rangle\langle 0|), \tag{103}$$

with a real parameter $\eta \in [0, 1]$. Then

$$\hat{\rho}_\eta(t) = \hat{U}\hat{\rho}_\eta(0)\hat{U}^\dagger = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1| + \eta\mathrm{e}^{-i\omega t}|0\rangle\langle 1| + \eta\mathrm{e}^{i\omega t}|1\rangle\langle 0|\right). \tag{104}$$

The probability to project on the state $|+\rangle$ is

$$\langle +|\hat{\rho}_\eta(t)|+\rangle = \frac{1}{2}(1 + \eta\cos\omega t). \tag{105}$$

We can write $\hat{\rho}_\eta(0)$ also

$$\begin{aligned}\hat{\rho}_\eta(0) =& \frac{1-\eta}{2}|0\rangle\langle 0| + \frac{1-\eta}{2}|1\rangle\langle 1| + \frac{\eta}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + |0\rangle\langle 1| + |1\rangle\langle 0|)\\ =& \frac{1-\eta}{2}|0\rangle\langle 0| + \frac{1-\eta}{2}|1\rangle\langle 1| + \eta|+\rangle\langle+|.\end{aligned} \tag{106}$$

### 4.1.3 Pure states and mixed states

A density matrix with a single non-vanishing eigenvalue describes a pure state $|\Psi\rangle\langle\Psi|$; a density matrix with at least two non-vanishing eigenvalues describe a mixed state.

- For pure states $\mathrm{Tr}\,\hat{\rho}^2 = 1$.
- For mixed states $\mathrm{Tr}\,\hat{\rho}^2 < 1$.

### 4.1.4 Expansion in operator basis

The operator $\hat{A}$ can be expressed as

$$\begin{aligned}\hat{A} &= \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{2}(A_{00}+A_{11})+\frac{1}{2}(A_{00}-A_{11}) & \frac{1}{2}(A_{01}+A_{10})+\frac{1}{2}(A_{01}-A_{10}) \\ \frac{1}{2}(A_{01}+A_{10})-\frac{1}{2}(A_{01}-A_{10}) & \frac{1}{2}(A_{00}+A_{11})-\frac{1}{2}(A_{00}-A_{11}) \end{pmatrix} \\ &= \frac{1}{2}(A_{00}+A_{11})\mathbb{1}+\frac{1}{2}(A_{00}-A_{11})\hat{\sigma}_z+\frac{1}{2}(A_{01}+A_{10})\hat{\sigma}_x+i\frac{1}{2}(A_{01}-A_{10})\hat{\sigma}_y \\ &= \frac{1}{2}\operatorname{Tr}\hat{A}\mathbb{1}+\frac{1}{2}\operatorname{Tr}\Big(\hat{A}\hat{\sigma}_z\Big)\hat{\sigma}_z+\frac{1}{2}\operatorname{Tr}\Big(\hat{A}\hat{\sigma}_x\Big)\hat{\sigma}_x+\frac{1}{2}\operatorname{Tr}\Big(\hat{A}\hat{\sigma}_y\Big)\hat{\sigma}_y,\end{aligned} \tag{107}$$

where

$$\operatorname{Tr}\Big(\hat{A}\hat{B}^\dagger\Big) = \sum_{ij} \langle i|\,\hat{A}\,|j\rangle\,\langle j|\,\hat{B}^\dagger\,|i\rangle = \sum_{ij} A_{ij}B^\dagger_{ji}. \tag{108}$$

Using $\hat{\sigma}_i^2 = \mathbb{1}$ and $\hat{\sigma}_i^\dagger = \hat{\sigma}_i$, and consider $\operatorname{Tr}\hat{A} = 1$ (normalised), then

$$\operatorname{Tr}\Big(\hat{A}^2\Big) = \frac{1}{4}\operatorname{Tr}\mathbb{1}+\frac{1}{4}\sum_{i=1}^{3}\mu_i^2\operatorname{Tr}\hat{\sigma}_i^2 = \frac{1}{2}+\frac{1}{2}\sum_{i=1}^{3}\mu_i^2 = \frac{1}{2}+\frac{1}{2}\boldsymbol{u}\cdot\boldsymbol{u}, \tag{109}$$

where $\boldsymbol{u} = \operatorname{Tr}\hat{A}\hat{\sigma}_i^\dagger$ is called the **Bloch vector**. The operator basis are $\hat{\sigma}_{1,2,3} = \hat{\sigma}_{x,y,z}$ and $\hat{\sigma}_4 = \mathbb{1}$.

## 4.2 Open quantum systems and decoherence

### 4.2.1 System-environment interaction

The Hamiltonian for system-environment interaction is

$$H_{\text{SE}} = \sum_i \underbrace{|i\rangle\,\langle i|}_{\text{sys}} \otimes \underbrace{\hat{h}_i}_{\text{env}}\,. \tag{110}$$

This Hamiltonian generates the time evolution

$$\hat{U}_i = \exp\left(-it\sum_i |i\rangle\,\langle i|\otimes\hat{h}_i\right) = \sum_i |i\rangle\,\langle i|\otimes \mathrm{e}^{-i\hat{h}_i t} = \sum_i |i\rangle\,\langle i|\otimes\hat{u}_i(t). \tag{111}$$

Suppose the initial state

$$|\Psi(0)\rangle = \sum_i \Psi_i\,|i\rangle\otimes|\Phi\rangle\,, \tag{112}$$

which is completely uncorrelated. Applying the evolution operators, we have

$$|\Psi(t)\rangle = \hat{U}_i\,|\Psi(0)\rangle = \sum_{ij}\Psi_j\,|i\rangle\,\langle i|j\rangle\otimes\hat{u}_i(t)\,|\Phi\rangle = \sum_i \Psi_i\,|i\rangle\otimes\hat{u}_i(t)\,|\Phi\rangle\,. \tag{113}$$

The reduced density matrix for the system reads

$$\begin{aligned}\hat{\rho}_{\text{sys}} =& \ \mathrm{Tr}_{\text{env}}\left(\sum_{ij}\Psi_i\Psi_j^* |i\rangle\langle j| \otimes \hat{u}_i(t)|\Phi\rangle\langle\Phi|\hat{u}_j^\dagger(t)\right), \\ =& \sum_{ij}\Psi_i\Psi_j^*|i\rangle\langle j|\langle\Phi|\hat{u}_i(t)\hat{u}_j^\dagger(t)|\Phi\rangle \\ =& \sum_{ij}\Psi_i\Psi_j^*|i\rangle\langle j|\langle\Phi_j|\Phi_i\rangle .\end{aligned} \tag{114}$$

