Lecture Notes on Quantum information processing with photons and atoms

Yu-Ao Chen
CAS Center for Excellence in Quantum Information and Quantum Physics
University of Science and Technology of China
2019.06
Introduction to our group

Excellence Center for Quantum Information and Quantum Physics

- Jointly supported by CAS and the Ministry of Education

Hosted by USTC

includes top institutes and universities on quantum physics

Shanghai Institute of Technical Physics

Institute of Optics and Electronics

Institute of Semiconductor

Nanjing University

and excellence groups among China’s universities:
Tsinghua University, Peking University, Jiaotong University, etc.
Introduction to our group

Quantum Foundations

Quantum Communication

Quantum Physics & Quantum Information

Quantum Metrology

Quantum Computation & Simulation
Visit us at http://quantum.ustc.edu.cn
China’s Future National Projects

The Center is now playing a leading role in organizing

- National Science and Technology Project on Quantum Information in the next 15 years, similar to European Quantum Technologies Flagship
- National Laboratory for Quantum Information Sciences (NLQIS)

Global Quantum Communication Networks

Scalable Quantum Computation and Quantum Simulation

Super-resolution Quantum Metrology
Ph. D & Postdoc position available
Lecture 1: Introduction to Quantum Physics and Quantum Information

Part 1: Quantum Foundations
Information Exchange in Human Evolution

About 100,000 years ago, Homo Neanderthalian and Homo Sapien co-existed in Europe.

Homo Neanderthalian ➤
• Stronger
• With even larger cranial capacity than modern human!

→ Homo Sapiens
Individually weaker than Homo Neanderthalian, but developed proto-symbol and language.

Why did Homo Sapien win the evolution battle and become our ancestors?

Information exchange ➔ Coordinating groups
Social Advancement & Privacy Protection

Privacy ➞ Freedom of thoughts ➞ Innovation and social advancement!

Social progress makes information exchange more efficient
The information exchange has been and will continue to be accompanied by the human evolution and social development.

Ever lasting questions:

• How to make information exchange more efficient?  
• How to protect privacy?

Computing power

Information security
《送杜少府之任蜀川》
——王勃
城阙辅三秦，风烟望五津。与君离别意，同是宦游人。
海内存知己，天涯若比邻。
“无为在歧路，儿女共沾巾。”
11th century, 北宋《武经总要》： 替换式密码

1请弓、2请箭、3请刀、4请甲、5请枪旗、6请锅幕、7请马、8 请衣赐、9请粮料、10请草料、...、39都将病、40战小胜

16th century, France, Vigenère cipher

Challenges in Information Security

Ancient Greek scytale, 400 BC

Caesar cipher, 50 BC
Challenges in Information Security

20th Century, Switzerland

Enigma Machine

Classical encryption based on computational complexity

Encrypt

- authentication
  - Authorized user

- Transmission
  - Security in data transfer

- Digital signature
  - No change in data

Encrypt
Challenges in Information Security

RSA 512: cracked in 1999
RSA 768: cracked in 2009
RSA 1024: ? shall not be used after December 31, 2013 by NIST
The next-generation code “pairing-based cryptography” Cracked in 2012......
Feb. 2017, SHA-1 cracked by Google

Crack via variations in the frequency of the occurrence of letters, by Al-Kindi (800-873)

Enigma machine broken by Alan Turing’s Bombe machine
All the classical encryption methods that depend on computational complexity, can be cracked in principle!

“......human ingenuity cannot concoct a cipher which human ingenuity cannot resolve”

—A few words on secret writing, Edgar Alan Poe (1841)
Challenges in the Computational Capacity

Classical computational bottleneck
The world’s total computing power is insufficient to search a target in $2^{80-90}$ database within a year.

A technological limit
The Moore’s law that predicts the transistor density doubles every 18 months has come to an end.

- 2003: 90 nm
- 2005: 65 nm
- 2007: 45 nm
- 2009: 32 nm
- 2011: 22 nm

- Invented SiGe Strained Silicon
- 2nd Gen. SiGe Strained Silicon
- Invented Gate-Last High-k Metal Gate
- 2nd Gen. Gate-Last High-k Metal Gate
- First to Implement Tri-Gate

2017, 14 nm ➔ 2022, 4 nm ➔ 0.2 nm (atomic scale) ➔ ???

Tunneling induced leakage ➔
The “0/1” logic in the transistors will fail.
Quantum physics, after one century’s development, comes to the rescue for the problems confronted in the classical information technologies.
Quantum Superposition

Classical World
\[ |\text{here}\rangle \text{ or } |\text{there}\rangle \]

Quantum World
\[ |\text{here}\rangle + |\text{there}\rangle \]
Quantum Superposition

A “quantum flight”: from Shanghai to Stockholm, two possible routes:

When arrived

- If I fell asleep during flight (do not know which route I take), I will feel: “both cold and warm”

- If I was awake during flight and checked which route I take, I will feel either cold (Moscow) or warm (Singapore)

I took both routes in one flight!? It confirms I can only take one of the routes!

In quantum world, the state of a quantum object can be affected by measurement!
When Classical Physics Meets Life Philosophy

Newton’s law precisely predicts every single movement for all objects in our daily life

- A manifest of the beauty and power of physics!
- However, does it imply determinism?
- Does it mean everything (e.g. lectures today) is already determined from Big-bang?
- Efforts meaningless?
- Fortunately, quantum mechanics tells that your act (measurement) can affect the world!
Qubit & Quantum Superposition

Classical Physics: “bit”

Quantum Physics: “qubit”
Quantum Superposition
Quantum Superposition
Quantum Superposition
Qubits: Polarization of Single Photon

- One bit of information per photon (encoded in polarization)

- Qubit:

\[ |\psi\rangle = \alpha |H\rangle + \beta |V\rangle \]
\[ |\alpha|^2 + |\beta|^2 = 1 \]

- Non-cloning theorem:
  An unknown quantum state can not be copied precisely!
\[ 00 \rightarrow 00, \]
\[ 10 \rightarrow 11, \]
\[ (0 + 1)0 \rightarrow 00 + 11 \]
\[ \neq (0 + 1)(0 + 1) \]
# Single-Qubit Operations

Column vector represent of two-dimensional quantum states

| $|H\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ | $|V\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ |

Pauli matrix $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Two eigenstates:

$|+\rangle = \frac{1}{\sqrt{2}} (|H\rangle + |V\rangle)$

$|-\rangle = \frac{1}{\sqrt{2}} (|H\rangle - |V\rangle)$

Unitary rotation:

$\sigma_x |H\rangle = |V\rangle$

$\sigma_x |V\rangle = |H\rangle$

Pauli matrix $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

Two eigenstates:

$|L\rangle = \frac{1}{\sqrt{2}} (|H\rangle - i|V\rangle)$

$|R\rangle = \frac{1}{\sqrt{2}} (|H\rangle + i|V\rangle)$

Unitary rotation:

$\sigma_y |H\rangle = -i|V\rangle$

$\sigma_y |V\rangle = i|H\rangle$

Pauli matrix $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Two eigenstates:

$|H\rangle$

$|V\rangle$

Unitary rotation:

$\sigma_z |H\rangle = |H\rangle$

$\sigma_z |V\rangle = -|V\rangle$
Single-Qubit Operations

The Hadamard gate

<table>
<thead>
<tr>
<th>0 &gt;</th>
<th>0 &gt; +</th>
<th>1 &gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 &gt;</td>
<td>0 &gt; -</td>
<td>1 &gt;</td>
</tr>
</tbody>
</table>
Mach-Zehnder Interferometer

\[ H \Phi H |0\rangle = \frac{1}{2} ((e^{i\phi} + 1)|0\rangle + (e^{i\phi} - 1)|1\rangle) \]
Mach-Zehnder Interferometer

Interaction-free measurement!
Origin of Zeno effect

Can the rabbit overtake the turtle?
Quantum Zeno Effect

Considering neutron spin evolving in magnetic field, the probability to find it still in spin up state after time $T$ is

$$P = \cos^2 \left( \frac{\omega T}{2} \right)$$

where $\omega$ is the Larmor frequency.
Quantum Zeno Effect

\[ G \text{ (cake is good)} = G_0 \times \frac{1 + \cos T}{2}, \ (\omega = 1) \]

