

SORBONNE UNIVERSITE

MASTER 1 - QUANTUM INFORMATION

2021/2022

Lecture notes
-
Quantum Kinematic



Contents

1	Introduction	2
1.1	Dirac notation	2
1.2	Measurement in a basis B	2
1.2.1	Qubit	2
1.2.2	Measurement in the basis $\{ \pm\rangle\}$	2
1.3	Wiesner’s Quantum Money	3
1.4	Bennett and Brassard Quantum Key Exchange: BB84	3
2	Unitary transformation	3
3	Composition of systems	4
3.1	No cloning theorem	4
4	Measurements	4
4.1	Projective measurement	4
4.2	Observables	5
4.3	Generalized measurements	5
4.4	POVMs	7

1 Introduction

Physical system which has $d \in \mathbb{N}$ possible distinguishable states. Its physical state $|\psi\rangle \in \mathcal{H}$, the Hilbert space \mathbb{C}^d .

$$|\psi\rangle = \begin{bmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_d \end{bmatrix} \text{ and } \forall i, \psi_i \in \mathbb{C}. \quad (1)$$

The result of the measurement in the computational basis on $|\psi\rangle$ is $i \in [1, \dots, d]$ with probability $|\psi_i|^2$.

And $\sum_{i=1}^d |\psi_i|^2 = \langle\psi|\psi\rangle = 1$: the state is normalized.

1.1 Dirac notation

- Ket:

$$|\psi\rangle = \begin{bmatrix} \psi_1 \\ \vdots \\ \psi_d \end{bmatrix} = \psi_1 |1\rangle + \dots + \psi_d |d\rangle = \sum_{i=1}^d \psi_i |i\rangle \quad (2)$$

- Bra:

$$\langle\psi| = |\psi\rangle^\dagger = |\psi^*\rangle^T \quad (3)$$

- Bracket:

$$\langle\psi|\phi\rangle = [\psi_1^* \dots \psi_d^*] \begin{bmatrix} \phi_1 \\ \vdots \\ \phi_d \end{bmatrix} = \psi_1^* \phi_1 + \dots + \psi_d^* \phi_d \quad (4)$$

$\langle\psi|\phi\rangle$ is the hermitian product of ψ and ϕ .

1.2 Measurement in a basis B

B is an orthonormal basis : $B = \{|b_i\rangle\}_{i=1}^d$ and $\forall i \langle b_i | b_i \rangle = \delta_{i,j}$.

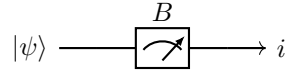


Figure 1: Circuit representation of the measurement of the state ψ

The probability of the output of a measurement is given by the following formula :

$$\mathbb{P}(\text{out} = |b_i\rangle) = |\langle b_i | \psi \rangle|^2 \quad (5)$$

The physical object is projected into the state $|b_i\rangle$, the is physically called the "wave packet reduction".

1.2.1 Qubit

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (6)$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (7)$$

1.2.2 Measurement in the basis $\{|\pm\rangle\}$

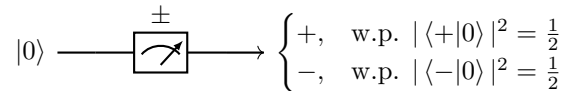


Figure 2: Measure of the state $|0\rangle$ in the basis $|\pm\rangle$

1.3 Wiesner's Quantum Money

Based on the conjugate coding.

- **bills:**
 - serial number
 - a set of random qubit $E_r \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^n$
 - **mint** knows {Serial Number + Random}, sends it to the bank.
- **Mint:** makes the bill, and gives it to the forger.
- **Forger:** tries to copy the bill, and spends the two to the bank.
- **Bank:** should accept the true one, reject the fake.

mint	forger basis	forger m.	bank m.
$ 0\rangle$	$\{ 0\rangle, 1\rangle\}$	$ 0\rangle$	$ 0\rangle$
$ 0\rangle$	$\{ \pm\rangle\}$	$\begin{cases} +\rangle, & \text{w.p. } \frac{1}{2} \\ -\rangle, & \text{w.p. } \frac{1}{2} \end{cases}$	$\begin{cases} 0\rangle, & \text{w.p. } \frac{1}{2} \\ 1\rangle, & \text{w.p. } \frac{1}{2} \end{cases}$

We therefore deduce that

$$\mathbb{P}(\text{get caught}) = 1 - (1 - \frac{1}{4})^n = 1 - (\frac{1}{4})^n \quad (8)$$

1.4 Bennett and Brassard Quantum Key Exchange: BB84

Goal: Alice and Bob \rightarrow share a secret bit string, Eve does not know anything.

Setting: Alice and Bob share a quantum channel and an authenticated classical channel.