### 4.2.2 Quantum channels and open quantum dynamics

Let's assume that am atom is the system $a|e\rangle + b|g\rangle$ surrounded by the vacuum fields $|0_\lambda\rangle$. Due to their interaction, the atomic field will be entangled with the vacuum photonic field

$$|\Psi(0)\rangle = (a|e\rangle + b|g\rangle)|0_\lambda\rangle , \tag{115}$$

$$\begin{aligned}|\Psi(t)\rangle &= a(\alpha|e\rangle|0_\lambda\rangle + \beta|g\rangle|1\rangle_\lambda) + b|g\rangle|0_\lambda\rangle \\ &= (a\alpha|e\rangle + b|g\rangle)|0_\lambda\rangle + a\beta|g\rangle|1_\lambda\rangle .\end{aligned} \tag{116}$$

The density operator of the system is

$$\hat{\rho}_{\text{system}} = \mathrm{Tr}_{\text{env}}|\Psi\rangle\langle\Psi| = (a\alpha|e\rangle + b|g\rangle)(a^*\alpha^*\langle e| + b^*\langle g|) + |a|^2|\beta|^2|g\rangle\langle g| . \tag{117}$$

In general, the total system $|\Psi\rangle$ and the evolution operator $\hat{U}(t) = \exp\left(-i\hat{H}t\right)$. Then the evolution of the total system is given by

$$|\Psi(t)\rangle = \exp\left(-i\hat{H}t\right)|\Psi(0)\rangle = \hat{U}(t)|\Psi(0)\rangle \tag{118}$$

Let's assume the initial total system is composed of the system and its environment $\hat{\rho}_{0,\text{total}} = \hat{\rho}_0 \otimes |\phi_{\text{env}}\rangle\langle\phi_{\text{env}}| = |\phi_{\text{env}}\rangle\hat{\rho}_0\langle\phi_{\text{env}}|$. To find the density operator for the system

$$\begin{aligned}\hat{\rho}(t) &= \mathrm{Tr}_{\text{env}}|\Psi(t)\rangle\langle\Psi(t)| = \sum_i \langle i|\hat{U}(t)|\Psi(0)\rangle\langle\Psi(0)|\hat{U}^\dagger|i\rangle \\ &= \sum_i \langle i|\hat{U}(t)|\phi_{\text{env}}\rangle\hat{\rho}_0\langle\phi_{\text{env}}|\hat{U}^\dagger|i\rangle = \sum_i \hat{F}_i(t)\hat{\rho}_0\hat{F}_i^\dagger(t),\end{aligned} \tag{119}$$

with the **Kraus operators**

$$\hat{F}_i(t) = \langle i|\hat{U}(t)|\phi_{\text{env}}\rangle , \tag{120}$$

which satisfy the relation

$$\sum_i \hat{F}_i^\dagger\hat{F}_i = \mathbb{1}. \tag{121}$$

The map

$$\hat{\rho}(t) = \Lambda(\hat{\rho}_0) = \sum_i \hat{F}_i(t)\hat{\rho}_0\hat{F}_i^\dagger(t), \tag{122}$$

is called the **quantum channel**.

### 4.2.3 Properties of quantum channels

Quantum channels $\hat{\Lambda}(\rho) = \sum_i \hat{F}_i \hat{\rho} \hat{F}_i^\dagger$ have the properties:

1. **Trace preserving**
$$\mathrm{Tr}\left(\hat{\Lambda}(\rho)\right) = \mathrm{Tr}\,\hat{\rho}, \tag{123}$$
due to $\sum_i \hat{F}_i^\dagger \hat{F}_i = \mathbb{1}$.

2. **Positive maps**
$$\langle\Phi| \sum_i \hat{F}_i \hat{\rho} \hat{F}_i^\dagger |\Phi\rangle = \sum_i \langle\Phi| \hat{F}_i \hat{\rho} \hat{F}_i^\dagger |\Phi\rangle = \sum_i \langle\Phi_i| \hat{\rho} |\Phi_i\rangle \geq 0, \tag{124}$$
where $|\Phi_i\rangle = \hat{F}_i^\dagger |\Phi\rangle$.

3. **Completely positive maps**: any positive maps whose extensions, i.e.
$$(\hat{\Lambda} \otimes \hat{\mathbb{1}})(\hat{\rho}) = \sum_i (\hat{F}_i \otimes \mathbb{1}) \hat{\rho} (\hat{F}_i^\dagger \otimes \mathbb{1}) \tag{125}$$
are positive maps, are called completely positive maps.

### 4.2.4 Exemplary quantum channels

1. **Dissipation channel**
Consider the Kraus operators
$$\hat{F}_1 = |0\rangle\langle 0|, \quad \hat{F}_2 = |0\rangle\langle 1|, \tag{126}$$
which satisfies $\sum_i \hat{F}_i^\dagger \hat{F}_i = \mathbb{1}$. Let us apply $\hat{F}_i$ to $\hat{\rho}$:
$$\sum_i \hat{F}_i \hat{\rho} \hat{F}_i^\dagger = \hat{F}_1 \hat{\rho} \hat{F}_1^\dagger + \hat{F}_2 \hat{\rho} \hat{F}_2^\dagger = (\rho_{00} + \rho_{11}) |0\rangle\langle 0| = |0\rangle\langle 0|. \tag{127}$$
We can turn this into a time-dependent process
$$\hat{F}_0(t) = \sqrt{1-p(t)}\mathbb{1}, \quad \hat{F}_1(t) = \sqrt{p(t)}\,|0\rangle\langle 0|, \quad \hat{F}_2(t) = \sqrt{p(t)}\,|0\rangle\langle 1|, \tag{128}$$
with
$$\sum_i \hat{F}_i^\dagger(t) \hat{F}_i(t) = (1-p(t))\mathbb{1} + p(t)\,|0\rangle\langle 0| + p(t)\,|1\rangle\langle 1| = \mathbb{1}. \tag{129}$$
Therefore,
$$\sum_i \hat{F}_i(t) \hat{\rho}(0) \hat{F}_i^\dagger(t) = (1-p(t))\hat{\rho}(0) + p(t)\,|0\rangle\langle 0|. \tag{130}$$