If we cut the bad part of the cake at time \( T = \pi/2 \), then at \( T = \pi \) we have \( G = 1/4 \times G_0 \).
Experiment

\[ P = \left[ \cos^2 \left( \frac{2\pi}{N} \right) \right]^N \]

In the limit of large \( N \): \( P = 1 - \frac{\pi^2}{4N} + O(N^{-2}) \)

Kwiat et al., PRL 74, 4763 (1995)

\[ |10\rangle \rightarrow |10\rangle \] with\
\[ P = \left[ \cos^2 \left( \frac{\pi}{2N} \right) \right]^N \]

Kwiat, et al., PRL 83 4725 (1999)
Quantum Zeno Effect

More complex structure: A nested and chained version of MZI

All-Pass:
\[ |100\rangle \rightarrow \cos^m_M \left( \cos_M |100\rangle + \sin_M |010\rangle \right) \]
\[ \downarrow_{m=M} \quad |100\rangle \]

All-Block:
\[ |100\rangle \rightarrow \cos m_M |100\rangle + \sin m_M |010\rangle \]
\[ \downarrow_{m=M} \quad |010\rangle \]

Quantum entanglement

- **Bell states** – maximally entangled states:

  $$|\pm\rangle_{12} = \frac{1}{\sqrt{2}} \left( |H\rangle_1 |H\rangle_2 \pm |V\rangle_1 |V\rangle_2 \right)$$


- **Quantum entanglement**

  $$|\pm\rangle_{12} = \frac{1}{\sqrt{2}} \left( |H\rangle_1 |V\rangle_2 \pm |V\rangle_1 |H\rangle_2 \right)$$

Two dices are entangled

*Spooky action at a distance*

--Albert Einstein
Quantum entanglement

GHZ states: three-photon maximally entangled states

\[
|\Phi^{\pm}\rangle_{123} = \frac{1}{\sqrt{2}} (|H\rangle_1 |H\rangle_2 |H\rangle_3 \pm |V\rangle_1 |V\rangle_2 |V\rangle_3 )
\]

\[
|\Psi^{\pm}\rangle_{123} = \frac{1}{\sqrt{2}} (|H\rangle_1 |H\rangle_2 |V\rangle_3 \pm |V\rangle_1 |V\rangle_2 |H\rangle_3 )
\]

\[
|\Xi^{\pm}\rangle_{123} = \frac{1}{\sqrt{2}} (|H\rangle_1 |V\rangle_2 |H\rangle_3 \pm |V\rangle_1 |H\rangle_2 |V\rangle_3 )
\]

\[
|\Theta^{\pm}\rangle_{123} = \frac{1}{\sqrt{2}} (|H\rangle_1 |V\rangle_2 |V\rangle_3 \pm |V\rangle_1 |H\rangle_2 |H\rangle_3 )
\]
Manipulation of Entanglement

Flip the target when control = 1:

\[ |00\rangle \rightarrow |00\rangle \]
\[ |01\rangle \rightarrow |01\rangle \]
\[ |10\rangle \rightarrow |11\rangle \]
\[ |11\rangle \rightarrow |10\rangle \]

Bell states

00 \rightarrow (0 + 1)0 = 00 + 10 \rightarrow (00 + 11)
\rightarrow (00 + 10) = (0 + 1)0 \rightarrow 00
000 → (0 + 1)00 = (00 + 10)0 → (00 + 11)0 = 000 + 110
→ 000 + 111 → 000 + 110 = (00 + 11)0 → (00 + 10)0
= (0 + 1)00 → 000
Spooky Action at a Distance?

Measurement time: $\Delta t$
Space-like separation: $L > \Delta t$

Quantum entanglement:

Entangled pair

Local Realism
Measurement on particle A will not affect particle B

Quantum Non-locality
Measurement on particle A will cause instant collapse on particle B
Quantum mechanics is certainly imposing. But an inner voice tells me that it is not yet the real thing. The theory says a lot, but does not really bring us any closer to the secret of the 'old one'. I, at any rate, am convinced that He does not throw dice.

Einstein, stop telling God what to do!
Bell’s Inequality: Testing This Battle

Experimental testable inequality:
Bell, Physics 1, 195 (1964)
Clauser et al., PRL 23, 880 (1969)

\[ S = |E(\phi_A \phi_A) - E(\phi_A \phi'_B) + E(\phi'_A \phi_B) + E(\phi'_A \phi'_B)| \]

- Einstein’s local realism: \( S_{\text{max}} \leq 2 \)
- Quantum mechanics: \( S_{\text{max}} = 2\sqrt{2} \)
Bell's Inequality: Testing This Battle

A simplified case: Sakurai’s Bell Inequality

Singlet state: anti-correlation of measurement results of two sides

\[ |\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}} (|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2) \]

Pick three arbitrary directions \(a, b, \) and \(c:\)

\[ P(a0, b0) = P_3 + P_4 \]
\[ P(a0, c0) = P_2 + P_4 \]
\[ P(c0, b0) = P_3 + P_7 \]

\[ P_3 + P_4 \leq P_3 + P_4 + P_2 + P_7 \]
Bell's Inequality: Testing This Battle

Local realism requires:
\[ P(a_0, b_0) \leq P(a_0, c_0) + P(c_0, b_0) \]

Quantum-mechanical prediction:
\[ P(a_0, b_0) = \frac{1}{2} \sin \left( \frac{a - b}{2} \right)^2 \]

For example, \( a = 90^\circ, b = 45^\circ, c = 0^\circ \), the inequality would require
\[ \frac{1}{2} \sin^2 45^\circ \leq \frac{1}{2} \sin^2 22.5^\circ + \frac{1}{2} \sin^2 22.5^\circ \]

\[ \frac{1}{2} \times 0.707 \leq \frac{1}{2} \times 0.408 + \frac{1}{2} \times 0.408 \]

\[ 0.354 \leq 0.1464 \]

An unsatisfactory feature
In the derivation of BI such a local realistic and thus classical picture can explain perfect correlations and is only in conflict with statistical prediction of quantum mechanics.
Conflict with Local Realism

Consider a three-photon GHZ state written in $\sigma_Z$ basis

$$|\psi_{123}\rangle = \frac{1}{\sqrt{2}}(|H_1\rangle|H_2\rangle|H_3\rangle + |V_1\rangle|V_2\rangle|V_3\rangle)$$

Linear polarization basis

\[\sigma_x : |H\rangle' = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \quad |V\rangle' = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle).\]

Circular polarization basis

\[\sigma_y : |R\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle), \quad |L\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle).\]
Conflict with Local Realism

\[ \sigma_{1y}\sigma_{2y}\sigma_{3x} : |\psi_{123}\rangle = \frac{1}{2} (R_1 L_2 H'_3 + L_1 R_2 H'_3 + R_1 R_2 V'_3 + L_1 L_2 V'_3) \]

\[ \sigma_{1y}\sigma_{2x}\sigma_{3y} : |\psi_{123}\rangle = \frac{1}{2} (R_1 H'_2 L_3 + L_1 H'_2 R_3 + R_1 V'_2 R_3 + L_1 V'_2 L_3) \]

\[ \sigma_{1x}\sigma_{2y}\sigma_{3y} : |\psi_{123}\rangle = \frac{1}{2} (H'_1 R_2 L_3 + H'_1 L_2 R_3 + V'_1 R_2 R_3 + V'_1 L_2 L_3) \]

Therefor state \(|\psi_{123}\rangle \) is the eigenstate of operators 
\( \sigma_{1y}\sigma_{2y}\sigma_{3x}, \sigma_{1y}\sigma_{2x}\sigma_{3y}, \sigma_{1x}\sigma_{2y}\sigma_{3y} \) with value -1
Conflict with Local Realism

- **EPR reality criterion:** operator is predeterminethe individual value of any local d
- There exists an element of local reality $S_{ix}$ corresponding to operator

\[ \sigma_{ix} \left( i = 1, 2, 3 \right). \]

All six of the elements of reality $S_{ix}$ and $S_{iy}$ have to be there, each with the values $+1$ and $-1$!

