

Introduction to quantum theory: Quantum states and quantum measurements

Ryuhei Mori

Tokyo Institute of Technology

2, Oct, 2020

What is “Quantum theory”?

Quantum theory

- Physics for microscopic phenomena, e.g., atoms, light.

Why is quantum theory important ?

- Just because it's **reality**.
- Because it gives more **efficient** information processing, e.g., quantum factoring algorithm, quantum secret-key sharing, etc.

On this course

We study **mathematical foundation** of quantum theory.

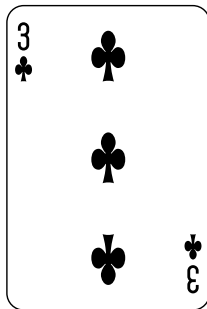
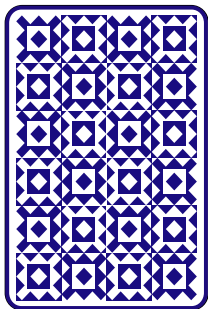
- Mathematical foundation of quantum physics
- Quantum algorithms
- Other quantum information processing, e.g, quantum communication, quantum error-correction.

Score

- Assignments: 100%

<https://github.com/QCQI2020>

Experimental fact



- ✗ The card was the three of club.
- ✓ When we flip the card, we see the three of club.
- State: The card
- Measurement: Flipping the card
- The number on the card before the flipping the card cannot be defined in quantum theory

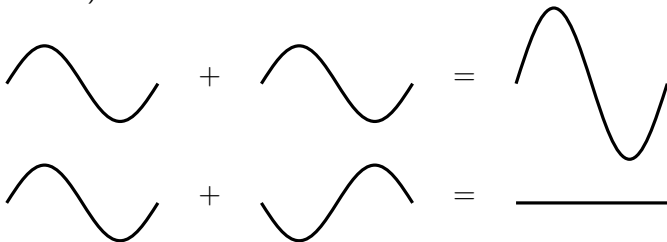
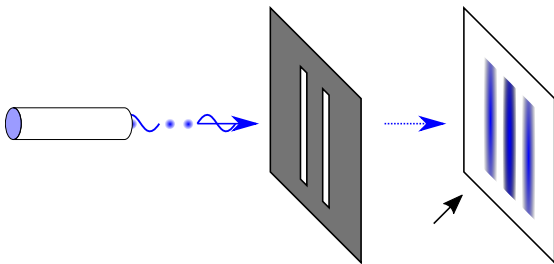
States, measurements and distinguishability

- Two states are equivalent if the probability distributions of outcomes are equal for **arbitrary measurement**.
- Two measurements are equivalent if the probability distributions of outcomes are equal for **arbitrary states**.
- **We should not distinguish states (measurements) mathematically if we cannot distinguish them physically.**

Light is wave (1801)



Thomas Young
(1773 – 1829)

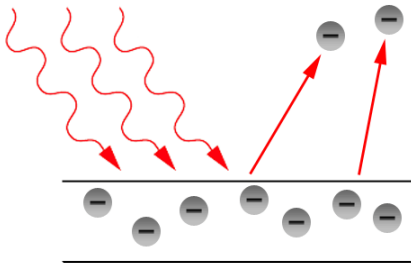


https://en.wikipedia.org/wiki/Young's_interference_experiment

Light is particle (1905)

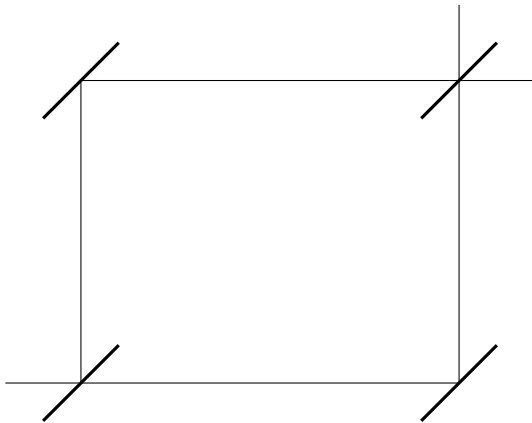


Albert Einstein
(1879 – 1955)



https://en.wikipedia.org/wiki/File:Photoelectric_effect.png

Mach-Zehnder interferometer



Quantum states and quantum measurements

A single photon \Rightarrow BS1 \Rightarrow BS2 \Rightarrow detection

State	Measurement
A single photon \Rightarrow BS1 \Rightarrow BS2	detection
A single photon \Rightarrow BS1	BS2 \Rightarrow detection
A single photon	BS1 \Rightarrow BS2 \Rightarrow detection

