Sorbonne Universite

Master 1 - Quantum Information

2021/2022

Lecture notes
-
Quantum Kinematic

SORBONNE
UNIVERSITÉ

Contents

1 Introduction

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

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

The result of the measurement in the computational basis on $|\psi\rangle$ is $i \in [1, \cdots, d]$ 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:

$$|\psi\rangle = \begin{bmatrix} \psi_1 \\ \vdots \\ \psi_d \end{bmatrix} = \psi_1 |1\rangle + \cdots + \psi_d |d\rangle = \sum_{i=1}^{d} \psi_i |i\rangle \tag{2}$$

- Bra:

$$\langle\psi| = |\psi\rangle^\dagger = |\psi^*\rangle^T \tag{3}$$

- Braket:

$$\langle\psi|\phi\rangle = \begin{bmatrix} \psi_1^* \cdots \psi_d^* \end{bmatrix} \begin{bmatrix} \phi_1 \\ \vdots \\ \phi_d \end{bmatrix} = \psi_1^*\phi_1 + \cdots + \psi_d^*\phi_d \tag{4}$$

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

1.2 Measurement in a basis B

B is an orthonormal basis : $B := \{|b_i\rangle\}_{i=1}^{d}$. B has the following properties:

$$\begin{aligned} &\forall i\ \langle b_i|b_i\rangle = \delta_{i,j} \quad \textit{(orthonormality)} \\ &\sum_{i=1}^{d} |b_i\rangle \langle b_j| = I \ \textit{(completeness)} \end{aligned} \tag{5}$$

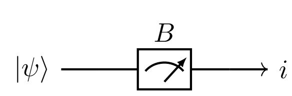

Figure 1: Circuit representation of the measurement of the state $|\psi\rangle$

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

$$\mathbb{P}(out = |b_i\rangle) = |\langle b_i|\psi\rangle|^2 \tag{6}$$

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

1.2.1 Qubit

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{7}$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{8}$$

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

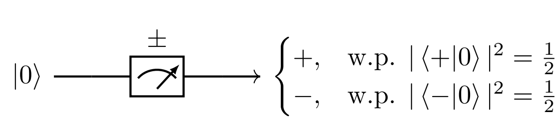

Figure 2: Measure of the state $|0\rangle$ in the basis $|\pm\rangle$

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

$$\mathbb{P}(\text{get caugth}) = 1 - (1 - \frac{1}{4})^n = 1 - (\frac{1}{4})^n \tag{9}$$

1.4 Bennett and Brassard Quantum Key Exchange: BB84

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

$$\langle T(|\psi\rangle)|T(|\psi\rangle)\rangle = \langle \psi|\psi\rangle \tag{10}$$

T is linear.

$$T(\alpha |\psi\rangle + \beta |\phi\rangle) = \alpha T(|\psi\rangle) + \beta T(|\phi\rangle) \tag{11}$$

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 $\{|b_i\rangle\}_i$

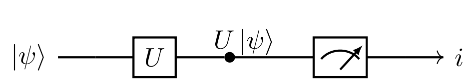

Figure 3: Circuit representation of the measurement unitary exptected behavior

$$\mathbb{P}(i) \overset{\text{def}}{=} |\langle i|U|\psi\rangle|^2 \overset{\text{goal}}{=} |\langle b_i|\psi\rangle|^2 \quad \forall\psi \tag{12}$$

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 ?

$$\begin{aligned}
U^\dagger U &= \Big(\sum_i |b_i\rangle\langle i|\Big)\Big(\sum_j |j\rangle\langle b_j|\Big) \\
&= \sum_{i,j} |b_i\rangle\langle i|j\rangle\langle b_j| \\
&= \sum_i |b_i\rangle\langle b_i| \\
&= Id \qquad\qquad U \text{ is an unitary.}
\end{aligned} \tag{13}$$