- $S_{1y}S_{2y}S_{3x} = -1,$
- $S_{i1}S_{2x}S_{3y} = -1,$
- $S_{1x}S_{2y}S_{3y} = -1.$
What Outcomes Are Possible?

Consider measurement of 45° linear polarization basis

Local realism:

\[ S_{1x} S_{2x} S_{3x} = S_{1x} (S_{1y})^2 S_{2x} (S_{2y})^2 S_{3x} (S_{3y})^2 \]

\[ = (S_{1x} S_{2y} S_{3y}) (S_{1y} S_{2x} S_{3y}) (S_{1y} S_{2y} S_{3y}) \]

\[ = -1 \]

Possible outcomes:

\[ V_1'V_2'V_3', H_1'H_2'V_3', H_1'V_2'H_3', V_1'H_2'H_3' \]
What Outcomes Are Possible?

Quantum physics

\[ |\psi_{123}\rangle = \frac{1}{2} \left( H_1 H_2 H_3 + H_1 V_2 V_3 + V_1 H_2 V_3 + V_1 V_2 H_3 \right) \]

\[ \Rightarrow S_{1x} S_{2x} S_{3x} = 1! \]

Possible outcomes:

\[ H_1 H_2 H_3', H_1 V_2 V_3', V_1 H_2 V_3', V_1 V_2 H_3' \]

Whenever local realism predicts a specific result definitely to occur for a measurement for one of the photons based on the results for the other two, quantum physics definitely predicts the opposite result.
First observation of quantum entanglement

The Angular Correlation of Scattered Annihilation Radiation*

C. S. Wu and I. Shaknov
Pupin Physics Laboratories, Columbia University, New York, New York
November 21, 1949

Phys. Rev. 27, 136 (1950)
• Freedman & Clauser, PRL 28, 938 (1972)
• Fry & Thompson, PRL 37, 465 (1976)

Two measurement sites are not space-like separated
Experimental Test of Bell Inequality

Aspect et al., PRL 49, 1804 (1982)

\[ S_{\text{exp}} = 0.101 \pm 0.020 \] violates a generalized inequality \( S \leq 0 \) by 5 standard deviations

Drawbacks: 1. locality loophole
2. detection loophole
Measurement devices may “tell” the EPR source their basis choices → the source may “select” according events to violate Bell inequality

Solution: basis choice and emission of EPR source must be also space-like separated (i.e., fast and random switch of measurement basis)
Experimental Test of Bell Inequality

Weihs et al., PRL 81, 5039 (1998)

\[ S_{\text{exp}} = 2.73 \pm 0.02 \] violates CHSH inequality \( S \leq 2 \) by 30 standard deviations

Drawback: detection loophole
Detection efficiency of single photon detectors is not unity ⇒ some events cannot contribute to $S > 2$ were not detected?

Solution: high detection efficiency (>83%)

Pearle, PRD 2, 1418 (1970)

Close both detection loophole and locality loophole
• Detection efficiency > 95%
• Switch time: 480 ns < 493 m/c

But still with loopholes...
**Freedom of Choice and Collapse Locality Loophole**

- **Freedom of choice loophole:** random number generators (RNGs) could be prior correlated → the choice of measurement bases are not truly random
  
  Brunner et al., RMP 86, 419 (2014)

- **Collapse locality loophole:** measurement outcome is not defined until it is registered by a human consciousness ➔
  
  Realized "events" have never been space-like separated
  
  Kent, PRA 72, 012107 (2005)
  
  Leggett, Compendium of Quantum Physics (Springer, 2009)
Bell-test experiment with human-observer

Solution for both loopholes: Bell-test experiment with human-observer!

☑ Basis choice by free will
☑ Measurement outcomes defined by consciousness

Leggett, Compendium of Quantum Physics (Springer, 2009)

Requirement:
Quantum signal transit time exceeds human reaction 100ms ➞
entanglement distribution at a distance on the order of one light-second
Quantum Information Processing (QIP)

Test of quantum nonlocality

Coherent manipulation of quantum systems
Enabling encode and process information in quantum states, outperform classical information systems in terms of

Unconditional security
Quantum communication

Computational capacities
Quantum computation and simulation

Super-resolution
Quantum metrology
Part 2: Quantum Communication
Quantum Key Distribution (QKD)

- **Single-photon-based key distribution:** [Bennett & Brassard 1984 protocol]

- **Entanglement-based key distribution:** [Ekert, PRL 67, 661 (1991)]
Error rate: \(50\% \times 50\% = 25\%\)
If Eve is present, the probability that Alice and Bob can not tell is \((0.25)^N\) after they compare \(N\) raw key's value!
BB84 Security

<table>
<thead>
<tr>
<th></th>
<th>one-way communication</th>
<th>two-way communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upper bound</td>
<td>14.6%</td>
<td>25%</td>
</tr>
<tr>
<td>Lower bound</td>
<td>11.0%</td>
<td>18.9%</td>
</tr>
</tbody>
</table>

- All the error rates are brought by the eavesdropping
- When the error rate is lower than the lower bound, we can utilize some classical cryptography method to let Eve know nothing about the key
- If the error rate is higher than the upper bound, the key is insecure

*Gottesman and Lo, IEEE TIT 49, 457 (2003)*
Perfect Cipher in Principle

QKD $\Rightarrow$ Secure key

+ One-time pad

- First Discovered by Gilbert Vernam
- Security Proved by Claude Shannon

[Bell Syst. Tech. J,28,656 (1949) ]

Unconditional security!
Dense Coding

Transmit two bits of information by sending one photon

Transformations between 4 Bell states:

\[ |\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}} (|H\rangle_1|H\rangle_2 + |V\rangle_1|V\rangle_2) \]

\[ |\Psi^+\rangle_{12} = \sigma_{X1}|\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}} (|H\rangle_1|V\rangle_2 + |V\rangle_1|H\rangle_2) \]

\[ |\Phi^-\rangle_{12} = \sigma_{Z1}|\Phi^+\rangle_{12} \frac{1}{\sqrt{2}} (|H\rangle_1|H\rangle_2 - |V\rangle_1|V\rangle_2) \]

\[ |\Psi^-\rangle_{12} = -i\sigma_{Y1}|\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}} (|H\rangle_1|V\rangle_2 + |V\rangle_1|H\rangle_2) \]

Bennett & Wiesner, PRL 69, 2881 (1992)
1. Alice and Bob share an entangled photon pair in the state of $|\Phi^+\rangle_{12}$

2. Bob chooses one of the four unitary transformation on his photon. The information of which choice is 2 bit.

   e.g. 00: $I$ 01: $\sigma_Z$ 10: $\sigma_X$ 11: $-i\sigma_Y$

3. Bob sends his photon to Alice

4. Alice does a joint Bell-state measurement (BSM) on the photon from Bob and her photon.

5. With the measurement result, she can know Bob’s unitary transformation and achieve the 2 bit information.
Quantum Teleportation

- Classical physics
  Scanning and reconstructing

- Quantum physics
  Principle of quantum measurement forbidden extracting all the information from an unknown quantum state!
Quantum Teleportation

Initial state
\[ |\Phi\rangle_1 = \alpha |H\rangle_1 + \beta |V\rangle_1 \]

The shared entangled pair
\[ |\Phi^+\rangle_{23} = \frac{1}{\sqrt{2}} (|H\rangle_2 |H\rangle_3 + |V\rangle_2 |V\rangle_3) \]

| \Psi\rangle_{123} = |\Phi\rangle_1 \otimes |\Phi^+\rangle_{23} \\
= |\Phi^\pm\rangle_{12} \otimes (|\alpha \rangle |H\rangle_3 + \beta |V\rangle_3) + \\
= |\Phi^\mp\rangle_{12} \otimes (|\alpha \rangle |H\rangle_3 - \beta |V\rangle_3) + \\
= |\Psi^+\rangle_{12} \otimes (|\alpha \rangle |V\rangle_3 + \beta |H\rangle_3) + \\
= |\Psi^-\rangle_{12} \otimes (|\alpha \rangle |V\rangle_3 - \beta |H\rangle_3) \]

BSM results on particles 1, 2
<table>
<thead>
<tr>
<th>operations on particle 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>[</td>
</tr>
<tr>
<td>[</td>
</tr>
<tr>
<td>[</td>
</tr>
<tr>
<td>[</td>
</tr>
</tbody>
</table>

Bennett et al., PRL 73, 3801 (1993)
Though nowadays we can only teleport two-particle composite system......