All understandings are valid

Mathematical representations of states and measurements

How “States” and “Measurements” are represented mathematically ?

A table of probabilities of outcome 'YES' for each binary measurement on each state

	Measurement 1	Measurement 2	...
State A	p_{A1}	p_{A2}	...
State B	p_{B1}	p_{B2}	...
⋮			

* The number of states and measurements are not necessarily countable.

Linear space

	Measurement 1	Measurement 2	...
State A	p_{A1}	p_{A2}	...
State B	p_{B1}	p_{B2}	...
State C	$0.7p_{A1} + 0.3p_{B1}$	$0.7p_{A2} + 0.3p_{B2}$	

Assumption

- Probabilistic mixture of states is also state.
- Probabilistic mixture of binary measurement is also binary measurement.

States and measurements can be represented by vectors!

Classical theory

States: 0, 1

Binary measurements: 0?, 1?

$$\underline{0}?(\underline{0}) = 1,$$

$$\underline{0}?(\underline{1}) = 0,$$

$$\underline{1}?(\underline{0}) = 0,$$

$$\underline{1}?(\underline{1}) = 1$$

	<u>0</u> ?	<u>1</u> ?
<u>0</u>	1	0
<u>1</u>	0	1

State and measurement

	<u>0</u> ?	<u>1</u> ?
<u>0</u>	1	0
<u>1</u>	0	1

$S := \underline{0}$ with probability p , $\underline{1}$ with probability $1 - p$.

S is also **regarded as a state**.

$$\underline{0}?(S) = p,$$

$$\underline{1}?(S) = 1 - p.$$

Similarly,

$E_1 := \underline{0}?$ with probability p , $\underline{1}?$ with probability $1 - p$.

$E_2 := (\underline{0} \text{ or } \underline{1})?$.

E_1 and E_2 are also **regarded as a binary measurement**.

Linear space

$$\omega_{\underline{0}} := \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

$$e_{\underline{0}} := \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

$$\omega_{\underline{1}} := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$e_{\underline{1}} := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\underline{0}?(0) = \langle e_{\underline{0}}, \omega_{\underline{0}} \rangle,$$

$$\underline{0}?(1) = \langle e_{\underline{0}}, \omega_{\underline{1}} \rangle$$

$$\underline{1}?(0) = \langle e_{\underline{1}}, \omega_{\underline{0}} \rangle,$$

$$\underline{1}?(1) = \langle e_{\underline{1}}, \omega_{\underline{1}} \rangle$$

$S := \underline{0}$ with probability p , $\underline{1}$ with probability $1 - p$

$$\omega_S = p\omega_{\underline{0}} + (1 - p)\omega_{\underline{1}} = \begin{bmatrix} p \\ 1 - p \end{bmatrix}.$$

$$\underline{0}?(S) = p = \langle e_{\underline{0}}, \omega_S \rangle.$$

States and measurements in a linear space

$$\omega_{\underline{0}} := \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

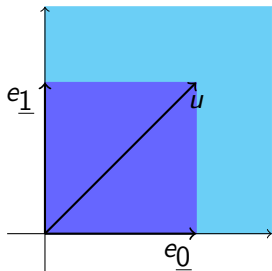
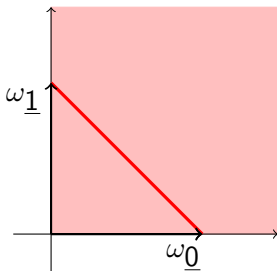
$$\omega_{\underline{1}} := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$e_{\underline{0}} := \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

$$e_{\underline{1}} := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\text{Set of states} = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \mid x \geq 0, y \geq 0, x + y = 1 \right\}.$$

$$\text{Set of binary measurements} = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \mid x \geq 0, y \geq 0, x \leq 1, y \leq 1 \right\}.$$