Steps:

1. Alice prepares n qubits $E_r \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^n$, and she sends them to Bob
2. Bob receives. He measure them in the basis $\{B_{0,1}, B_{+,-}\}$
3. They use the public classical channel to compare the basis Bob used. They throw away the *bad basis* qubits.
4. Alice and Bob sample the data and compare the error rate e . If $e = 0$, they keep the key; if $e = 25$, Eve knows the key.

What if $0 < e < 25$? Eve knows a part of the key.

2 Unitary transformation

A transformation is an isolated system, and it is reversible.

Let T to be a transformation.

$$\langle T(|\psi\rangle) | T(|\psi\rangle) \rangle = \langle \psi | \psi \rangle \quad (9)$$

T is linear.

$$T(\alpha|\psi\rangle + \beta|\phi\rangle) = \alpha T(|\psi\rangle) + \beta T(|\phi\rangle) \quad (10)$$

T acts like an unitary operator. T corresponds to a complex matrix U : $T(|\phi\rangle) = U|\phi\rangle$, $U \in \mathbb{C}^{n \times n}$, such that $U^\dagger U = Id$.

In the basis $\{|i\rangle\}_{i=0}^n$, $\langle T(|\psi\rangle) | T(|\psi\rangle) \rangle = \langle i | j \rangle = \delta_{i,j}$

We have :

- measurement in computational basis
- a machine making arbitrary unitary U

Let's build a measurement in basis $\{|b_i\rangle\}_i$

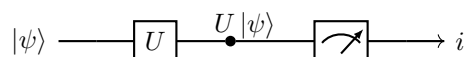


Figure 3: Circuit representation of the measurement unitary expected behavior

$$\mathbb{P}(i) \stackrel{\text{def}}{=} |\langle i | U | \psi \rangle|^2 \stackrel{\text{goal}}{=} |\langle b_i | \psi \rangle|^2 \quad \forall \psi \quad (11)$$

We want $\langle i | U = \langle b_i | \Leftrightarrow U^\dagger | i \rangle = | b_i \rangle \Leftrightarrow U = \sum_i | i \rangle \langle b_i |$

Is U an unitary ?

$$\begin{aligned}
U^\dagger U &= \left(\sum_i |b_i\rangle \langle i| \right) \left(\sum_j |j\rangle \langle b_j| \right) \\
&= \sum_{i,j} |b_i\rangle \langle i|j\rangle \langle b_j| \\
&= \sum_i |b_i\rangle \langle b_i| \\
&= Id
\end{aligned} \tag{12}$$

U is an unitary.

3 Composition of systems

Let $A \in \mathcal{H}_A = \mathbb{C}^{d_A}$ and $B \in \mathcal{H}_B = \mathbb{C}^{d_B}$ to be two systems in their respective vector spaces. Then we can construct the space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, its basis is $\{|ij\rangle_{AB}\}_{i,j}$, and $\dim(\mathcal{H}_{AB}) = d_A \times d_B$. If $|\alpha\rangle = \sum_i \alpha_i |i\rangle_A$ and $|\beta\rangle = \sum_i \beta_i |i\rangle_B$, then $|\phi\rangle_{AB} = |\alpha\rangle \otimes |\beta\rangle = \sum_{i,j} \alpha_i \beta_j |i\rangle_A |j\rangle_B$, and $|\phi\rangle_{AB} \in \mathcal{H}_{AB}$. $|\phi\rangle_{AB}$ is a joint state of systems A and B .

Not all states of \mathcal{H}_{AB} are separables into one state of \mathcal{H}_A and one state of \mathcal{H}_B

For example : $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \in \mathcal{H}_{AB}$, but $\nexists |\alpha\rangle \in \mathcal{H}_A, |\beta\rangle \in \mathcal{H}_B$, such that $|\alpha\rangle \otimes |\beta\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

3.1 No cloning theorem

The no cloning theorem

$$\text{There is no } U \text{ such that } \forall |\psi\rangle \in \mathcal{H}, U |\psi\rangle = |\psi\rangle \otimes |\psi\rangle \in \mathcal{H} \otimes \mathcal{H}. \tag{13}$$

Proof

Suppose there exists a such unitary U , then U is a cloning operator.

$$\begin{aligned}
U |0\rangle &\stackrel{\text{def}}{=} |0\rangle |0\rangle \\
U |1\rangle &\stackrel{\text{def}}{=} |1\rangle |1\rangle
\end{aligned} \tag{14}$$

By computing the application of U on the state $|+\rangle$, we get on the one hand, by linearity of unitaries

$$U\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{15}$$

and on the other hand, by definition of the operator behavior

$$U\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \tag{16}$$

which is a contradiction. Then such a U operator can not exist.