Essential ingredient for distributed quantum information processing!
Part 3: Quantum Computation and Quantum Metrology
Quantum Computation

Quantum Parallelism

Bits

<table>
<thead>
<tr>
<th>0 or 1</th>
<th>Qubits</th>
<th>V. S.</th>
<th>0 + 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>00, 01, 10 or 11</td>
<td>00 + 01 + 10 + 11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>000, 001, 010......</td>
<td>000 + 001 + 010 + ......</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Evaluating function $f(x)$ for many different $x$ simultaneously

$$U \frac{1}{\sqrt{2^N}} \sum_{i=0}^{2^N-1} |i\rangle|0\rangle = \frac{1}{\sqrt{2^N}} \sum_{i=0}^{2^N-1} |i\rangle|f(i)\rangle$$

Exponentially speedup!

This is what makes famous quantum algorithms, such as Shor’s algorithm for factoring, or Grover’s algorithm for searching
RSA Encryption and Factorizing

RSA public-key cryptosystem

• Produce a large integer $N$
  \[ m_1 \times m_2 = N, \text{ (with } m_1 \text{ and } m_2 \text{ primes) } \]

• $N$ is made public available and is used as a key ($x$) to encrypt data

• $m_1$ and $m_2$ are the secret keys ($k$) enable one to decrypt the data

\[
\begin{align*}
C &= E_x(P) \\
P &= D_k(C) = D_k(E_x(P))
\end{align*}
\]

$X$: Public Key; $K$: Private Key

$P$: Plain Text; $E$: Encryption; $C$: Ciphertext; $D$: Decryption

Riverst, Shamir and Adleman, MIT/LCS/TR-212, Jan. 1979
• To crack a code, a code breaker needs to factorize $N$

• The security of RSA based on the ease with which $N$ can be calculated from $m_1$ and $m_2$, and the difficulty of calculating $m_1$ and $m_2$ from $N$
Problem: given a number, what are its prime factors?

e.g. a 129-digit odd number which is the product of two large primes,

\[ \begin{align*}
11438162575788886766923577997614661201021829672124236256256184293570 \\
693524573389783059712363958705058989075147599290026879543541 \\
= 3490529510847650949147849619903898133417764638493387843990820577 \\
x 32769132993266709549961988190834461413177642967992942539798288533
\end{align*} \]

Best factorizing algorithm requires sources that grow exponentially in the size of the number: \( \exp \left( O\left( n^{1/3} \log^{2/3} n \right) \right) \), with \( n \) the length of \( N \).
Algorithms for quantum computation: discrete logarithms and factorizing
E.g. factor a 300-digit number with

- Classical THz computer: $10^{24}$ steps $\Rightarrow$ 150,000 years
- Quantum THz computer: $10^{10}$ steps $\Rightarrow$ 1 second!

Foundations of Computer Science, 1994 Proceedings. 35th Annual Symposium

- Code-breaking can be done in minutes, not in millennia
- Public key encryption, based on factoring, will be vulnerable!
Deutsch-Jozsa Algorithm

Deutsch’s problem: two types of functions $f$

Considering input $n$ bits,

• **Constant $f$:** for all $2^n$ inputs, $f=0$ or $f=1$
• **Balanced $f$:** for $2^{n-1}$ inputs, $f=0$, for another $2^{n-1}$ inputs, $f=1$

**Question:** given a function $f$, whether is it constant or balanced?

**Classical deterministic algorithm:** at most $2^{n-1}+1$ inquiries

• All outputs are the same $\Rightarrow$ constant
• At least 1 output is different from others $\Rightarrow$ balanced
Deutsch-Jozsa Algorithm

The simplest example:
(x=0 or 1)

 CONSTANT:
\( f(0) = 1 \)
\( f(1) = 1 \)

 BALANCED:
\( f(0) = 0 \)
\( f(1) = 1 \)

- Classical algorithm needs 2 inquiries
- Deutsch-Jozsa quantum algorithm:
  Assume \( f \) was mapped into a quantum oracle \( U \) satisfying

\[
U |x⟩|y⟩ \rightarrow |x⟩|y \oplus f(x)⟩
\]
e. g.,

\[
U_C = \begin{bmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{bmatrix}
\quad U_B = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{bmatrix}
\]
Deutsch-Jozsa Algorithm

• Prepare two qubits input state $|\psi_i\rangle = |0\rangle|1\rangle$

• Perform Hadamard operation $|\psi_i\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$

• Perform $U$

$$U|x\rangle \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = |x\rangle \left( \frac{|f(x)\rangle - |1 - f(x)\rangle}{\sqrt{2}} \right) = (-1)^{f(x)}|x\rangle \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Output state:

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

• Measure the first qubit on {+/−} basis: $|+\rangle \Rightarrow$ constant $f$, $|−\rangle \Rightarrow$ balanced $f$

Quantum algorithm only needs one inquiry.
Deutsch-Jozsa Algorithm

Consider a more general case with n-bit inputs x: x=0, 1, 2, ..., 2^n-1

• Prepare n+1 qubits input state \( |\psi_i\rangle = |0\rangle^{\otimes n} |1\rangle \)

• Perform Hadamard operation on all qubits \( |\psi_i\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |\rangle \)

The binary representation of x corresponds to values of each qubits, e.g.,

\[
(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) = |00\rangle + |01\rangle + |10\rangle + |11\rangle
= |x = 0\rangle + |x = 1\rangle + |x = 2\rangle + |x = 3\rangle
\]

• Perform \( U \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle |\rangle \)
Deutsch-Jozsa Algorithm

- Measure the first $n$-qubit on $\{+/\}$ basis: $\Rightarrow$ if and only if the output is $|+\rangle^\otimes n$, $f$ is constant

Only needs one inquiry!


Deutsch problem is not a practically important problem, but Deutsch-Jozsa algorithm firstly demonstrated the superiority of quantum computation!
Grover's Search Algorithm

How quickly can you find a needle in a haystack?
The simplest example:
Which one is equal to -1 in a database?

<table>
<thead>
<tr>
<th>Serial</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>......</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1 ......</td>
</tr>
</tbody>
</table>

- **Classically search**
  - Sequentially try all N possibilities
  - Average search takes $N/2$ steps

- **Quantum search**
  - Simultaneously try all possibilities
  - Refining process reveals answer
  - Average search takes $N^{1/2}$ steps
Grover's Search Algorithm

A databased is encoded with a $N \times N$ diagonal matrix $R$ (rotate phase)

$$R = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & -1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{bmatrix}$$

$R|i\rangle = \begin{cases} -|i\rangle, & i = x \\ |i\rangle, & \text{otherwise} \end{cases}$

The task is to find $x$

Take a $m$-qubit register ($2^m=\bar{N}$), and prepare the registers in an equal superposition state of all the states

$$|\varphi\rangle = \frac{1}{\sqrt{\bar{N}}} \sum_{i=0}^{\bar{N}} |i\rangle$$

Perform rotate phase matrix $R$ on the register
Then perform diffusion operator $D$

$$D = \begin{bmatrix}
-1 + \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\
\frac{2}{N} & -1 + \frac{2}{N} & \cdots & \frac{2}{N} \\
\vdots & \vdots & \ddots & \vdots \\
\frac{2}{N} & \frac{2}{N} & \cdots & -1 + \frac{2}{N}
\end{bmatrix}$$

Iterations of operators $R$ and $D$

Measure the register to get the specific state $|x\rangle$ with nearly unity probability
Grover's Search Algorithm

Formulas

- **Initial state:**

  \[
  |\varphi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N} |i\rangle = \frac{1}{\sqrt{N}} |x\rangle + \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} i \equiv |\alpha\rangle + |\beta\rangle
  \]