State and measurement in a linear space

$$\text{Set of states} = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \mid x \geq 0, y \geq 0, x + y = 1 \right\}.$$

$$\text{Set of binary measurements} = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \mid x \geq 0, y \geq 0, x \leq 1, y \leq 1 \right\}.$$

$$\text{Let } C_{\geq 0} \text{ be the set of nonnegative vectors and } u := \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

$$\text{Set of states} = \{ \omega \in \mathbb{R}^2 \mid \omega \in C_{\geq 0}, \langle u, \omega \rangle = 1 \}.$$

$$\text{Set of binary measurements} = \{ e \in \mathbb{R}^2 \mid e \in C_{\geq 0}, u - e \in C_{\geq 0} \}.$$

$$\text{Set of measurements} = \{ (e_1, \dots, e_k) \mid e_1 + \dots + e_k = u, e_i \in C_{\geq 0} \\ i = 1, 2, \dots, k, k = 1, 2, \dots \}$$

Outcome of the measurement $M = (e_1, \dots, e_k)$ on ω is i with probability $\langle e_i, \omega \rangle$.

Quantum theory

$C_{\geq 0} \subseteq \mathbb{R}^2$: the set of nonnegative vectors, $u := \begin{bmatrix} 1 \\ 1 \end{bmatrix}$.

Set of states = $\{\omega \in \mathbb{R}^2 \mid \omega \in C_{\geq 0}, \langle u, \omega \rangle = 1\}$.

Set of binary measurements = $\{e \in \mathbb{R}^2 \mid e \in C_{\geq 0}, u - e \in C_{\geq 0}\}$.

Set of measurements = $\{(e_1, \dots, e_k) \mid e_1 + \dots + e_k = u, e_i \in C_{\geq 0}$
 $i = 1, 2, \dots, k, k = 1, 2, \dots, \}$

V : the linear space on \mathbb{R} spanned by 2×2 Hermitian matrices.
 $\langle e, \omega \rangle := \text{Tr}(e\omega)$ for $\omega, e \in V$ (Hilbert-Schmidt inner product).

$C_{\succeq 0} \subseteq V$: the set of positive semidefinite matrices, $u := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Set of states = $\{\omega \in V \mid \omega \in C_{\succeq 0}, \langle u, \omega \rangle = 1\}$.

Set of binary measurements = $\{e \in V \mid e \in C_{\succeq 0}, u - e \in C_{\succeq 0}\}$.

Linear space spanned by 2x2 Hermitian matrices

Basis

$$A := \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, B := \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, C := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, D := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Another choice of basis

$$I := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Both are orthogonal basis.

The second basis (I and Pauli matrices X , Y and Z) has nice properties.

- 1 $\text{Tr}(I) = 2$. $\text{Tr}(X) = \text{Tr}(Y) = \text{Tr}(Z) = 0$.
- 2 $X^2 = Y^2 = Z^2 = I$ (X , Y and Z have eigenvalues ± 1).
- 3 $XY = -YX$, $YZ = -ZY$, $ZX = -XZ$.

Positive semidefinite cone

$$I := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\rho = \frac{1}{\sqrt{2}} (a_I I + a_X X + a_Y Y + a_Z Z)$$

$$\lambda_1 \geq 0, \lambda_2 \geq 0 \iff \lambda_1 + \lambda_2 \geq 0, \lambda_1 \lambda_2 \geq 0$$