3 Composition of systems

Let $A \in \mathscr{H}_A = \mathbb{C}^{d_A}$ and $B \in \mathscr{H}_B = \mathbb{C}^{d_B}$ to be two systems in their respective vector spaces. Then we can construct the space

$$\mathscr{H}_{AB} = \mathscr{H}_A \otimes \mathscr{H}_B \tag{14}$$

Its orthonormal basis is $\{|ij\rangle_{AB}\}_{i,j}$, and

$$\dim\mathscr{H}_{AB} = \dim\mathscr{H}_A \cdot \dim\mathscr{H}_B \tag{15}$$

If $|\alpha\rangle = \sum_i \alpha_i |i\rangle_A$ and $|\beta\rangle = \sum_i \beta_i |i\rangle_B$, then

$$|\phi\rangle_{AB} = |\alpha\rangle \otimes |\beta\rangle = \sum_{i,j} \alpha_i\beta_j |i\rangle_A |j\rangle_B \tag{16}$$

and $|\phi\rangle_{AB} \in \mathscr{H}_{AB}$. $|\phi\rangle_{AB}$ is a joint state of systems A and B.
The inner product between two basis states can be defined as

$$\langle i,j|k,l\rangle = \langle i|k\rangle_A \langle j|l\rangle_B = \delta_{ik}\delta_{jl} \tag{17}$$

The most general state in the space $\mathscr{H}_{AB}$ can be written

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \tag{18}$$

with the usual condition for $|\psi\rangle$ to be normalized:

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1 \tag{19}$$

Not all states of $\mathscr{H}_{AB}$ are separable into one state of $\mathscr{H}_A$ and one state of $\mathscr{H}_B$
For example : $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \in \mathscr{H}_{AB}$, but $\nexists\, |\alpha\rangle \in \mathscr{H}_A, |\beta\rangle \in \mathscr{H}_B$, such that $|\alpha\rangle \otimes |\beta\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
Necessary condition on the coefficients $(\alpha, \beta, \gamma, \delta)$ of a state to be separable:

$$\alpha\delta = \beta\gamma \tag{20}$$

3.1 No cloning theorem

The no cloning theorem

$$\text{There is no } U \text{ such that } \forall\, |\psi\rangle \in \mathscr{H}, U|\psi\rangle = |\psi\rangle \otimes |\psi\rangle \in \mathscr{H} \otimes \mathscr{H}. \tag{21}$$

Proof

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

$$\begin{aligned}
U|0\rangle &\stackrel{\text{def}}{=} |0\rangle|0\rangle \\
U|1\rangle &\stackrel{\text{def}}{=} |1\rangle|1\rangle
\end{aligned} \tag{22}$$

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

$$U\Big(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\Big) = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{23}$$

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

$$U\Big(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\Big) = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \tag{24}$$

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

3.2 Superdense coding

Superdense coding involves two parties, `Alice` and `Bob`. The protocol allows `Alice` and `Bob` to share two bits of information by exchanging just one qubit. Basically, `Alice` is in possession of two classical bits of information, which she wishes to send to `Bob`.

Suppose `Alice` and `Bob` initially share a pair of qubits in the entangled state

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{25}$$

Here is the procedure.

The state `Alice` wants to send	The gate she applies	The states after
00	I	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}} = \|\phi^+\rangle$
01	Z	$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}} = \|\phi^-\rangle$
10	X	$\frac{\|10\rangle+\|01\rangle}{\sqrt{2}} = \|\psi^+\rangle$
11	Y	$\frac{\|01\rangle-\|10\rangle}{\sqrt{2}} = \|\psi^-\rangle$

`Alice` send her qubit to `Bob` and he measures the resulting pair in the base $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. This is indeed a basis, and its name is the *Bell basis*, and the states are called the *Bell states*.

3.3 Quantum teleportation

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:

$$\forall j, \Pi_j^2 = \Pi_j \qquad \Pi_j \Pi_i = \delta_{i,j} \Pi_j \tag{26}$$

A projector is defined as follows:

$$\Pi_j = \sum_{l=1}^{d_j} |l_l^j\rangle \langle l_l^j| \tag{27}$$

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

$$\langle\psi|\Pi_j|\psi\rangle = \|\Pi_j |\psi\rangle\|^2 \tag{28}$$

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

$$\frac{\Pi_j |\psi\rangle}{\|\Pi_j |\psi\rangle\|^2} \tag{29}$$

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:

$$O \stackrel{\text{def}}{=} \sum_i o_i \underbrace{|b_i\rangle \langle b_i|}_{\text{projector on } |b_i\rangle} = \sum_j o_j \Pi_j \tag{30}$$

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 $\langle\psi|\Pi_i|\psi\rangle$