- **Phase rotation \( R \):**

  \[
  R|\varphi\rangle = -|\alpha\rangle + |\beta\rangle
  \]

- **Diffusion operator \( D \):**

  \[
  DR|\alpha\rangle = \left(1 - \frac{2}{N}\right)|\alpha\rangle - \frac{2}{N} |\beta\rangle
  \]

  \[
  DR|\beta\rangle = \left(2 - \frac{2}{N}\right)|\alpha\rangle + \left(1 - \frac{2}{N}\right)|\beta\rangle
  \]

  \[
  DR|\varphi\rangle = \left(3 - \frac{4}{N}\right)|\alpha\rangle + \left(1 - \frac{4}{N}\right)|\beta\rangle
  \]
**Grover’s Search Algorithm**

### Formulas

- After n iteration:
  \[ |\varphi_n\rangle = (DR)^n|\varphi\rangle \approx \sin \left( \frac{2n}{\sqrt{N}} \right) |x\rangle + \frac{\cos \left( \frac{2n}{\sqrt{N}} \right)}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \]

- The probability to collapse into the \( x \)
  \[ P = \left| \sin \left( \frac{2n}{\sqrt{N}} \right) \right|^2 \]

- Choose iteration steps
  \[ n = \left\lceil \frac{\pi}{4} \sqrt{N} \right\rceil \]

- The probability of failure:
  \[ 1 - P \leq \cos^2 \left( \frac{\pi}{2} - \frac{1}{\sqrt{N}} \right) \xrightarrow{N \to \infty} 0 \]

*Grover, PRL 79, 325 (1997)*
Quantum Metrology

Super-resolution with multi-particle entanglement

Single particle:
\[ |\psi\rangle = |0\rangle + e^{i\phi}|1\rangle \]

N-particle NOON state
\[ |\psi\rangle = |00\ldots0\rangle + e^{iN\phi}|11\ldots1\rangle \]

Phase uncertainty with N sampling: \( 1/\sqrt{N} \)

Phase uncertainty with same cost of resource N: \( 1/N \)
Part 4: Quantum Repeaters and Quantum Error Correction
Unavoidable interaction with environment and decoherence will happen

\[ |0\rangle\langle E| \xrightarrow{U(t)} |0\rangle\langle E_0(t)| \quad |1\rangle\langle E| \xrightarrow{U(t)} |1\rangle\langle E_1(t)| \]

• \(|0\rangle, |1\rangle\) represents the qubit state and \(|E\rangle\) represents the environment initial state, \(U(t)\) is the joint unitary time evolution operator.

• For arbitrary qubit state:

\[
(\alpha_0|0\rangle + \alpha_1|1\rangle)\langle E| \xrightarrow{U(t)} \alpha_0|0\rangle\langle E_0(t)| + \alpha_1|1\rangle\langle E_1(t)| \quad \rho_q(t) = Tr_E\rho_{q+E} = \begin{bmatrix}
|\alpha_0|^2 & \alpha_0\alpha_1^* \langle E_1|E_0\rangle \\
\alpha_1\alpha_0^* \langle E_0|E_1\rangle & |\alpha_1|^2
\end{bmatrix}
\]

The off-diagonal element of the qubit density matrix will drop down with the rate \(\langle E_0(t)|E_1(t)\rangle = e^{-\Gamma t}\)

The maximally entangled state will be in some mixed state with a certain entanglement fidelity due to the process.
Photon loss increases exponentially with channel length: $A \propto e^{-\Gamma L}$ (e.g., in commercial fiber $\Gamma = 0.2\text{dB/km}$)

For 1000 km commercial fiber, even with a perfect 10 GHz single-photon source and ideal detectors, only 0.3 photon can be transmitted on average per century!
Solutions in Quantum Communication

Quantum repeater

- Solution to photon loss: Entanglement swapping
- Solution to decoherence: Entanglement purification

Briegel et al., PRL 81, 5932 (1998)
Entanglement Swapping

Entangling the remote particles which never interacted!

\[
|\Psi\rangle_{1234} = |\Phi^+\rangle_{14} \otimes |\Phi^+\rangle_{23}
\]

\[
= |\Phi^+\rangle_{12} \otimes |\Phi^+\rangle_{34} + |\Phi^-\rangle_{12} \otimes |\Phi^-\rangle_{34} + |\Psi^+\rangle_{12} \otimes |\Psi^+\rangle_{34} + |\Psi^-\rangle_{12} \otimes |\Psi^-\rangle_{34}
\]

Zukowski et al., PRL 71, 4287 (1993)
Entanglement Swapping

- Probability of transmission with channel loss: $P^2$

- Without entanglement swapping, the total cost in multi-stage is $\sim 1/P^{2N}$
- With entanglement swapping, the total cost is $\sim 1/P^2$
  (assume that the emission probability of ERP sources is unity)
Initially pure singlet state

\[ |\psi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2) \]

Mixed state:

\[ M = \sum_{i=1}^{n} E_i |\psi^-\rangle\langle \psi^- | E_i^\dagger \]

Fidelity:

\[ F = \langle \psi^- | M | \psi^- \rangle \]

Goal: to extract from a large ensemble of low-fidelity M a small sub-ensemble with sufficiently high fidelity
Random bilateral Pauli rotation on each photon in the states $M$ change arbitrary mixed state into Werner state: [Werner, PRA 40, 4277 (1989)]

$$W_F = F|\psi^-\rangle\langle\psi^-| + \frac{1-F}{3}|\psi^+\rangle\langle\psi^+| + \frac{1-F}{3}|\phi^+\rangle\langle\phi^+| + \frac{1-F}{3}|\phi^-\rangle\langle\phi^-|$$

For two same pairs of Werner states, we consider them as source pair and target pair respectively.

A unilateral $\sigma_Y$ is performed on each of the two pairs: $|\psi^\pm\rangle \leftrightarrow |\phi^\mp\rangle$

i.e., states with a large component ($F > 1/2$) of $|\phi^+\rangle$, and equal components of the other three Bell states.
Perform CNOT operation on source and target pairs:

Measure target pair in \{H/V\} basis, keep the unmeasured source pair when measuring results are same

<table>
<thead>
<tr>
<th>Probability</th>
<th>Source</th>
<th>Target</th>
<th>Source</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>(F^2)</td>
<td>(</td>
<td>\Phi^+\rangle)</td>
<td>(</td>
<td>\Phi^+\rangle)</td>
</tr>
<tr>
<td>(F(1 - F)/3)</td>
<td>(</td>
<td>\Phi^-\rangle)</td>
<td>(</td>
<td>\Phi^+\rangle)</td>
</tr>
<tr>
<td>(F(1 - F)/3)</td>
<td>(</td>
<td>\psi^+\rangle)</td>
<td>(</td>
<td>\Phi^+\rangle)</td>
</tr>
<tr>
<td>(F(1 - F)/3)</td>
<td>(</td>
<td>\psi^-\rangle)</td>
<td>(</td>
<td>\Phi^+\rangle)</td>
</tr>
<tr>
<td>((1 - F)^2/9)</td>
<td>(</td>
<td>\psi^+\rangle)</td>
<td>(</td>
<td>\psi^+\rangle)</td>
</tr>
<tr>
<td>((1 - F)^2/9)</td>
<td>(</td>
<td>\psi^-\rangle)</td>
<td>(</td>
<td>\psi^+\rangle)</td>
</tr>
<tr>
<td>(F(1 - F)/3)</td>
<td>(</td>
<td>\Phi^+\rangle)</td>
<td>(</td>
<td>\psi^+\rangle)</td>
</tr>
<tr>
<td>((1 - F)^2/9)</td>
<td>(</td>
<td>\Phi^-\rangle)</td>
<td>(</td>
<td>\psi^+\rangle)</td>
</tr>
<tr>
<td>((1 - F)^2/9)</td>
<td>(</td>
<td>\psi^+\rangle)</td>
<td>(</td>
<td>\psi^-\rangle)</td>
</tr>
<tr>
<td>((1 - F)^2/9)</td>
<td>(</td>
<td>\psi^-\rangle)</td>
<td>(</td>
<td>\psi^-\rangle)</td>
</tr>
<tr>
<td>(F(1 - F)/3)</td>
<td>(</td>
<td>\Phi^+\rangle)</td>
<td>(</td>
<td>\psi^-\rangle)</td>
</tr>
<tr>
<td>((1 - F)^2/9)</td>
<td>(</td>
<td>\Phi^-\rangle)</td>
<td>(</td>
<td>\psi^-\rangle)</td>
</tr>
</tbody>
</table>
After that, the component of $|\Phi^+\rangle\langle\Phi^+|$ of the target pair will be

$$F' = \frac{F^2 + \frac{1}{9}(1 - F)^2}{F^2 + \frac{2}{3}F(1 - F) + \frac{5}{9}(1 - F)^2} > F, \quad \text{when } F > \frac{1}{2}$$

