Quantum Information and Communication

quantum mechanics
- uncertainty principle
- wave function
- superposition state

information/communication
- cryptography
- signal processing

Quantum Information/Communication
- quantum cryptography
- quantum computation
Quantum mechanical superposition state
- Schrödinger’s cat -

Q: What is the cat’s state in the box?

A1: The cat is *either* alive *or* dead. It is determinative though not observed.

A2: The cat may be alive *and* dead.

We do not know which, thus it can be alive *and* dead. Both is possible.
Quantum mechanics employs A2; “the cat in the box is alive *and* dead.”

A superposition state is mathematically expressed as:

\[
\text{(cat in the box)} = a \times \text{alive} + b \times \text{dead}
\]

Parameters \(a\) and \(b\) are coefficients representing the probabilities.

When the box is opened, the cat state is instantly determined to be dead *or* alive.
To be a superposition state, whether dead or alive is unknown in principle.

(The cat necessarily dies when the time comes)

Dead or alive is known in principle, even when the box is sealed.

\[
\begin{align*}
\text{before the set time} & \\
\text{after the set time} \\
\end{align*}
\]

\textit{not superposition state}
Anything is composed of minimum units that cannot be further divided.

A material is composed of nuclei and electrons.

Light energy is composed of photons.

Detection signal is discrete.
Superposition state of a photon

Ex.1) A beam-split photon

\[
\text{output photon} = a \times (\text{transmitted photon}) + b \times (\text{reflected photon})
\]

Ex.2) A photon split and recombined

\[
\text{output photon} = a \times (\text{photon} @ \{A, \text{fast}\}) + b \times (\text{photon} @ \{B, \text{slow}\}) + c \times (\text{photon} @ \{A, \text{fast}\}) + d \times (\text{photon} @ \{B, \text{slow}\})
\]
Coefficients in superposition are regarded as wave

Ex.3) A photon split and recombined (2)

Here are postulates;
- A coefficient has a fine structure like wave.
  → The change due to the glass plate is expressed by a shift in the wave-like structure
- The probability is given by its height.
  → The probability is the same for $c$ and $c'$.

$$\text{output photon} = a \times (\text{photon@}\{A, \text{ fast}\})
+ b \times (\text{photon@}\{B, \text{ fast}\})
+ c' \times (\text{photon@}\{A, \text{ slow}\})
+ d' \times (\text{photon@}\{B, \text{ slow}\})$$
Coefficients in superposition behave like wave

Ex. 3) A photon split and recombined (2)

output photon @A = $c_1 \times \text{(photon via L1)} + c_2 \times \text{(photon via L2)}$

= $(c_1 + c_2) \times \text{(photon @A)}$
Total of coefficients depends on relative undulation

+  

II  

enhanced  

canceled
The coefficient of photon via A and that via B are recombined on the screen.
Which slit a photon passes through must be unknown for interference to occur

\[
\text{photon} @ \text{slit} = a \times (\text{photon} @ A) + b \times (\text{photon} @ B)
\]

\[
\text{photon} @ \text{slit} = \begin{cases} 
(\text{photon} @ A) \\
(\text{photon} @ B)
\end{cases}
\]
Applications to information/communication technologies

Utilizing superposition states for cryptography

Quantum cryptography (quantum key distribution)

Utilizing superposition states for computation

Quantum computer
Quantum cryptography

Alice encrypt

Bob decrypt
Public key cryptosystem

Alice

encrypting key (public)

367 \times 521 = ? : easy (answer is 191207 )

\begin{align*}
? & \times ? = 191207 : difficult
\end{align*}

Deciphering is possible in principle

Bob

decrypting key (closed)
Secret key cryptosystem

To provide secret keys to distant parties

The security of the keys is guaranteed by quantum mechanics

Quantum Cryptography (Quantum Key Distribution)

purpose: To provide secret keys to distant parties

selling point: The security of the keys is guaranteed by quantum mechanics
Quantum Cryptography (Quantum Key Distribution)

Cryptosystem utilizing quantum superposition states

Key data are transmitted utilizing interference of a photon.

Eavesdropping is revealed from the state change due to observation.
Configuration of QKD system (example)

Superposition states on temporal position are transmitted

A photon is detected by detector A or B, according to the relative undulation of coefficients
Quantum Computing
—computing utilizing superposition states—

◆ Plural data are simultaneously expressed by a superposition state
◆ Ultra parallel processing utilizing quantum interference
Quantum Bit
- Fundamental element for quantum processing-

Photon’s polarization state
\[ a \times \text{(horizontal state)} + b \times \text{(vertical state)} \]

Electron’s spin state
\[ a \times \text{(up-spin)} + b \times \text{(down-spin)} \]

Atom’s energy state
\[ a \times \text{(upper state)} + b \times \text{(lower state)} \]

Superconducting current state
\[ a \times \text{(right direction)} + b \times \text{(left direction)} \]
Plural data are simultaneously expressed by a superposition

Two quantum bits

Each Q bit is a superposition of ↑ and ↓, thus the whole state is;

\[ | \uparrow \downarrow \uparrow \downarrow > = c_1 | \uparrow \uparrow > + c_2 | \uparrow \downarrow > + c_3 | \downarrow \uparrow > + c_4 | \downarrow \downarrow > \]

\[ = c_1 "1" + c_2 "2" + c_3 "3" + c_4 "4" \]

4 digits are expressed

N quantum bits

\[ 2^n \text{ digits can be simultaneously expressed} \]
Parallel processing utilizing a superposition

Problem:
To find \(x\) satisfying the following equation
\[ f(x) = c \]

classical way

\[
\begin{array}{cccc}
  x_1 & x_2 & x_3 & \cdots & x_n \\
  \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\
  f(x_1) & f(x_2) & f(x_3) & \cdots & f(x_n) \\
  \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\
  a & b & c & \cdots & z \\
\end{array}
\]

Examing all candidates one by one

quantum way

\[
\begin{array}{cccc}
  x_1 & x_2 & x_3 & \cdots & x_n \\
  \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\
  |\phi\rangle = |x_1\rangle + |x_2\rangle + |x_3\rangle + \cdots + |x_n\rangle \\
  \downarrow \\
  U|\phi\rangle = U|x_1\rangle + U|x_2\rangle + U|x_3\rangle + \cdots + U|x_n\rangle \\
  \downarrow \\
  |\phi_{\text{out}}\rangle = 0|x_1'\rangle + 0|x_2'\rangle + 1|x_3'\rangle + \cdots + 0|x_n'\rangle \\
\end{array}
\]

Conducting one operation

(ex) prime decomposition
\[
367 \times 521 = 191207 \\
191207 = x \times y
\]
Image of parallel processing

Simultaneous operation based on interference

prepared state

$\left| 1 \mod N \right>$

$\left| m^1 \mod N \right>$

$\left| m^2 \times 1 \mod N \right>$

$\left| m^{q-1} \mod N \right>$
Unfortunately, implementation is quite difficult.

Quantum bits are very fragile. They easily collapse due to disturbances.
Quantum Information/Communication

quantum mechanics
- uncertainty principle
- wave function
- superposition state

information/communication
- cryptography
- signal processing

quantum cryptography
quantum computation