4.2.1 Expectation value and standard deviation

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

$$\begin{aligned}\langle O\rangle &= \sum_i o_i \mathbb{P}(i\,|\psi\rangle) \\ &= \sum_i o_i \|\Pi_i\,|\psi\rangle\,\|^2 \\ &= \sum_i o_i\,\langle\psi|\Pi_i|\psi\rangle \\ &= \langle\psi|\sum_i o_i \Pi_i\,|\psi\rangle \\ &= \langle\psi|O|\psi\rangle\end{aligned} \tag{31}$$

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

$$\Delta^2 O = \langle (O-\langle O\rangle)^2\rangle = \langle O^2\rangle - \langle O\rangle^2 \tag{32}$$

Note: If $|\psi\rangle$ is an eigenstate of O, then $O\,|\psi\rangle = \lambda\,|\psi\rangle$.
Hence:

$$\begin{aligned}\langle O\rangle &= \langle\psi|O|\psi\rangle \\ &= \langle\psi|\lambda|\psi\rangle \\ &= \lambda\,\langle\psi|\psi\rangle \\ &= \lambda\end{aligned} \tag{33}$$

And:

$$\begin{aligned}O\,|\psi\rangle = \langle O\rangle\,|\psi\rangle &\Rightarrow \Delta^2 O = (\lambda^2 - \lambda^2) = 0 \\ &\Rightarrow \Delta O = 0\end{aligned} \tag{34}$$

4.2.2 Commutators

A key property of quantum physics is the existence of incompatible measurements: for any physical property A, there exists another physical property B which is incompatible with A. The incompatible means it is physically impossible to prepare a state $|\psi\rangle$ which gives perfectly predictible outputs for both measurements A and B. Let us first assume A and B to be observables. A key property of this pair of observable is their commutator

$$[A,B] := AB - BA \tag{35}$$

If A and B commute (i.e $[A,B]=0 \Leftrightarrow AB = BA$), there exists a basis such that the result of a measurement of A and a measurement of B are perfectly defined.

Conversely, if such a basis exists, then $[A,B]=0$

Therefore, if A and B do not commute, they correspond to incompatible measurements. (The proofs are in the 4^{th} tutorial.)

4.2.3 The Robertson-Heisenberg uncertainty relation

This relation evaluates the sharpness of two observables we will call A and B through the standard deviations ΔA and ΔB, and the states that, for any state $|\psi\rangle$ and any observable A and B

$$\Delta A \Delta B \geq \frac{1}{2}|\,\langle\psi|[A,B]|\psi\rangle \tag{36}$$

4.2.4 Anti-commutator

The anti commutator of two observables A and B is defined by

$$\{A,B\} = AB + BA \tag{37}$$

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 $|\theta\rangle := \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$
Then

$$\begin{aligned}\langle X\rangle_{|\theta\rangle} &= \langle\theta|X|\theta\rangle \\ &= [\cos\theta \sin\theta]\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}\cos\theta\\ sin\theta\end{bmatrix} \\ &= 2\sin\theta\cos\theta \\ &= sin2\theta\end{aligned} \tag{38}$$

4.3 Generalized measurements

A generalized measurement is defined by

$$\{K_i\}_i \text{ such that } \sum_i K_i^\dagger K_i = Id \tag{39}$$

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 $K_i |\psi\rangle = \frac{K_i|\psi\rangle}{\|K_i|\psi\rangle\|^2}$

Generalized measurement → Operator

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

Generalized measurement → 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 :

$$\begin{aligned} \mathbb{P}(ij) &= P_j \langle\psi|\Pi_{ij} U^\dagger U \Pi_{ij}|\psi\rangle \\ &= P_j \langle\psi|\Pi_{ij}|\psi\rangle \end{aligned} \tag{40}$$

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

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

$$\begin{aligned} \sum_{ij} K_{ij}^\dagger K_{ij} &= \sum_{ij} P_j \Pi_{ij} U^\dagger U \Pi_{ij} \\ &= \sum_j P_j \sum_i \Pi_{ij} \\ &= \sum_j P_j \\ &= Id \end{aligned} \tag{41}$$