Equivalently, the fidelity $\langle\Psi^-|M|\Psi^-\rangle$ is equal to $F'$

Via several this kind processes, we can purify a general mixed state into a highly entangled state

Bennett et al., PRL 76, 722 (1996)
Quantum error correction

Analogy between classical error correction:

Goal: store an unknown single bit for a time $t$

Errors:

- In a time interval $\tau$ one error occurs with the probability $P_\tau$
- Only one type of error: bit flips $0 \rightarrow 1, 1 \rightarrow 0$
- Suppose errors cause each physical bit to be flipped independently
Correct the errors by using a "redundant coding", e.g.:

- Physical bits 000 → Logical bit 0
- Physical bits 111 → Logical bit 1

Network for encoding:

Network for decoding:
After the errors occur

- Probability of no errors: \((1 - P_\tau)^3\)
- Probability of error in one bit: \(3P_\tau(1 - P_\tau)^2\)
- Probability of error in two bits: \(3P_\tau^2(1 - P_\tau)\)
- Probability of error in three bits: \(P_\tau^3\)
Correction for a long time

To keep the state for a very long time \( t \):

Correct errors as frequently as possible

- Consider \( P_\tau = c\tau \) for time \( \tau \) sufficiently short
- Divide \( t \) in \( N \) intervals of duration \( \tau = t/N \)
- After the time \( t \):

\[
P_t^c = \left[ 1 - 3 \left( \frac{ct}{N} \right)^2 + 2 \left( \frac{ct}{N} \right)^3 \right] \to 1, \text{ when } N \gg 3(ct)^3
\]

Zeno effect!
Decode the logical bits by taking the majority answer of the three bits and correct the encoded bits

- $000 \rightarrow 000$
- $001 \rightarrow 000$ (with correction)
- $010 \rightarrow 000$
- $100 \rightarrow 000$
- $111 \rightarrow 111$
- $011 \rightarrow 111$
- $101 \rightarrow 111$
- $110 \rightarrow 111$

The correct state with a probability

$$P^c_T = (1 - P_T)^3 + 3P_T(1 - P_T)^2 = 1 - 3P_T^2 + 2P_T^3$$
Quantum Errors

- Measurement of error destroys superpositions
- No-cloning theorem prevents repetition
- Multiple types of errors

- **Bit flip** ($\sigma_X$): $\sigma_X(\alpha|0\rangle + \beta|1\rangle) \rightarrow \alpha|1\rangle + \beta|0\rangle$
- **Phase flip** ($\sigma_Z$): $\sigma_Z(\alpha|0\rangle + \beta|1\rangle) \rightarrow \alpha|0\rangle - \beta|1\rangle$
- **Mixed** ($\sigma_Y$): $-i\sigma_Y(\alpha|0\rangle + \beta|1\rangle) \rightarrow \alpha|1\rangle - \beta|0\rangle$
A 3-bit quantum error correction scheme uses an encoder and a decoder circuit. Logical qubit is encoded to three qubits. Measure syndrome qubits. Operations according to measurement results. Any correction must be done without looking at the output.
3-qubit Error Correction

Similar to classical error correction $|0\rangle \rightarrow |000\rangle$ $|1\rangle \rightarrow |111\rangle$

Superposition $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$

Quantum circuit for encoding

Decoder looks just like the encoder
3-qubit Error Correction

All the possible error conditions

<table>
<thead>
<tr>
<th>Error</th>
<th>Decoded</th>
<th>Correction</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha</td>
<td>000\rangle + \beta</td>
<td>111\rangle$</td>
</tr>
<tr>
<td>$\alpha</td>
<td>100\rangle + \beta</td>
<td>011\rangle$</td>
</tr>
<tr>
<td>$\alpha</td>
<td>010\rangle + \beta</td>
<td>101\rangle$</td>
</tr>
<tr>
<td>$\alpha</td>
<td>001\rangle + \beta</td>
<td>110\rangle$</td>
</tr>
</tbody>
</table>

After decoding, the states of syndrome qubits are orthogonal enabling to distinguish which qubit is the error occurred on.
**Phase-Flip Error Correction**

**Phase flip:** \( \alpha |0\rangle + \beta |1\rangle \rightarrow \alpha |0\rangle - \beta |1\rangle \)  
Represent with \{+/-\} basis \(|\pm\rangle = \frac{1}{\sqrt{2}} (|0\rangle \pm |1\rangle)\)

\((\alpha + \beta) |+\rangle + (\alpha - \beta) |-\rangle \rightarrow (\alpha + \beta) |-\rangle + (\alpha - \beta) |+\rangle \)  
**Bit flip error in \{+/-\} basis**

Similar to bit flip error correction, a logical qubit is encoded with

\[
|0\rangle \rightarrow |++ +\rangle \quad |1\rangle \rightarrow |-- --\rangle
\]

\[
\alpha |0\rangle + \beta |1\rangle
\]

\[
|0\rangle
\]

\[
|0\rangle
\]

**Encoder**

**Decoder**
Shor's 9 Qubits Error Correcting Code

**Concatenated code**

- **Bit flip error correction:** $|0\rangle \rightarrow |000\rangle$  $|1\rangle \rightarrow |111\rangle$

  Consider $|000\rangle$ as $|0\rangle'$, $|111\rangle$ as $|1\rangle'$

- **Phase flip error correction:** $|0\rangle' \rightarrow |+\,' +\,' +\,'\rangle$  $|1\rangle' \rightarrow |-\,' -\,' -\,'\rangle$

  Corrects both bit flip and phase flip errors!

$|0\rangle \rightarrow \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right)^3$  $|1\rangle \rightarrow \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right)^3$

Shor, PRA 52, 2493 (1995)
• **General single-qubit error**: $E = c_0 I + c_1 \sigma_Z + c_1 \sigma_X + c_3 \sigma_X \sigma_Z$

• Each term will be represented with orthogonal states of syndrome bits ➔ If a code can correct both bit flip and phase flip errors, it can correct arbitrary single-qubit error!
More Efficient Code

The Steane (CSS) code

$$\begin{align*}
|0\rangle & \rightarrow |0_L\rangle = \frac{1}{\sqrt{8}} \left[ |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\
& \quad + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \right] \\
|1\rangle & \rightarrow |1_L\rangle = \frac{1}{\sqrt{8}} \left[ |1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\
& \quad + |1100000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle \right]
\end{align*}$$

Calderbank and Shor, PRA 54, 1098 (1996)
What is The Minimum Number to Encode 1 Qubit?