2. **Dephasing channel**

(a) Consider two Kraus operators

$$\hat{F}_1 = \sqrt{\frac{1+p}{2}}\mathbb{1}, \quad \hat{F}_2 = \sqrt{\frac{1-p}{2}}\hat{\sigma}_z, \tag{131}$$

with $\hat{\rho} = \rho_{00}|0\rangle\langle 0| + \rho_{11}|1\rangle\langle 1| + \rho_{01}|0\rangle\langle 1| + \rho_{10}|1\rangle\langle 0|$. One obtains

$$\hat{F}_1\hat{\rho}\hat{F}_1^\dagger = \frac{1+p}{2}(\rho_{00}|0\rangle\langle 0| + \rho_{11}|1\rangle\langle 1| + \rho_{01}|0\rangle\langle 1| + \rho_{10}|1\rangle\langle 0|), \tag{132}$$

$$\hat{F}_2\hat{\rho}\hat{F}_2^\dagger = \frac{1-p}{2}(\rho_{00}|0\rangle\langle 0| + \rho_{11}|1\rangle\langle 1| - \rho_{01}|0\rangle\langle 1| - \rho_{10}|1\rangle\langle 0|), \tag{133}$$

$$\hat{\Lambda}(\hat{\rho}) = \rho_{00}|1\rangle\langle 1| + \rho_{11}|1\rangle\langle 1| + p(\rho_{01}|0\rangle\langle 0| + \rho_{10}|1\rangle\langle 0|). \tag{134}$$

(b) Consider another set of Kraus operators

$$\hat{F}_1 = \sqrt{p}\mathbb{1}, \quad \hat{F}_2 = \sqrt{1-p}\,|0\rangle\langle 0|, \quad \hat{F}_3 = \sqrt{1-p}\,|1\rangle\langle 1|. \tag{135}$$

Then

$$\hat{\Lambda}(\hat{\rho}) = \sum_i \hat{F}_i\hat{\rho}\hat{F}_i^\dagger = \rho_{00}|0\rangle\langle 0| + \rho_{11}|1\rangle\langle 1| + p(\rho_{01}|0\rangle\langle 1| + \rho_{10}|1\rangle\langle 0|). \tag{136}$$

(c) Consider the Kraus operators

$$\hat{F}_1 = \frac{1}{\sqrt{2}}\exp\Big(i\frac{\varphi}{2}\hat{\sigma}_z\Big), \quad \hat{F}_2 = \frac{1}{\sqrt{2}}\exp\Big(-i\frac{\varphi}{2}\hat{\sigma}_z\Big). \tag{137}$$

Then

$$\hat{\Lambda}(\hat{\rho}) = \rho_{00}|0\rangle\langle 0| + \rho_{11}|1\rangle\langle 1| + \cos\varphi(\rho_{01}|0\rangle\langle 1| + \rho_{10}|1\rangle\langle 0|). \tag{138}$$

We see that there is **non-uniqueness** of Kraus operators.

3. **Depolarising channel**
Consider the Kraus operators

$$\hat{F}_0 = \sqrt{1-p}\mathbb{1}, \quad \hat{F}_1 = \sqrt{\frac{p}{3}}\hat{\sigma}_x, \quad \hat{F}_2 = \sqrt{\frac{p}{3}}\hat{\sigma}_y, \quad \hat{F}_3 = \sqrt{\frac{p}{3}}\hat{\sigma}_z. \tag{139}$$

Then

$$\hat{\Lambda}(\hat{\rho}) = \sum_i \hat{F}_i\hat{\rho}\hat{F}_i^\dagger = (1-p)\hat{\rho} + \frac{p}{3}(\hat{\sigma}_x\hat{\rho}\hat{\sigma}_x + \hat{\sigma}_y\hat{\rho}\hat{\sigma}_y + \hat{\sigma}_z\hat{\rho}\hat{\sigma}_z). \tag{140}$$

The depolarising channel brings the original quantum state to the identity $\mathbb{1}$.

### 4.2.5 Generalised measurements

1. **von Neumann measurements / projective measurements**
   Consider the operator $\hat{\sigma}_z$

$$\hat{\sigma}_z |0\rangle = +1 |0\rangle, \quad \hat{\sigma}_z |1\rangle = -1 |1\rangle, \tag{141}$$

   then

$$\hat{\sigma}_z = |0\rangle \langle 0| - |1\rangle \langle 1|. \tag{142}$$

   The probability that $\hat{\sigma}_z$ give the result $+1$

$$P(+1) = \langle 0| \hat{\rho} |0\rangle = \mathrm{Tr}(\hat{\rho} |0\rangle \langle 0|). \tag{143}$$

   In general, we define a projector

$$\hat{P} = |\lambda_i\rangle \langle \lambda_i|. \tag{144}$$

   The properties of projectors are

   (a) They are Hermitian.
   (b) They are positive operators.
   (c) They are complete.
   (d) They are orthonormal.

   These are also the conditions for the von Neumann measurements.

2. **Generalised measurements**
   Let's consider the four measurement bases for two qubits

$$|\Phi_1\rangle = \frac{1}{\sqrt{2}} \left( |1\rangle |0\rangle + \tan\theta |0\rangle |0\rangle + \sqrt{1 - \tan^2\theta} |1\rangle |1\rangle \right), \tag{145}$$
$$|\Phi_2\rangle = \frac{1}{\sqrt{2}} \left( |1\rangle |0\rangle - \tan\theta |0\rangle |0\rangle - \sqrt{1 - \tan^2\theta} |1\rangle |1\rangle \right), \tag{146}$$
$$|\Phi_3\rangle = \sqrt{1 - \tan^2\theta} |0\rangle |0\rangle - \tan\theta |1\rangle |1\rangle, \tag{147}$$
$$|\Phi_4\rangle = |0\rangle |1\rangle, \tag{148}$$

   where $0 \leq \theta \leq \pi/4$, and the projectors are $|\Phi_i\rangle \langle \Phi_i|$. We assume that we prepare the second qubit in $|0\rangle$. Then the four projectors will result in the projection the first qubit on

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|1\rangle + \tan\theta |0\rangle), \tag{149}$$

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}}(|1\rangle - \tan\theta |0\rangle), \tag{150}$$

$$|\Psi_3\rangle = \sqrt{1 - \tan^2\theta} |0\rangle, \tag{151}$$

while $|\Psi_i\rangle\langle\Psi_i|$ satisfy the properties (a), (b) and (c) above while they are not orthogonal to each other. We can also consider

$$\hat{\Pi}_0 = (1-p)\,|0\rangle\langle 0| + p\,|1\rangle\langle 1|\,, \tag{152}$$
$$\hat{\Pi}_1 = (1-p)\,|1\rangle\langle 1| + p\,|0\rangle\langle 0|\,. \tag{153}$$

The two measurements are not orthogonal to each other. When $p = 0$, then $\hat{\Pi}_0 = |0\rangle\langle 0|$ and $\hat{\Pi}_1 = |1\rangle\langle 1|$.