4 Measurements

4.1 Projective measurement

A projective measurement is described by an observable, a Hermitian operator. They are defined by a set of projectors $\{\Pi_j\}_{j=1}^k, k \leq d$.

Projectors properties:

$$\forall j, \Pi_j^2 = \Pi_j \quad \Pi_j \Pi_i = \delta_{i,j} \Pi_j \tag{17}$$

A projector is defined as follows:

$$\Pi_j = \sum_{l=1}^{d_j} |l_l^j\rangle \langle l_l^j| \tag{18}$$

Upon measuring the state $|\psi\rangle$, the probability of getting result j is given by

$$\langle \psi | \Pi_j | \psi \rangle = \|\Pi_j |\psi\rangle\|^2 \tag{19}$$

Given that outcome j occurred, the state of the quantum system immediately after the measurement is

$$\frac{\Pi_j |\psi\rangle}{\|\Pi_j |\psi\rangle\|^2} \tag{20}$$

4.2 Observables

Observables correspond to physical quantities, with values in \mathbb{R} . They are well defined in a basis $\{|b_i\rangle\}_i$ (i.e $\forall |b_i\rangle, \exists a_i \in \mathbb{R}$)

Note : $\alpha |b_1\rangle + \beta |b_2\rangle$ has **not always** a well defined value.

An observable is defined as follow:

$$O \stackrel{\text{def}}{=} \sum_i o_i \underbrace{|b_i\rangle\langle b_i|}_{\text{projector on } |b_i\rangle} = \sum_j o_j \Pi_j \quad (21)$$

O is diagonalizable by definition and $O^\dagger = O$: O is hermitian.

$$\text{Shape of } O : \begin{pmatrix} o_1 & 0 & \cdots & 0 \\ 0 & o_2 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & a_d \end{pmatrix}$$

The probability of getting the result i by measuring O on a state $|\psi\rangle$ is $\langle\psi|\Pi_i|\psi\rangle$

Average value of an observable

The average value of O , written $\langle O \rangle$, is by definition given by

$$\begin{aligned} \langle O \rangle &= \sum_i o_i \mathbb{P}(i|\psi) \\ &= \sum_i o_i \|\Pi_i |\psi\rangle\|^2 \\ &= \sum_i o_i \langle\psi|\Pi_i|\psi\rangle \\ &= \langle\psi|\sum_i o_i \Pi_i|\psi\rangle \\ &= \langle\psi|O|\psi\rangle \end{aligned} \quad (22)$$

From this formula for the average follows a formula for the standard deviation associated to the observation of O

$$\Delta^2 O = \langle (O - \langle O \rangle)^2 \rangle = \langle O^2 \rangle - \langle O \rangle^2 \quad (23)$$

Example

Using the Pauli matrix $\sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |+\rangle\langle +| - |-\rangle\langle -|$.

Known results : $X|+\rangle = |+\rangle$ and $X|-\rangle = -|-\rangle$.

We define $|\theta\rangle := \cos \omega |0\rangle + \sin \omega |1\rangle$

Then

$$\begin{aligned} \langle X \rangle_{|\theta\rangle} &= \langle \theta | X | \theta \rangle \\ &= [\cos \theta \sin \theta] \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \cos \theta \\ \sin \theta \end{bmatrix} \\ &= 2 \sin \theta \cos \theta \\ &= \sin 2\theta \end{aligned} \quad (24)$$

4.3 Generalized measurements

A generalized measurement is defined by

$$\{K_i\}_i \text{ such that } \sum_i K_i^\dagger K_i = Id \quad (25)$$

where the K_i are called Kraus Operators. The probability of getting the result i from a general measurement operator is given by $\mathbb{P}(i) = \|K_i |\psi\rangle\|^2$, and the state of the system just after the measurement is $K_i |\psi\rangle = \frac{K_i |\psi\rangle}{\|K_i |\psi\rangle\|}$

Generalized measurement \rightarrow Operator

If $i \in \{1\}$ then $K_1^\dagger K_1 = Id \Rightarrow K_1$ is unitary.

Generalized measurement \rightarrow Set of projectors

If $K_i := \Pi_i$ then $\sum_i K_i^\dagger K_i = \sum_i \Pi_i^\dagger \Pi_i = \sum_i \Pi_i = Id$

Example

With prob. P_j , I measure $\{\Pi_{ij}\}_i$ ($\sum_i \Pi_{ij} = Id$) and I measure U_j on the output state. Probability of getting ij :

$$\begin{aligned}\mathbb{P}(ij) &= P_j \langle \psi | \Pi_{ij} U^\dagger U \Pi_{ij} | \psi \rangle \\ &= P_j \langle \psi | \Pi_{ij} | \psi \rangle\end{aligned}\quad (26)$$

And the resulting state is $\frac{U \Pi_{ij} | \psi \rangle}{\| \Pi_{ij} | \psi \rangle \|^2}$

Let $\{K_{ij} = \sqrt{P_j} U \Pi_{ij}\}_{ij}$, then

$$\begin{aligned}\sum_{ij} K_{ij}^\dagger K_{ij} &= \sum_{ij} P_j \Pi_{ij} U^\dagger U \Pi_{ij} \\ &= \sum_j P_j \sum_i \Pi_{ij} \\ &= \sum_j P_j \\ &= Id\end{aligned}\quad (27)$$

Can we associate each set $\{K_i\}_i$ with a U and a $\{\Pi_i\}_i$?