Argument

- Encode 1 logical qubit using \( n \) physical qubits
- \( n-1 \) syndrome bits \( \Rightarrow \) them can represent \( 2^{n-1} \) states at most
- \( n \) qubits \( \Rightarrow \) \( 3n \) possible errors and also the case of no errors

\[ n \text{ must satisfies: } 3n + 1 \leq 2^{n-1} \]

The minimum number in theory is 5
5 Qubits Error Correcting Code

\[ |0\rangle \xrightarrow{\text{encode}} \frac{1}{\sqrt{8}} (|00000\rangle - |01111\rangle - |10011\rangle + |11100\rangle \]
\[ + |00110\rangle + |01001\rangle + |10101\rangle + |11010\rangle) \]

\[ |1\rangle \xrightarrow{\text{encode}} \frac{1}{\sqrt{8}} (|11111\rangle - |10000\rangle + |01100\rangle - |00011\rangle \]
\[ + |11001\rangle + |10110\rangle - |01010\rangle - |00101\rangle) \]

Laflamme et al., PRL 77, 198 (1996)
5 Qubits Error Correcting Code

\[ \alpha |0\rangle + \beta |1\rangle \xrightarrow{\text{encode}} \alpha \frac{1}{\sqrt{8}} \left( |0_1 0_2 0_3 0_4 0_5\rangle - |0_1 0_2 1_3 1_4 1_5\rangle - |1_0 2_0 0_3 1_4 1_5\rangle + |1_1 2_0 1_4 0_5\rangle \\
+ |0_1 0_2 1_3 1_4 0_5\rangle + |0_1 2_0 0_3 0_4 1_5\rangle + |1_0 2_1 0_3 1_4 1_5\rangle + |1_1 2_0 3_4 0_5\rangle \right) \\
+ \beta \frac{1}{\sqrt{8}} \left( |1_1 2_1 1_4 1_5\rangle - |1_1 0_2 0_3 0_4 0_5\rangle + |0_1 1_2 3_0 4_0 5\rangle - |0_1 0_2 0_3 4_1 1_5\rangle \\
+ |1_1 2_0 3_0 4_1 5\rangle + |1_0 2_1 3_1 4_0 5\rangle - |0_1 0_2 3_1 4_0 5\rangle - |0_1 0_2 3_1 4_0 5\rangle \right) \]

**Encoding circuit**

\[ |0\rangle \]
\[ |0\rangle \]
\[ \alpha |0\rangle + \beta |1\rangle \]
\[ |0\rangle \]
\[ |0\rangle \]

**Phase shift \( \pi \)**
Rules of Shifting Phase and Flip Bit

If qubit 1 is '1', **flip qubits 3 and 5**

If qubits 2, 3 and 4 are '1', **shift the phase**

If qubits 2 and 4 is '0' and qubit 3 is '1', **shift the phase**
Signal after Hadamards

Hadamard

\[
\left(\frac{\left|0_1\right> + \left|1_1\right>}{\sqrt{2}}\right) \left(\frac{\left|0_2\right> + \left|1_2\right>}{\sqrt{2}}\right) (\alpha \left|0_3\right> + \beta \left|1_3\right>) \left(\frac{\left|0_4\right> + \left|1_4\right>}{\sqrt{2}}\right) \left|0_5\right>
\]

\[
= \frac{1}{\sqrt{4}} \left(\left|0_10_2\right> + \left|0_11_2\right> + \left|1_10_2\right> + \left|1_11_2\right>\right) (\alpha \left|0_3\right> + \beta \left|1_3\right>) \frac{1}{\sqrt{2}} \left(\left|0_40_5\right> + \left|1_40_5\right>\right)
\]

\[
= \frac{\alpha}{\sqrt{8}} \left(\left|0_10_20_30_40_5\right> + \left|0_11_20_30_40_5\right> + \left|1_10_20_30_40_5\right> + \left|1_11_20_30_40_5\right>ight.
\]

\[
+ \left|0_10_20_31_40_5\right> + \left|0_11_20_31_40_5\right> + \left|1_10_20_31_40_5\right> + \left|1_11_20_31_40_5\right>)
\]

\[
+ \frac{\beta}{\sqrt{8}} \left(\left|0_10_21_30_40_5\right> + \left|0_11_21_30_40_5\right> + \left|1_10_21_30_40_5\right> + \left|1_11_21_30_40_5\right>
\]

\[
+ \left|0_10_21_31_40_5\right> + \left|0_11_21_31_40_5\right> + \left|1_10_21_31_40_5\right> + \left|1_11_21_31_40_5\right>)
\]
Step-by-step Analysis of Encoding Circuit

\[ \frac{\alpha}{\sqrt{8}} (|Q_2 Q_3 Q_4 Q_5 \rangle + |Q_1 Q_3 Q_4 Q_5 \rangle + |1 Q_2 Q_3 Q_4 Q_5 \rangle + |1_2 Q_3 Q_4 Q_5 \rangle + |Q_2 Q_3 Q_4 Q_5 \rangle + |Q_1 Q_3 Q_4 Q_5 \rangle + |1 Q_2 Q_3 Q_4 Q_5 \rangle + |1_2 Q_3 Q_4 Q_5 \rangle) \]

\[ + \frac{\beta}{\sqrt{8}} (|Q_2 Q_3 Q_4 Q_5 \rangle + |Q_1 Q_3 Q_4 Q_5 \rangle + |1 Q_2 Q_3 Q_4 Q_5 \rangle + |1_2 Q_3 Q_4 Q_5 \rangle + |Q_2 Q_3 Q_4 Q_5 \rangle - |Q_1 Q_3 Q_4 Q_5 \rangle - |1 Q_2 Q_3 Q_4 Q_5 \rangle - |1_2 Q_3 Q_4 Q_5 \rangle) \]

Shifting phase when 2, 3, 4 are “1”

Shifting phase when 2, 4 are “0” and 3 is “1”
Step-by-step Analysis of Encoding Circuit

\[ \frac{\alpha}{\sqrt{8}} \left( |Q_1 Q_2 Q_3 Q_4 Q_5 \rangle + |Q_1' Q_2 Q_3 Q_4 Q_5 \rangle + |1_1 Q_2 Q_3 Q_4 Q_5 \rangle + |1_1 Q_2 Q_3 Q_4 Q_5 \rangle 
+ |Q_1 Q_2 Q_3 Q_4 Q_5 \rangle + |Q_1 Q_2 Q_3 Q_4 Q_5 \rangle + |1_1 Q_2 Q_3 Q_4 Q_5 \rangle + |1_1 Q_2 Q_3 Q_4 Q_5 \rangle \right) \]

\[ + \frac{\beta}{\sqrt{8}} \left( -|Q_1 Q_2 Q_3 Q_4 Q_5 \rangle + |Q_1 Q_2 Q_3 Q_4 Q_5 \rangle - |1_1 Q_2 Q_3 Q_4 Q_5 \rangle + |1_1 Q_2 Q_3 Q_4 Q_5 \rangle \right) \]

Flipping bits 5 when bit 3 is “1” and then flipping bit 3 and 5 when bit 1 is “1”

Flipping bits 3 and 5 with “1” in bits 2 and 4
Step-by-step Analysis of Encoding Circuit

\[ \frac{\alpha}{\sqrt{8}} (|0_1 0_2 0_3 0_4 0_5 \rangle + |0_1 1_2 0_3 0_4 1_5 \rangle + |1_1 0_2 1_3 0_4 1_5 \rangle + |1_1 1_2 1_3 0_4 0_5 \rangle ) \]
\[ + |0_1 0_2 1_3 1_4 0_5 \rangle - |0_1 1_2 1_3 1_4 1_5 \rangle - |1_1 0_2 0_3 1_4 1_5 \rangle + |1_1 1_2 0_3 1_4 0_5 \rangle ) \]
\[ + \frac{\beta}{\sqrt{8}} (|0_1 0_2 1_3 0_4 1_5 \rangle + |0_1 1_2 1_3 0_4 0_5 \rangle - |1_1 0_2 0_3 0_4 0_5 \rangle + |1_1 1_2 0_3 0_4 1_5 \rangle ) \]
\[ - |0_1 0_2 0_3 1_4 1_5 \rangle - |0_1 1_2 0_3 1_4 0_5 \rangle + |1_1 0_2 1_3 1_4 0_5 \rangle + |1_1 1_2 1_3 1_4 1_5 \rangle ) \]

Shifting phase in data bit when bits 4 and 5 are “1″
• Assuming at most 1 qubit error and the error is just as likely to affect any qubit

• The decoding circuit is the encoding circuit in reverse:
Example: Error is Phase and Bit Flip on 3rd Qubit