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

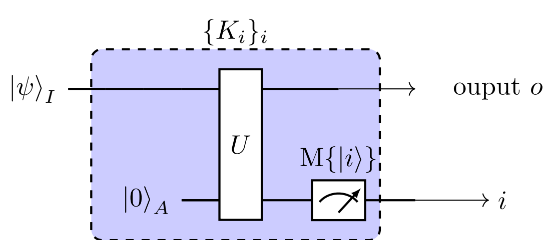

Figure 4: Circuit representation of such U and $\{\Pi_i\}_i$.
Note : $\mathscr{H}_A \otimes \mathscr{H}_I = \mathscr{H}_O \otimes \mathscr{H}_M$

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

$$(I_o \otimes |i\rangle_M \langle i|) U |\psi\rangle \otimes |0\rangle_A = |i\rangle_M \langle i|U|0\rangle_A |\psi\rangle_I \tag{42}$$

Assume $K_i =_M \langle i|U|0\rangle_A$. With (42), we deduce that the output state is $K_i |\psi\rangle$, w.p. $\langle\psi|K_i^\dagger K_i|\psi\rangle$. Is $\{K_i\}_i$ a valid set of operators ?

$$\begin{aligned} \sum_i K_i^\dagger K_i &= \sum_i ({}_A\langle 0| \otimes I_I) U^\dagger (|i\rangle_M \otimes I_O)(I_O \otimes_M \langle i|) U (I_I \otimes |0\rangle_A) \\ &= ({}_A\langle 0| \otimes I_I)\, U^\dagger \underbrace{(\underbrace{\underbrace{\sum_i |i\rangle_M}_{=I_M} \otimes I_O)(I_O \otimes_M \langle i|}_{=I_{OM}})(I_I \otimes |0\rangle_A)}_{=I_{OA}} \\ &= ({}_A\langle 0| \otimes I_I) I_{OA} (I_I \otimes |0\rangle_A) \\ &= I_O \qquad \{K_i\}_i \text{ is a valid set.} \end{aligned} \tag{43}$$

$\{K_i\}_i \to$ **Unitary**

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

$$U|\psi\rangle \otimes |0\rangle_A = \sum_i K_i |\psi\rangle \otimes |i\rangle \tag{44}$$

And then

$$\begin{aligned}
{}_A\langle 0|U^\dagger U|0\rangle_A &= {}_A\langle 0| (\sum_i |0\rangle_{AM} \langle i| K_i^\dagger \cdot \sum_j K_j |j\rangle_{AM} \langle 0|) |0\rangle_A \\
&= \underbrace{{}_A\langle 0|0\rangle_A}_{=1} \cdot \sum_{ij} ({}_M\langle i| \otimes K_i^\dagger)(|j\rangle_M \otimes K_j) \underbrace{{}_A\langle 0|0\rangle_A}_{=1} \\
&= \sum_{ij} \underbrace{\langle i|j\rangle}_{\delta_{ij}} K_i^\dagger K_j \\
&= \sum_i K_i^\dagger K_i \\
&= Id
\end{aligned} \tag{45}$$

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 $\to$ Kraus operators

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

4.5 The global phase

Lemma: The global phase is irrelevant
Of couse, the state $|\psi\rangle \neq e^{i\phi}|\psi\rangle$

Proof: First, we have

$$|\langle\psi|e^{i\phi}|\psi\rangle|^2 = |e^{i\phi}|^2 = 1 \tag{46}$$

Using the generalized measurements $\{K_i\}_i$ such that $\sum_i K_i = Id$
Then:

$$K_i e^{i\phi}|\psi\rangle = e^{i\phi} K_i |\psi\rangle \tag{47}$$

The phase of the input is the same as the phase of the output.
And

$$\|K_i e^{i\phi}|\psi\rangle\|_2^2 = \begin{cases} \|K_i|\psi\rangle\|_2^2 = & \sqrt{\mathbb{P}(i\,|\psi\rangle)} \\ \|e^{i\phi}K_i|\psi\rangle\|_2^2 & \sqrt{\mathbb{P}(i|e^{i\phi}|\psi\rangle)} \end{cases} \tag{48}$$

Hence, the global phase is irrelevant, and there is no way to measure the global phase.
However, the relative phase is important for later computations.

$$\frac{1}{\sqrt{2}}(|0\rangle + \underbrace{e^{i\phi}}_{\text{relative phase}} |1\rangle) \tag{49}$$

4.6 General quantum state

Number of parameters to describe a quantum state

Let $\mathscr{H} = \mathbb{C}^{\mathrm{d}}$ and $|\psi\rangle \in \mathscr{H} : |\psi\rangle = \sum_{i=0}^d \alpha_i |i\rangle$, (with $\alpha_i \in \mathbb{C}$ and $\sum_i |\alpha_i|^2 = 1$). If we consider $\alpha_i \in \mathbb{R}$ is the global phase, then $2d-2$ real parameters are needed to represent the quantum state.