## 4.3 Error correction

### 4.3.1 Classical error correction

For instance, three qubits realise one logical bit

$$\underset{\text{logical qubit}}{\bar{0}} = \underset{\text{physical qubits}}{000}, \quad \bar{1} = 111. \tag{154}$$

The probability of two or three errors (error probability $p \ll 1$)

$$p^3 + 3p^2(1-p) \ll 1. \tag{155}$$

### 4.3.2 Quantum error correction

1. **Bit flip error** $|0\rangle \to |1\rangle\,, |1\rangle \to |0\rangle$
   Let us measure on $\{|0\rangle\,, |1\rangle\}$ basis, the qubit can be expressed as

   $$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{156}$$

   then the logical qubits

   $$|\bar{\psi}\rangle = \alpha\,|000\rangle + \beta\,|111\rangle\,. \tag{157}$$

   Let us find out how to achieve the logical qubits. Consider the quantum circuits in Fig. 8(a).

   - $1^{\text{st}}$ CNOT works on qubit 1 and 2:

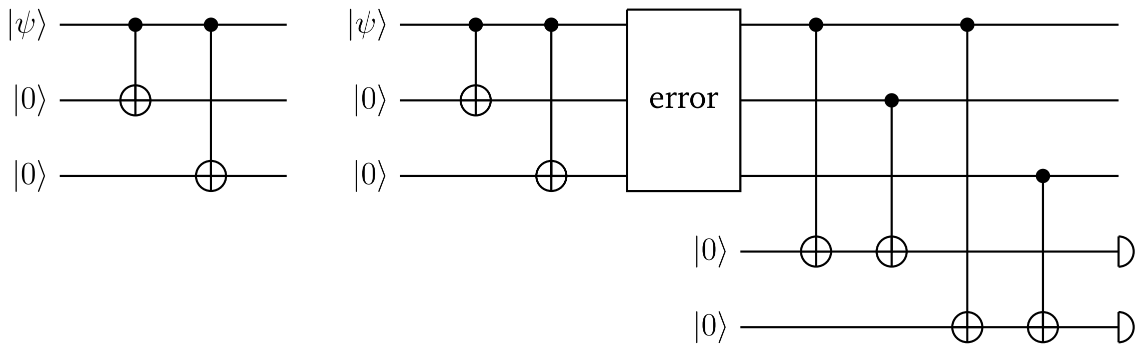
     $$(\alpha\,|0\rangle + \beta\,|1\rangle)\,|00\rangle \to \alpha\,|000\rangle + \beta\,|110\rangle\,. \tag{158}$$

   - $2^{\text{nd}}$ CNOT works on qubit 1 and 3:

     $$\alpha\,|000\rangle + \beta\,|110\rangle \to \alpha\,|000\rangle + \beta\,|111\rangle\,. \tag{159}$$

   Then we consider the bit flip errors (Fig. 8(b)). If a bit-flip error happens on the first qubit $Q_1$, then the state before first CNOT gate can be $\alpha\,|100\rangle + \beta\,|011\rangle$. The qubits follow the process:

   $$\begin{aligned}\alpha\,|100\rangle\,|00\rangle + \beta\,|011\rangle\,|00\rangle &\to \alpha\,|100\rangle\,|10\rangle + \beta\,|011\rangle\,|00\rangle \\ &\to \alpha\,|100\rangle\,|10\rangle + \beta\,|011\rangle\,|10\rangle \\ &\to \alpha\,|100\rangle\,|11\rangle + \beta\,|011\rangle\,|10\rangle \\ &\to \alpha\,|100\rangle\,|11\rangle + \beta\,|011\rangle\,|11\rangle\,.\end{aligned} \tag{160}$$




(a) (b)

**Figure 8:** (a) Prepare the logical qubits. (b) Bit flip error detection.

Finally, we can write the error and the corresponding results $|\text{data}\rangle\,|\text{ancilla}\rangle$:

$$\begin{array}{ll} \text{no} & (\alpha\,|000\rangle + \beta\,|111\rangle)\,|00\rangle \\ Q_1 & (\alpha\,|100\rangle + \beta\,|011\rangle)\,|11\rangle \\ Q_2 & (\alpha\,|010\rangle + \beta\,|101\rangle)\,|10\rangle \\ Q_3 & (\alpha\,|001\rangle + \beta\,|110\rangle)\,|01\rangle\,. \end{array}$$

To correct the bit-flip errors, we can perform $\hat{\sigma}_x$ on the qubits, which can realise $|0\rangle \to |1\rangle$ and $|1\rangle \to |0\rangle$.

2. **Phase flip error** $|+\rangle \to |-\rangle\,, |-\rangle \to |+\rangle$
We encode the information on basis $\{|+\rangle\,, |-\rangle\}$, then the physical qubit

$$|\psi\rangle = \alpha\,|+\rangle + \beta\,|-\rangle\,. \tag{161}$$

The corresponding logical qubits

$$|\bar{0}\rangle = |+++\rangle\,, \quad |\bar{1}\rangle = |---\rangle\,, \tag{162}$$

and

$$|\bar{\psi}\rangle = \alpha\,|+++\rangle + \beta\,|---\rangle\,, \tag{163}$$

which are generated by Hadamard gate (see in Fig. 9).