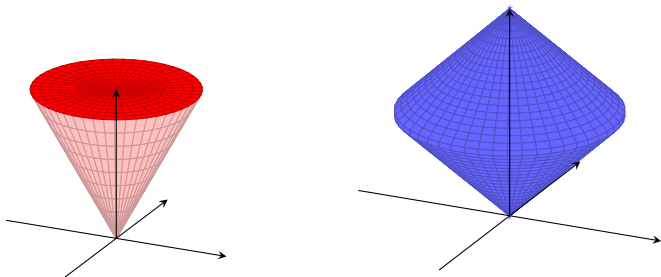
$$\iff \text{Tr}(\rho) \geq 0, \text{Tr}(\rho)^2 - \text{Tr}(\rho^2) \geq 0$$

$$\iff a_I \geq 0, 2a_I^2 - (a_I^2 + a_X^2 + a_Y^2 + a_Z^2) \geq 0$$

$$\iff a_I \geq 0, a_I^2 \geq a_X^2 + a_Y^2 + a_Z^2$$

$$\text{Tr}(\rho) = 1 \iff a_I = \frac{1}{\sqrt{2}}$$

Geometry of quantum states and effects



Convex cone and dual cone

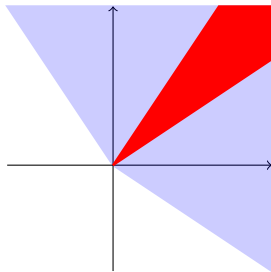
$$C \subseteq V \text{ is a convex cone} \iff x + y \in C, \lambda x \in C, \\ \forall x \in C, y \in C, \lambda \geq 0$$

Proper cone: closed, not V , full-dimensional.

$C^* \subseteq V$ is a dual cone of C

$$\iff C^* := \{x \in V \mid \langle x, y \rangle \geq 0, \forall y \in C\}$$

$C_{\geq 0}$ and $C_{\leq 0}$ are self-dual cones.



Generalized probabilistic theories

C : convex cone.

$u \in$ interior of C^* .

Set of states = $\{\omega \in V \mid \omega \in C, \langle u, \omega \rangle = 1\}$.

Set of effects = $\{e \in V \mid e \in C^*, u - e \in C^*\}$.

Set of measurements = $\{(e_1, \dots, e_k) \mid e_1 + \dots + e_k = u, e_i \in C^*,$
 $i = 1, 2, \dots, k, k = 1, 2, \dots\}$

Classical theory

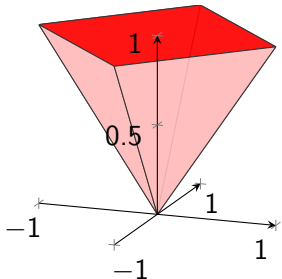
$V = \mathbb{R}^n$, $C = C_{\geq 0}$, u = the all-1 vector.

Quantum theory

V = A set of $n \times n$ Hermitian matrices, $C = C_{\geq 0}$, $u = I$.

Other theories ?