Example

Qubit in $\mathscr{H}$:

- $d = 2 \to 2 \cdot 2 - 2 = 2$ right parameters : (θ, φ).
- $d = 3 \to 4$ real parameters.

A quantum state can be written, with the parameters θ and φ as

$$|\theta, \varphi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{50}$$

5 Bloch sphere

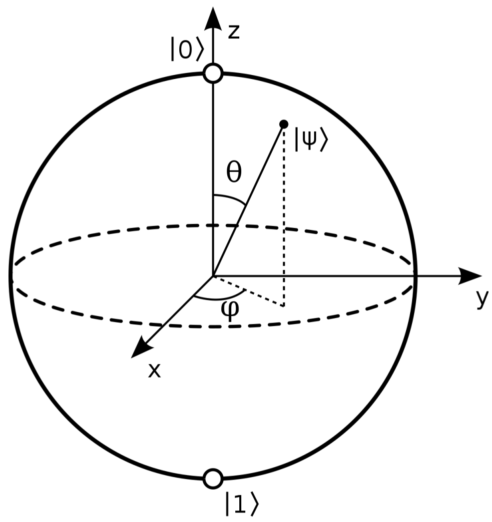

Figure 5: Graphical representation of a quantum state in the Bloch sphere

We will denote $|\psi\rangle$ as the vector $\vec{m}$ in the later computations.

$$\begin{aligned} \vec{m} &= \begin{bmatrix} u \\ v \\ w \end{bmatrix} \text{ such that } u^2+v^2+w^2 = 1 \\ \vec{m} &= \begin{bmatrix} \cos\theta\cdot\cos\varphi \\ \sin\theta\cdot\sin\varphi \\ \cos\theta \end{bmatrix} \end{aligned} \tag{51}$$

Are $\vec{m}$ and $-\vec{m}$ orthogonal ?

$$\begin{aligned} \langle m|-m\rangle &= \langle\theta,\varphi|\pi-\theta,\varphi+\pi[2\pi]\rangle \\ &= \Big(\cos\frac{\theta}{2}\langle 0| + e^{i\varphi}\sin\frac{\theta}{2}\langle 1|\Big)\Big(\underbrace{\cos(\frac{\pi}{2}-\frac{\theta}{2})}_{\sin\frac{\theta}{2}}|0\rangle + e^{i(\varphi+\pi)}\underbrace{\sin(\frac{\pi}{2}-\frac{\theta}{2})}_{\cos\frac{\theta}{2}}|1\rangle\Big) \\ &= \cos\frac{\theta}{2}\sin\frac{\theta}{2}\langle 0|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}(-e^{i\varphi})\cos\frac{\theta}{2}\langle 1|1\rangle \\ \langle m|-m\rangle &= 0 \end{aligned} \tag{52}$$

Orthogonal states in the Hilbert space correspond to opposite vectors in the Bloch sphere.

6 Pauli operators

6.1 Pauli matrices and properties

There are four extremely useful two by two matrices called the *Pauli matrices*.

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \sigma_1 \equiv \sigma_x = X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$
$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Properties

- they are indeed hermitian:

$$\forall i \in \{1,2,3\} f \quad \sigma_i^\dagger \sigma = \sigma_i^2 = Id \tag{53}$$

- braket decomposition

$$\begin{aligned} \sigma_x &= |0\rangle\langle 1| + |1\rangle\langle 0| \\ \sigma_y &= -i|0\rangle\langle 1| + i|1\rangle\langle 0| \\ \sigma_z &= |0\rangle\langle 1| - |1\rangle\langle 1| \end{aligned} \tag{54}$$

- commutation relation

$$[X,Y] = 2iZ; \quad [Y,Z] = 2iX; \quad [Z,X] = 2iY \tag{55}$$

6.1.1 Expectation values of the operators

- measure σ_z on the state $|\theta, \varphi\rangle$

$$\begin{aligned}\langle\sigma_z\rangle &= \langle\theta, \varphi|Z|\theta, \varphi\rangle \\ &= \frac{1}{2} + \frac{1}{2}\cos\theta - \frac{1}{2} + \cos\theta \\ &= \cos\theta = w \text{ (the } w \text{ component of } \vec{m})\end{aligned} \tag{56}$$