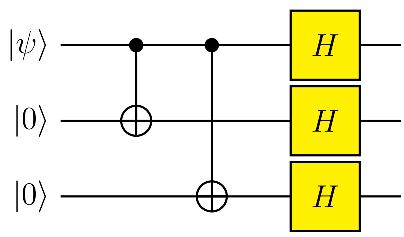



**Figure 9:** Prepare the logical qubits for phase error detection.

## 4.4 Stabiliser formalism

### 4.4.1 Stabilisers

**Definition (Stabiliser)**
*A state $|\psi\rangle$ is defined to be stabilised by operators $\hat{K}$ if it is a $(+1)$ eigenstate of $\hat{K}$*

$$\hat{K}\,|\psi\rangle = |\psi\rangle\,. \tag{164}$$

*Here, $|K\rangle$ is called the stabilisers of $|\psi\rangle$.*

For qubit systems, let's consider the Pauli group

$$P = \left\{\pm\mathbb{1}, \pm i\mathbb{1}, \pm\hat{X}, \pm i\hat{X}, \pm\hat{Y}, \pm i\hat{Y}, \pm\hat{Z}, \pm i\hat{Z}\right\}. \tag{165}$$

For $N$ qubits

$$P_N = P^{\otimes N}. \tag{166}$$

An $N$-qubit stabiliser state $|\psi\rangle$ is then defined by the $N$ generators of an Abelian (all elements commute) sub-group, $G$, of the $N$-qubit Pauli group

$$G = \left\{\hat{K}_i \middle| \hat{K}_i\,|\psi\rangle = |\psi\rangle\,, [\hat{K}_i, \hat{K}_j] = 0, \forall(i,j)\right\}, \tag{167}$$

where $\hat{K}_i$ is Hermitian and $\hat{K}_i\hat{K}_i = \mathbb{1}$. If we encode $k$ logical qubits into $n$ physical qubits, the number of stabilisers for the stabiliser code is $l = n - k$.
**Example**

1. GHZ state

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \tag{168}$$

   is stabilised by

$$\hat{K}_1 = \hat{X}\hat{X}\hat{X}, \quad \hat{K}_2 = \hat{Z}\hat{Z}\mathbb{1}, \quad \hat{K}_3 = \mathbb{1}\hat{Z}\hat{Z}. \tag{169}$$

   **Note.** Where is $\hat{K}_4 = \hat{Z}\mathbb{1}\hat{Z}$? The four Paulis $\hat{K}_1, \hat{K}_2, \hat{K}_3, \hat{K}_4$ are not mutual exclusive generators, because $\hat{K}_4 = \hat{K}_2\hat{K}_3$ (or any other permutation). Hence, to generate this specific stabilizer we only need $\hat{K}_1$ and any two of the set $\hat{K}_2, \hat{K}_3, \hat{K}_4$.

2. Shor code

$$|\bar{0}\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) = |+++\rangle\,, \tag{170}$$

$$|\bar{1}\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle) = |---\rangle\,. \tag{171}$$

3. Consider the following 7-qubit code

$$\begin{aligned}|\bar{0}\rangle = \frac{1}{\sqrt{8}}(\,&|0000000\rangle + |1010101\rangle + |0110011\rangle + |0001111\rangle \\ &+ |1011010\rangle + |0111100\rangle + |1101001\rangle + |1100110\rangle),\end{aligned} \tag{172}$$

$$|\bar{1}\rangle = \frac{1}{\sqrt{8}}(\,|1111111\rangle + |0101010\rangle + |1001100\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle + |0011001\rangle). \tag{173}$$

The stabiliser set for the 7-qubit code is specified by

$$\hat{K}_1 = \mathbb{1}\mathbb{1}\mathbb{1}\hat{X}\hat{X}\hat{X}\hat{X}, \quad \hat{K}_2 = \hat{X}\mathbb{1}\hat{X}\mathbb{1}\hat{X}\mathbb{1}\hat{X}, \tag{174}$$

$$\hat{K}_3 = \mathbb{1}\hat{X}\hat{X}\mathbb{1}\mathbb{1}\hat{X}\hat{X}, \quad \hat{K}_4 = \mathbb{1}\mathbb{1}\mathbb{1}\hat{Z}\hat{Z}\hat{Z}\hat{Z}, \tag{175}$$

$$\hat{K}_5 = \hat{Z}\mathbb{1}\hat{Z}\mathbb{1}\hat{Z}\mathbb{1}\hat{Z}, \quad \hat{K}_6 = \mathbb{1}\hat{Z}\hat{Z}\mathbb{1}\mathbb{1}\hat{Z}\hat{Z}. \tag{176}$$

### 4.4.2 Error measurements

By the definition of stabiliser codes

$$\hat{K}_i\,|\psi\rangle_L = |\psi\rangle_L\,, \tag{177}$$

where the subscript $L$ denotes logical qubits. The errors are assumed to happen in the form $\hat{X}, \hat{Y}, \hat{Z}$. Denoting the error by $\hat{E}$, we know that $\hat{E}$ and $\hat{K}$ are Pauli operators, so

$$[\hat{K}_i, \hat{E}] = 0, \quad \text{or} \quad \{\hat{K}_i, \hat{E}\} = 0. \tag{178}$$

We can write

$$\hat{K}_i\hat{E}\,|\psi\rangle_L = (-1)^m\hat{E}\hat{K}_i\,|\psi\rangle_L = (-1)^m\hat{E}\,|\psi\rangle_L\,, \tag{179}$$

where $m = 0$ if $[\hat{K}_i, \hat{E}] = 0$, $m = 1$ if $\{\hat{K}_i, \hat{E}\} = 0$.
Since an error-free state is already a $+1$ eigenstate of all the stabilisers, errors which anticommute with any of the stabilisers will flip the relevant eigenstate giving the eigenvalue $-1$.