Assume encoded qubit damaged such that:

$$\frac{a}{\sqrt{8}} (|0_10_20_30_40_5\rangle - |0_11_21_31_41_5\rangle - |1_10_20_31_41_5\rangle + |1_11_21_30_40_5\rangle$$
$$+ |0_10_21_31_40_5\rangle + |0_11_20_30_41_5\rangle + |1_10_21_30_41_5\rangle + |1_11_20_31_40_5\rangle)$$
$$+ \frac{b}{\sqrt{8}} (|1_11_21_31_41_5\rangle - |1_10_20_30_40_5\rangle + |0_11_20_31_40_5\rangle - |0_10_20_31_40_5\rangle$$
$$+ |1_11_20_31_40_5\rangle + |1_10_21_31_40_5\rangle - |0_11_20_31_40_5\rangle - |0_10_21_31_40_5\rangle)$$

Phase and bit flip on 3rd qubit \((-i\sigma_y)\)
Continuation of Error Analysis in Decoder

\[ \frac{\alpha}{\sqrt{8}} \left( |0,0,1,0,0,0,0,0,0,1\rangle + |0,1,0,0,1,0,0,0,0,0\rangle + |0,1,1,0,1,0,0,0,0,0\rangle - |0,1,0,1,1,0,0,0,0,0\rangle - |1,1,0,0,1,0,0,0,0,0\rangle - |1,1,1,0,1,0,0,0,0,0\rangle \right) 

+ \frac{\beta}{\sqrt{8}} \left( - |1,1,0,0,1,0,0,0,0,0\rangle - |1,1,1,0,1,0,0,0,0,0\rangle - |0,1,0,0,1,0,0,0,0,0\rangle - |0,1,1,0,1,0,0,0,0,0\rangle + |1,1,0,0,1,0,0,0,0,0\rangle + |1,1,1,0,1,0,0,0,0,0\rangle \right) \]

Phase and bit flip on 3rd qubit

Shift phase when bits 4 and 5 are "1"
Continuation of Error Analysis in Decoder

\[ \frac{\alpha}{\sqrt{8}} \left( |0_1 0_2 1_3 0_4 0_5 \rangle - |0_1 1_2 1_3 1_4 0_5 \rangle + |1_1 0_2 0_3 1_4 1_5 \rangle - |1_1 1_2 0_3 0_4 1_5 \rangle 
- |0_1 0_2 1_3 1_4 0_5 \rangle + |0_1 1_2 1_3 0_4 0_5 \rangle - |1_1 0_2 0_3 0_4 1_5 \rangle + |1_1 1_2 0_3 1_4 1_5 \rangle \right) 
+ \frac{\beta}{\sqrt{8}} \left( + |1_1 1_2 1_3 1_4 0_5 \rangle - |1_1 0_2 1_3 1_4 0_5 \rangle - |0_1 1_2 0_3 0_4 1_5 \rangle + |0_1 0_2 0_3 1_4 1_5 \rangle 
+ |1_1 1_2 1_3 0_4 0_5 \rangle - |1_1 0_2 1_3 1_4 0_5 \rangle - |0_1 1_2 0_3 1_4 1_5 \rangle + |0_1 0_2 0_3 0_4 1_5 \rangle \right) \]  

Flipping bit 3 when bit 4 is “1” and flipping bit 5 when bit 2 is “1”

Flipping bits 3 and 5 when bit 1 is “1” and then flipping bit 5 when bit 3 is “1”
Continuation of Error Analysis in Decoder

\[
\frac{\alpha}{\sqrt{8}} \left( -|0_1 0_2 1_3 0_4 1_5\rangle + |0_1 2_1 3_4 1_5\rangle + |1_1 0_2 1_3 1_4 1_5\rangle - |1_1 2_1 1_3 0_4 1_5\rangle \\
- |0_1 0_2 1_3 1_4 1_5\rangle + |0_1 2_1 3_4 0_4 1_5\rangle + |1_1 0_2 1_3 0_4 1_5\rangle - |1_1 2_1 1_3 1_4 1_5\rangle \right)
\]

\[
+ \frac{\beta}{\sqrt{8}} \left( + |1_1 2_0 1_3 4_1 1_5\rangle - |1_1 0_2 0_3 0_4 1_5\rangle - |0_1 2_0 3_0 0_4 1_5\rangle + |0_1 0_2 0_3 1_4 1_5\rangle \\
+ |1_1 2_0 0_3 0_4 1_5\rangle - |1_1 0_2 0_3 1_4 1_5\rangle - |0_1 2_0 3_1 4_1 1_5\rangle + |0_1 0_2 0_3 0_4 1_5\rangle \right)
\]

Shifting phase on bit 5 when 2,3,4 are “1”
Re-express equation to prepare for Hadamard transform:

\[
\frac{\alpha}{\sqrt{8}} \left( -|0_10_21_30_41_5\rangle + |0_11_21_31_41_5\rangle + |1_10_21_31_41_5\rangle - |1_11_21_30_41_5\rangle \\
- |0_10_21_31_41_5\rangle + |0_11_21_30_41_5\rangle + |1_10_21_30_41_5\rangle - |1_11_21_31_41_5\rangle \right) \\
+ \frac{\beta}{\sqrt{8}} \left( + |1_11_20_31_41_5\rangle - |1_10_20_30_41_5\rangle - |0_11_20_30_41_5\rangle + |0_10_20_30_41_5\rangle \\
+ |1_11_20_30_41_5\rangle - |1_10_20_30_41_5\rangle - |0_11_20_30_41_5\rangle + |0_10_20_30_41_5\rangle \right)
\]

\[
= \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left( \frac{\alpha}{\sqrt{4}} \left( -|0101\rangle + |1111\rangle - |0111\rangle + |1101\rangle \right) + \frac{\beta}{\sqrt{4}} \left( -|1001\rangle + |0011\rangle - |1011\rangle + |0001\rangle \right) \right)
\]

\[
= \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left( \frac{\alpha}{\sqrt{2}} \left( -|101\rangle - |111\rangle \right) + \frac{\beta}{\sqrt{2}} \left( |011\rangle + |001\rangle \right) \right)
\]

\[
= \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) (-\alpha |1\rangle + \beta |0\rangle) \left( \frac{|01\rangle + |11\rangle}{\sqrt{2}} \right)
\]

\[
= \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) (-\alpha |1\rangle + \beta |0\rangle) \left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) (|1\rangle) \]

Input to Hadamard
Qubits 1, 2, 4 and 5 are the syndrome bits which indicate the exact error that occurred and the current state of qubit 3:

- So apply a phase shift and a bit flip on qubit 3 to obtain the protected qubit $\alpha|0\rangle + \beta|1\rangle$
### Syndromes Table after Decoding

**Syndrome qubits:** q1, q2, q4, q5  **Output qubit:** q3

<table>
<thead>
<tr>
<th>Syndrome states</th>
<th>Error on</th>
<th>Output qubit</th>
</tr>
</thead>
<tbody>
<tr>
<td>q1   q2   q3   q4   q5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0000</td>
<td>-</td>
<td>$\alpha</td>
</tr>
<tr>
<td>0001</td>
<td>X</td>
<td>$\alpha</td>
</tr>
<tr>
<td>0010</td>
<td>Z</td>
<td>$-\alpha</td>
</tr>
<tr>
<td>0011</td>
<td>X</td>
<td>$-\alpha</td>
</tr>
<tr>
<td>0100</td>
<td>Z</td>
<td>$-\alpha</td>
</tr>
<tr>
<td>0101</td>
<td>Y</td>
<td>$\alpha</td>
</tr>
<tr>
<td>0110</td>
<td>X</td>
<td>$-\alpha</td>
</tr>
<tr>
<td>0111</td>
<td>X</td>
<td>$-\alpha</td>
</tr>
</tbody>
</table>
Recalling that these codes require $P_\tau \propto \tau \ll 1$ for time $\tau$ sufficiently short

- In realistic devices, $\tau$ cannot be infinite small
  - threshold for tolerable error rate

Highest threshold: $2.02 \times 10^{-5}$ Extremely hard to achieve!

Spedalieri et al., Quantum Inf. Comput. 9, 666 (2009)

- A possible solution: Topological error correction!
  - Topological homology of 3D cluster state
    (encoding one logical qubit with 180 physical qubits )
  - Relax the error threshold rate from $10^{-5}$ to $10^{-2}$
Thanks for your attention!