- measure σ_x on the state $|\theta, \varphi\rangle$

$$\begin{aligned}\langle\sigma_x\rangle &= \langle\theta, \varphi|X|\theta, \varphi\rangle \\ &= \Big(\cos\frac{\theta}{2}\langle 0| + e^{i\varphi}\sin\frac{\theta}{2}\langle 1|\Big) + \underbrace{\Big(\cos\frac{\theta}{2}|1\rangle + e^{i\varphi}\sin\frac{\theta}{2}|0\rangle\Big)}_{=X|\theta,\varphi\rangle} \\ &= \cos\frac{\theta}{2}\sin\frac{\theta}{2}\Big(\underbrace{e^{i\varphi} + e^{-i\varphi}}_{=2\cos\varphi}\Big) \\ &= \sin\theta\cos\varphi = u \text{ (the } u \text{ component of } \vec{m})\end{aligned} \tag{57}$$

- measure σ_y on the state $|\theta, \varphi\rangle$

$$\langle\sigma_y\rangle = v \tag{58}$$

Hence $\vec{m} = \begin{bmatrix}\langle X\rangle \\ \langle Y\rangle \\ \langle Z\rangle\end{bmatrix}$. The set (X, Y, Z) is tomographically complete.

Pauli matrices as unitary

- $\sigma_z = \begin{bmatrix}1 & 0 \\ 0 & -1\end{bmatrix}$

$$\begin{aligned}\sigma_z|\theta, \varphi\rangle &= \cos\frac{\theta}{2}|0\rangle - e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \\ &= \cos\frac{\theta}{2}|0\rangle + e^{i(\varphi+\pi)}\sin\frac{\theta}{2}|1\rangle \\ &= |\theta, \varphi + \pi\rangle \\ &= R_z(\pi)|\theta, \varphi\rangle\end{aligned} \tag{59}$$

It is a rotation of an angle π around the z axis on the Bloch sphere.

- $\sigma_x = \begin{bmatrix}0 & 1 \\ 1 & 0\end{bmatrix}$

$$\begin{aligned}\sigma_x|\theta, \varphi\rangle &= e^{i\varphi}\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle \\ &= e^{i\varphi}(\cos\frac{\pi-\theta}{2}|0\rangle + e^{-i\varphi}\sin\frac{\pi-\theta}{2}|1\rangle) \\ &= e^{i\varphi}|\pi-\theta, -\varphi\rangle \\ &= R_x(\pi)|\theta, \pi\rangle\end{aligned} \tag{60}$$

- $\sigma_y = \begin{bmatrix}0 & -i \\ i & 0\end{bmatrix}$

$$\begin{aligned}\sigma_y|\theta, \varphi\rangle &= i\cos\frac{\theta}{2}|1\rangle - ie^{i\varphi}\sin\frac{\theta}{2}|0\rangle \\ &= i\cos\frac{\theta}{2}|1\rangle + ie^{i(\varphi+\pi)}\sin\frac{\theta}{2}|0\rangle \\ &= ie^{i(\pi+\varphi)}\Big(e^{-i(\pi+\varphi)}\cos\frac{\theta}{2}|1\rangle + \sin\frac{\theta}{2}|0\rangle\Big) \\ &= ie^{i(\pi+\varphi)}\Big(\cos\frac{\theta-\pi}{2}|1\rangle + e^{-i(\pi-\varphi)}\sin\frac{\pi-\theta}{2}|1\rangle) \\ &= ie^{i(\pi+\varphi)}|\pi+\theta, -\pi-\theta\rangle \\ &= R_x(\pi)|\theta, \varphi\rangle\end{aligned} \tag{61}$$

6.1.2 Pauli Group

The Pauli group is defined by the set $G_1 = \{\eta I, \eta\sigma_x, \eta\sigma_y, \eta\sigma_z\}_{\eta\in\{\pm1,\pm i\}}$.