### 4.4.3 Preparation of eigenstates for a Pauli group operator

Consider the circuits in Fig. 10. Before the measurement,

$$\begin{aligned}
|0\rangle\,|\Psi\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|\Psi\rangle \\
&\xrightarrow{C-U} \frac{1}{\sqrt{2}}(|0\rangle\,|\Psi\rangle + |1\rangle\,U\,|\Psi\rangle) \\
&\xrightarrow{H} \frac{1}{2}\left[(|0\rangle + |1\rangle)\,|\Psi\rangle + (|0\rangle - |1\rangle)U\,|\Psi\rangle\right] \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle \otimes \frac{|\Psi\rangle + U\,|\Psi\rangle}{\sqrt{2}} + |1\rangle \otimes \frac{|\Psi\rangle - U\,|\Psi\rangle}{\sqrt{2}}\right).
\end{aligned} \tag{180}$$

If the measurement outcome is 0, then

$$|\Psi_{F1}\rangle = \frac{1}{\sqrt{2}}(|\Psi\rangle + U\,|\Psi\rangle). \tag{181}$$

If the measurement outcome is 1, then

$$|\Psi_{F2}\rangle = \frac{1}{\sqrt{2}}(|\Psi\rangle - U\,|\Psi\rangle). \tag{182}$$

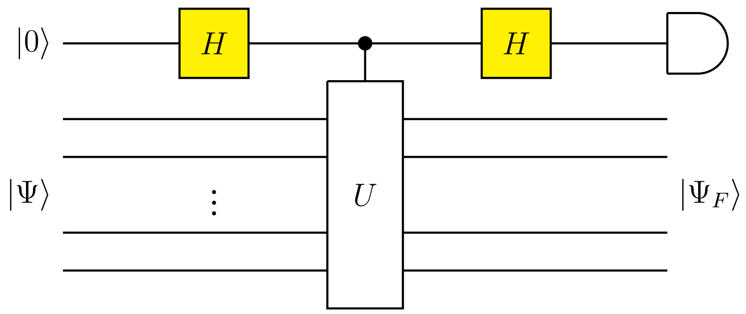



**Figure 10:** Preparation of eigenstates for $\hat{U}$, where $\hat{U}$ is a unitary gate, and $\hat{U}^2 = \mathbb{1}$.

The two states are eigenstates of $\hat{U}$:

$$U|\Psi_{F1}\rangle = \frac{1}{\sqrt{2}}(U|\Psi\rangle + U^2|\Psi\rangle) = \frac{1}{\sqrt{2}}(|\Psi\rangle + U|\Psi\rangle) = |\Psi_{F1}\rangle\,, \tag{183}$$

$$U|\Psi_{F2}\rangle = \frac{1}{\sqrt{2}}(U|\Psi\rangle - U^2|\Psi\rangle) = -\frac{1}{\sqrt{2}}(|\Psi\rangle - U|\Psi\rangle) = -|\Psi_{F2}\rangle\,. \tag{184}$$

For instance, if $\hat{U} = \hat{K}_1$, we generate an eigenstate of $\hat{K}_1$.

# 5 Properties and applications of entangled states

## 5.1 Definition and measures of entanglement

### 5.1.1 Pure states

**Definition**

*When two qubits can be written as*

$$|\psi\rangle = |\phi_A\rangle \otimes |\phi_B\rangle\,, \tag{185}$$

*then we say $|\psi\rangle$ is separable, otherwise $|\psi\rangle$ is entangled.*

**Example**

Special examples of pure states are the Bell states

$$|\Psi_\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \tag{186}$$

$$|\Phi_\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle). \tag{187}$$

Consider Alice's measurement in orthogonal bases $\{|\alpha\rangle\,, |\beta\rangle\}$ on $|\Phi_+\rangle$

1. If the measurement outcome is $|\alpha\rangle$, then the Bob's state becomes

$$|\Psi_\alpha\rangle_B = \langle\alpha|\Phi_+\rangle = \langle\alpha|\,\frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle) = \frac{1}{\sqrt{2}}(\langle\alpha|0\rangle\,|0\rangle + \langle\alpha|1\rangle\,|1\rangle). \tag{188}$$

2. If the measurement outcome is $|\beta\rangle$, then the Bob's state becomes

$$|\Psi_\beta\rangle_B = \langle\beta|\Phi_+\rangle = \langle\beta|\,\frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle) = \frac{1}{\sqrt{2}}(\langle\beta|0\rangle\,|0\rangle + \langle\beta|1\rangle\,|1\rangle). \tag{189}$$

The states are orthogonal to each other:

$${}_B\langle\Psi_\alpha|\Psi_\beta\rangle_B = \frac{1}{2}(\langle 0|\alpha\rangle\,\langle\beta|0\rangle + \langle 1|\alpha\rangle\,\langle\beta|1\rangle) = \frac{1}{2}\,\langle\beta|\alpha\rangle = 0, \tag{190}$$

So Alice can predict Bob's measurement result in $|\psi_\alpha\rangle$, or $|\psi_\beta\rangle$.

To define the measure of entanglement for a bipartite state $|\Psi\rangle$, let us consider the **von-Neumann entropy** defined as

$$\boxed{E = -\operatorname{Tr}\hat{\rho}_B \log_2 \hat{\rho}_B,} \tag{191}$$

for the reduced density matrix $\hat{\rho}_B = \operatorname{Tr}_A|\Psi\rangle\,\langle\Psi|$. The von Neumann measures the mixedness of the reduced density matrix. When $E = 0$, the state is separable; when $E = 1$, the state is maximally entangled.

**Example**

$$\hat{\rho}_B = \operatorname{Tr}_A|\Phi_+\rangle\,\langle\Phi_+| = \frac{1}{2}\,|0\rangle\,\langle 0| + \frac{1}{2}\,|1\rangle\,\langle 1| = \frac{1}{2}\mathbb{1}. \tag{192}$$

The von-Neumann entropy $E$ for $\hat{\rho}_B$ is 1.

### 5.1.2 Mixed state entanglement

**Definition**

*A bipartite system is separable when the density matrix $\hat{\rho}$ can be written as*

$$\hat{\rho} = \sum_i p_i \hat{\rho}_{Ai} \otimes \hat{\rho}_{Bi}, \tag{193}$$

*where* $0 \leq p_i \leq 1$.

When $\hat{\rho}$ is a density matrix, the transpose $\hat{\rho}^T$ is another density matrix. If $\hat{\rho}$ is separable, *i.e.*, $\hat{\rho} = \sum_i p_i \hat{\rho}_{Ai} \otimes \hat{\rho}_{Bi}$, then the partial transpose $\rho^{T_B} = \sum_i p_i \hat{\rho}_{Ai} \otimes \hat{\rho}_{Bi}^T \geq 0$. Otherwise when $\hat{\rho}^{T_B} < 0$, $\hat{\rho}$ is entangled.