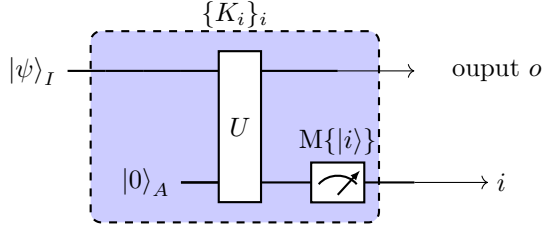


Figure 4: Circuit representation of such U and $\{\Pi_i\}_i$.

Note : $\mathcal{H}_A \otimes \mathcal{H}_I = \mathcal{H}_O \otimes \mathcal{H}_M$

$\forall i$, the output state of the system is

$$(I_O \otimes |i\rangle_M \langle i|) U | \psi \rangle \otimes |0\rangle_A = |i\rangle_M \langle i| U |0\rangle_A | \psi \rangle_I \quad (28)$$

Assume $K_i = {}_M \langle i| U |0\rangle_A$. With (28), we deduce that the output state is $K_i | \psi \rangle$, w.p. $\langle \psi | K_i^\dagger K_i | \psi \rangle$. Is that a valid set of operators $\{K_i\}_i$?

$$\begin{aligned}\sum_i K_i^\dagger K_i &= \sum_i ({}_A \langle 0| \otimes I_I) U^\dagger (|i\rangle_M \otimes I_O) (I_O \otimes {}_M \langle i|) U (I_I \otimes |0\rangle_A) \\ &= ({}_A \langle 0| \otimes I_I) U^\dagger \underbrace{\left(\sum_i \underbrace{|i\rangle_M \otimes I_O}_{=I_M} \right)}_{=I_{OM}} (I_O \otimes {}_M \langle i|) U (I_I \otimes |0\rangle_A) \\ &\quad \underbrace{\hspace{10em}}_{=I_{OA}} \\ &= ({}_A \langle 0| \otimes I_I) I_{OA} (I_I \otimes |0\rangle_A) \\ &= I_O \quad K_i \text{ is a valid set.}\end{aligned}\quad (29)$$

$\{K_i\}_i \rightarrow$ Unitary

Let $U := \sum_i K_i \otimes |i\rangle_{MA} \langle 0| + \dots$. The \dots represent extra terms used to make U a unitary, but can be neglected in the computation. By tensoring with $|0\rangle_A$, we obtain

$$U | \psi \rangle \otimes |0\rangle_A = \sum_i K_i | \psi \rangle \otimes |i\rangle \quad (30)$$

And then

$$\begin{aligned}{}_A \langle 0| U^\dagger U |0\rangle_A &= {}_A \langle 0| \left(\sum_i |0\rangle_{AM} \langle i| K_i^\dagger \cdot \sum_j K_j |j\rangle_{AM} \langle 0| \right) |0\rangle_A \\ &= \underbrace{{}_A \langle 0|0\rangle_A}_{=1} \cdot \sum_{ij} ({}_M \langle i| \otimes K_i^\dagger) (|j\rangle_M \otimes K_j) \underbrace{{}_A \langle 0|0\rangle_A}_{=1} \\ &= \sum_{ij} \underbrace{\langle i|j\rangle}_{\delta_{ij}} K_i^\dagger K_j \\ &= \sum_i K_i^\dagger K_i \\ &= Id\end{aligned}\quad (31)$$

4.4 POVMs

POVMs means Projective Operator Valued Measure : we "only care about the output i , not the state $K_i |\psi\rangle$ ". The probability of getting i is $\langle\psi|K_i^\dagger K_i|\psi\rangle$.

Let $E_i = K_i^\dagger K_i$. POVMs are then defined by the set $\{E_i\}_i$, such that $\sum_i E_i = Id, E_i \geq 0$.

E_i is semi-definite positive: $\forall\psi, \langle\psi|E_i|\psi\rangle \geq 0$. This implies that E_i is hermitian, and all its eigenvalues are ≥ 0 .

POVM \rightarrow Kraus operators

Let $K_i = \sqrt{E_i}$. $\{K_i\}_i$ is a well defined set of operators.