Toy theory: Gbit



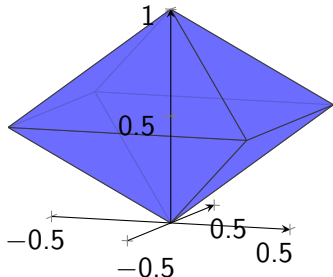
$$\omega_0 = [1 \ 0 \ 1],$$

$$\omega_2 = [-1 \ 0 \ 1],$$

$$e_0 = \frac{1}{2} [1 \ 1 \ 1],$$

$$e_2 = \frac{1}{2} [1 \ -1 \ 1],$$

$$u = [0 \ 0 \ 1].$$



$$\omega_1 = [0 \ 1 \ 1],$$

$$\omega_3 = [0 \ -1 \ 1].$$

$$e_1 = \frac{1}{2} [-1 \ 1 \ 1],$$

$$e_3 = \frac{1}{2} [-1 \ -1 \ 1],$$

Nonlocality

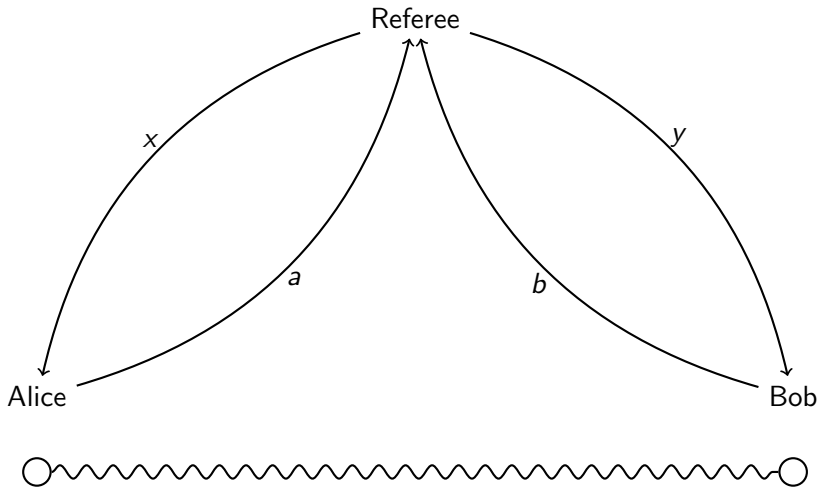
OK, generalized probabilistic theory is quite simple and easy to understand.

But, what is essential difference between classical theory and quantum theory ?

Can quantum theory be “simulated” or “explained” by classical theory ?

Are Hermitian positive-semidefinite matrices really needed for explaining reality ?

Bell test: CHSH game (1964, 1969)



Alice and Bob win iff $a \oplus b = x \wedge y$.

Bell inequality

a_x : Output of Alice for given x .

b_y : Output of Bbob for given y .

$$a_0 \oplus b_0 = 0$$

$$a_1 \oplus b_0 = 0$$

$$a_0 \oplus b_1 = 0$$

$$a_1 \oplus b_1 = 1$$

By adding all equations, we get $0 = 1$, which means there is no solution. Hence, the winning probability 1 cannot be achieved.

Three equalities can be satisfied, so that the largest winning probability is $3/4$ (Bell inequality or CHSH inequality).

If Alice and Bob share quantum states, then the largest winning probability is $(2 + \sqrt{2})/4 \approx 0.854$ (Violation of Bell/CHSH inequality)

Locality (Hidden variable model)

Joint preparation and independent measurements.

Probability distribution $P(a, b \mid x, y)$ is said to be **local** if

$$P(a, b \mid x, y) = \sum_{\lambda} P(\lambda) P(a \mid x, \lambda) P(b \mid y, \lambda).$$

Quantum physics allow **nonlocal** behaviors.

Einstein–Podolsky–Rosen (EPR) paradox (1935)

$$P(a, b \mid x, y) = \sum_{\lambda} P(\lambda) P(a \mid x, \lambda) P(b \mid y, \lambda).$$

\iff there exists a joint distribution of (a_0, a_1, b_0, b_1) .



In quantum physics, a_0, a_1, b_0, b_1 **cannot exists** simultaneously.



In quantum physics, position and momentum **cannot exists** simultaneously.

Summary

- Let V be the linear space spanned by $n \times n$ Hermitian matrices. Let $C_{\succeq 0}$ be the set of PSD matrices. Let I be the $n \times n$ identity matrix. Let $\langle e, \omega \rangle := \text{Tr}(e\omega)$ for $\omega, e \in V$ (Hilbert-Schmidt inner product).

$$\text{Set of states} = \{\omega \in V \mid \omega \in C_{\succeq 0}, \langle u, \omega \rangle = 1\}.$$

$$\text{Set of binary measurements} = \{e \in V \mid e \in C_{\succeq 0}, u - e \in C_{\succeq 0}\}.$$

- Classical theory and quantum theory are special cases of generalized probabilistic theories.
- Violation of Bell (CHSH) inequality show that quantum theory is essentially different from classical theory (Arguments on joint system is needed).

Assignments

- 1 Show the dimension and one of the basis of real linear space spanned by $n \times n$ Hermitian matrices.
- 2 Show that $XY = -YX$, $YZ = -ZY$ and $ZX = -XZ$.
- 3 Show that the Hilbert–Schmidt inner product satisfies the axioms of inner product.
- 4 Show that $C_{\succeq 0}$ is a self-dual cone.