**Example**

Consider the density matrix

$$\hat{\rho} = p\left|\Psi_-\right\rangle\left\langle\Psi_-\right| + (1-p)\frac{\mathbb{1}}{4} = \frac{1}{4}\begin{pmatrix} 1-p & 0 & 0 & 0 \\ 0 & 1+p & -2p & 0 \\ 0 & -2p & 1+p & 0 \\ 0 & 0 & 0 & 1-p \end{pmatrix}. \tag{194}$$

Consider the relation

$$A \otimes B = \begin{pmatrix} A_{00}B & A_{01}B \\ A_{10}B & A_{11}B \end{pmatrix} \quad \Rightarrow \quad A \otimes B^T = \begin{pmatrix} A_{00}B^T & A_{01}B^T \\ A_{10}B^T & A_{11}B^T \end{pmatrix} \tag{195}$$

So the partial transpose density matrix of $\hat{\rho}$ can be written as

$$\hat{\rho}^{T_B} = \frac{1}{4}\begin{pmatrix} 1-p & 0 & 0 & -2p \\ 0 & 1+p & 0 & 0 \\ 0 & 0 & 1+p & 0 \\ -2p & 0 & 0 & 1-p \end{pmatrix}. \tag{196}$$

Then, we have to find the eigenvalues

$$\begin{aligned} \det\left(\rho^{T_B} - \lambda\mathbb{1}\right) &= \left(\frac{1-p}{4} - \lambda\right)^2 \left(\frac{1+p}{4} - \lambda\right)^2 - \left(\frac{p}{2}\right)^2 \left(\frac{1+p}{4} - \lambda\right)^2 \\ &= \left(\frac{1+p}{4} - \lambda\right)^2 \left[\left(\frac{1-p}{4} - \lambda\right)^2 - \left(\frac{p}{2}\right)^2\right] \\ &= \left(\frac{1+p}{4} - \lambda\right)^3 \left(\frac{1-3p}{4} - \lambda\right) = 0. \end{aligned} \tag{197}$$

The eigenvalues are

$$\lambda_1 = \lambda_2 = \lambda_3 = \frac{1+p}{4} > 0, \quad \lambda_4 = \frac{1-3p}{4}. \tag{198}$$

When $0 \leq p \leq \frac{1}{3}$, $\hat{\rho}^{T_B} \geq 0$, the density matrix $\hat{\rho}$ is separable; while $\frac{1}{3} < p \leq 1$, the density matrix $\hat{\rho}$ is entangled.

### 5.1.3 Multipartite entanglement

A system is multipartite entangled when the system is not bi-separable.

**Example**

1. Consider the GHZ (Greenberger-Horne-Zeilinger) state

$$|\Psi_{\text{GHZ}}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \tag{199}$$

   - $\text{Tr}_A |\Psi_{\text{GHZ}}\rangle \langle\Psi_{\text{GHZ}}| = \frac{1}{2}(|00\rangle \langle 00| + |11\rangle \langle 11|)$ is mixed.
   - $\text{Tr}_B (\text{Tr}_A |\Psi_{\text{GHZ}}\rangle \langle\Psi_{\text{GHZ}}|) = \frac{1}{2}(|0\rangle \langle 0| + |1\rangle \langle 1|)$ is mixed.

2. Consider the state

$$|\Psi_-\rangle_{AB} |0\rangle_C = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) |0\rangle \,. \tag{200}$$

   - $\text{Tr}_A \hat{\rho} = \frac{1}{2}(|1\rangle \langle 1| - |0\rangle \langle 0|) \otimes |0\rangle \langle 0|$ is mixed.
   - $\text{Tr}_B \hat{\rho} = \frac{1}{2}(|0\rangle \langle 0| - |1\rangle \langle 1|) \otimes |0\rangle \langle 0|$ is mixed.
   - $\text{Tr}_C \hat{\rho} = |\Psi_-\rangle \langle \Psi_-|$ is pure.

3. Consider the W-state

$$|\Psi_{\text{W}}\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle). \tag{201}$$

   - $\text{Tr}_A |\Psi_{\text{W}}\rangle \langle\Psi_{\text{W}}| = \frac{1}{3}|00\rangle \langle 00| + \frac{1}{3}(|10\rangle + |01\rangle)(\langle 10| + \langle 01|)$ is mixed.

## 5.2 Schmidt decomposition

Suppose $|\Psi\rangle$ is a pure state of a bipartite system $A$ and $B$.

$$|\Psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle \,, \tag{202}$$

where $\lambda_i$ are non-negative real numbers and $\sum_i \lambda_i^2 = 1$. $\lambda_i$ are called **Schmidt coefficients**. We can find $\lambda_i$ through the eigenequations

$$\hat{\rho}_A |i\rangle = \lambda_i |i\rangle \,, \tag{203}$$

where $\hat{\rho}_A = \text{Tr}_B \hat{\rho}$.

**Proof**
Any state $|\Psi\rangle$ can be written as

$$|\Psi\rangle = \sum_{ij} a_{ij} |i\rangle |j\rangle \,. \tag{204}$$

We do a singular value decomposition

$$a = udv, \tag{205}$$

where $u$ and $v$ are unitary and $d$ is non-negative diagonal

$$a_{ij} = u_{ik} d_{kk} v_{jk}. \tag{206}$$

Then

$$\begin{aligned} |\Psi\rangle &= \sum_{ij} a_{ij} |i\rangle |j\rangle = \sum_{ijk} u_{ik} d_{kk} v_{kj} |i\rangle |j\rangle \\ &= \sum_k d_{kk} \left( \sum_i u_{ik} |i\rangle \right) \left( \sum_j v_{kj} |j\rangle \right) = \sum_k d_{kk} |k_A\rangle |k_B\rangle . \end{aligned} \tag{207}$$

## 5.3 Quantum teleportation

We consider three qubits, and assume that the first two qubits are situated in Alice's lab and the third qubit is situated in Bob's lab. The total system

$$|\Xi\rangle = |\chi\rangle |\Phi_+\rangle = |\chi\rangle \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{\alpha |000\rangle + \alpha |011\rangle + \beta |100\rangle + \beta |111\rangle}{\sqrt{2}}, \tag{208}$$

where $|\chi\rangle = \alpha |0\rangle + \beta |1\rangle$ is a general qubit. Alice performs Bell measurements on $\{|\Phi_\pm\rangle, |\Psi_\pm\rangle\}$ bases.

- If Alice's outcome is $|\Phi_+\rangle$, Bob's state is

$$_{12}\langle \Phi_+ | \Xi \rangle_{123} = \frac{1}{2}(\alpha |0\rangle + \beta |1\rangle)_3 = \frac{1}{2} |\chi\rangle_3 . \tag{209}$$

- If Alice's outcome is $|\Phi_-\rangle$, Bob's state is

$$_{12}\langle \Phi_- | \Xi \rangle_{123} = \frac{1}{2}(\alpha |0\rangle - \beta |1\rangle)_3 = \frac{1}{2}\hat{\sigma}_z |\chi\rangle_3 . \tag{210}$$

- If Alice's outcome is $|\Psi_+\rangle$, Bob's state is

$$\langle \Psi_+ | \Xi \rangle = \frac{1}{2}(\alpha |1\rangle + \beta |0\rangle)_3 = \frac{1}{2}\hat{\sigma}_x |\chi\rangle_3 . \tag{211}$$

- If Alice's outcome is $|\Psi_-\rangle$, Bob's state is

$$\langle \Psi_- | \Xi \rangle = \frac{1}{2}(\alpha |1\rangle - \beta |0\rangle)_3 = \frac{1}{2}\hat{\sigma}_z \hat{\sigma}_x |\chi\rangle_3 . \tag{212}$$

Therefore, Bob has the state

$$\hat{\rho}_\mathrm{B} = \frac{1}{4} \left( |\chi\rangle \langle\chi| + \hat{\sigma}_z |\chi\rangle \langle\chi| \hat{\sigma}_z + \hat{\sigma}_x |\chi\rangle \langle\chi| \hat{\sigma}_x + \hat{\sigma}_z \hat{\sigma}_x |\chi\rangle \langle\chi| \hat{\sigma}_x \hat{\sigma}_z \right) = \frac{1}{2}\mathbb{1}. \tag{213}$$

That is, no measurement on the third particle permits to infer any information on the state $|\chi\rangle$ without Alice's information. Furthermore, Bob cannot even tell if Alice has actually performed a measurement. The teleportation works only if there is classical communication between the labs. This ensures that no information is transferred faster than the speed of light.

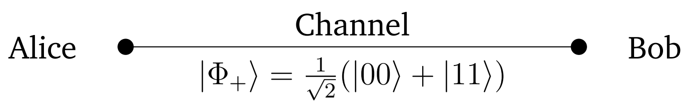



**Figure 11:** Super dense coding

## 5.4 Super dense coding

To send two-bit information $00, 01, 10, 11$, we prepare an entangled channel between Alice and Bob:

$$|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B). \tag{214}$$

1. **00-encoding:** Alice does nothing to her qubit and sends it to Bob. Bob receive $|\Phi_+\rangle$.

2. **01-encoding:** Alice performs $\hat{\sigma}_z$ to her qubit then sends it to Bob. Bob receive $|\Phi_-\rangle$:
$$\hat{\sigma}_z \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Phi_-\rangle\,. \tag{215}$$

3. **10-encoding:** Alice performs $\hat{\sigma}_x$ to her qubit then sends it to Bob. Bob receive $|\Psi_+\rangle$:
$$\hat{\sigma}_x \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = |\Psi_+\rangle\,. \tag{216}$$

4. **11-encoding:** Alice performs $\hat{\sigma}_y$ to her qubit then sends it to Bob. Bob receive $|\Psi_-\rangle$:
$$\hat{\sigma}_y \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{i}{\sqrt{2}}(|10\rangle - |01\rangle) \to |\Psi_-\rangle\,. \tag{217}$$

## 5.5 QKD example: Ekert 92

Alice and Bob can share a string of random numbers using entangled states.

1. Alice and Bob share maximally entangled qubits. Let us consider
$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|-+\rangle - |+-\rangle). \tag{218}$$

2. Alice and Bob perform measurements on their qubits in $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ basis (by independent random choice).

3. Alice and Bob compare the measurement bases and choose only the ones which agree each others. If their measurement sets match, the two should have the same measurement outcome.

4. Alice and Bob compare some of the measurement outcomes to check whether Eve exists.

## 5.6 Bell measurements

Let's consider one of the Bell states

$$|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \text{CNOT}\hat{H}_1 |0\rangle_1 |0\rangle_2 , \tag{219}$$

where $\hat{H}_1$ is the Hadamard operator on the first qubit. The projection can be done by CNOT on the given qubits followed by Hadamard:

$$\hat{H}_1\text{CNOT} |\Phi_+\rangle = \hat{H}_1\text{CNOT} \cdot \text{CNOT}\hat{H}_1 |0\rangle_1 |0\rangle_2 = |00\rangle . \tag{220}$$

The outcome is $|00\rangle$. Similarly, after CNOT and $\hat{H}$ operations, if the measurement outcome is $|10\rangle$ the projection is on $|\Phi_-\rangle$. If the outcome is $|01\rangle$ then $|\Psi_+\rangle$. If the outcome is $|11\rangle$ then the projection is on $|\Psi_-\rangle$.

## 5.7 Entanglement distillation

Let us assume two pairs of non-maximally entangled states

$$|\Phi(\theta)\rangle_{12} = \cos\theta\, |00\rangle_{12} + \sin\theta\, |11\rangle_{12} , \tag{221}$$
$$|\Phi(\theta)\rangle_{34} = \cos\theta\, |00\rangle_{34} + \sin\theta\, |11\rangle_{34} . \tag{222}$$

The total system is

$$|\Phi(\theta)\rangle_{12} |\Phi(\theta)\rangle_{34} = \cos^2\theta\, |0000\rangle + \sin^2\theta\, |1111\rangle + \sin\theta\cos\theta(|0011\rangle + |1100\rangle). \tag{223}$$

If we perform the Bell measurement on particles 2 and 3, when the outcome is

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{224}$$

the qubits are collapsed to

$$|\psi\rangle = \langle\Psi_+|_{23} |\Phi(\theta)\rangle_{12} |\Phi(\theta)\rangle_{34} = \frac{1}{\sqrt{2}}\sin\theta\cos\theta(|01\rangle + |10\rangle). \tag{225}$$

The normalisation of $|\psi\rangle$ is $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. So the probabilities of the measurement outcome is

$$P(|\psi\rangle) = \sin^2\theta\cos^2\theta. \tag{226}$$