- they are their own inverse : $\sigma_i^{-1} = \sigma_i$
- their product is in G_1: The Pauli matrices anti-commute: $\{\sigma_i, \sigma_j\} = 0, \forall i \neq j$
  - $\sigma_x\sigma_y = i\sigma_z = -\sigma_y\sigma_x$
  - $\sigma_y\sigma_z = i\sigma_x = -\sigma_z\sigma_y$
  - $\sigma_z\sigma_x = i\sigma_y = -\sigma_x\sigma_z$

7 Generic observables

7.1 Projector onto $\vec{m}$ for an arbitrary vector $|\theta, \varphi\rangle$

Following the definition (51) of the vector $\vec{m}$, we can define a projector onto the vector $\vec{m}$ for any arbitrary state $|\theta, \varphi\rangle$.

$$\begin{aligned}
|\vec{m}\rangle\langle\vec{m}| &= \cos^2\frac{\theta}{2}|0\rangle\langle 0| + \sin^2\frac{\theta}{2}|1\rangle\langle 1| + \cos\frac{\theta}{2}\sin\frac{\theta}{2}\Big(e^{i\varphi}|1\rangle\langle 0| + e^{i\varphi}|0\rangle\langle 1|\Big) \\
&= \underbrace{\frac{1}{2}(1+\cos\theta)|0\rangle\langle 0| + \frac{1}{2}(1-\cos\theta)|1\rangle\langle 1|}_{\text{diagonal}} + \underbrace{\frac{1}{2}\sin\theta\Big(e^{i\varphi}|1\rangle\langle 0| + e^{-i\varphi}|0\rangle\langle 1|\Big)}_{\text{anti-diagonal part}} \\
&= \frac{1}{2}\Big(I + \cos\theta\sigma_z + \sin\theta\cos\varphi\sigma_x + i\sin\theta\cos\varphi\sigma_y\Big) \\
&= \frac{1}{2}\Big(I + u\sigma_x + v\sigma_y + w\sigma_z\Big) \\
&= \frac{1}{2}(I + \vec{m}\vec{\sigma}) \quad \text{considering } \vec{\sigma} = \begin{bmatrix}\sigma_x & \sigma_y & \sigma_z\end{bmatrix}
\end{aligned} \tag{62}$$

7.2 Generic observable

Let $\sigma_{\vec{m}} := 1|\vec{m}\rangle\langle\vec{m}| - 1|-\vec{m}\rangle\langle-\vec{m}|$. (recall from (52), $\vec{m}$ and $-\vec{m}$ are orthogonal).

$$\begin{aligned}
\sigma_{\vec{m}} &= |\vec{m}\rangle\langle\vec{m}| - |-\vec{m}\rangle\langle-\vec{m}| \\
&= \frac{1}{2}(I + \vec{m}\vec{\sigma} - I - (-\vec{m}\vec{\sigma}) \\
&= \vec{m}\vec{\sigma}
\end{aligned} \tag{63}$$

We have $\sigma_{\vec{m}} = \vec{m}\vec{\sigma}$ and $\sigma_{\vec{m}}^\dagger = \sigma_{\vec{m}}$.

$$\begin{aligned}
\sigma_{\vec{m}}^2 &= (u\sigma_x + v\sigma_y + w\sigma_z)(u\sigma_x + v\sigma_y + w\sigma_z) \\
&= (u^2+v^2+w^2)I + uv(\sigma_x\sigma_y + \sigma_y\sigma_x) + uw(\sigma_x\sigma_z + \sigma_z\sigma_x) + \cdots \\
&= \underbrace{(u^2+v^2+w^2)}_{=1(\text{by def. } 51)} I + \underbrace{uv\{\sigma_x;\sigma_y\}}_{=0} + \underbrace{uw\{\sigma_x,\sigma_z\}}_{=0} \\
&= I
\end{aligned} \tag{64}$$

$\sigma_{\vec{m}}$ corresponds to a rotation around the $\vec{m}$ axis.

Example

$$\sigma_{\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\end{bmatrix}} = H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$$

7.3 Arbitrary rotation

The hamiltonian of a system is given by the formula

$$H = \frac{\hbar\omega}{2}\sigma_z \tag{65}$$

And we can build an unitary that express the hamiltonian

$$U(t) = e^{-\frac{i}{\hbar}Ht} = e^{-i\frac{\omega t}{2}\sigma_z} = \begin{bmatrix} e^{i\omega\frac{t}{2}} & \cdot \\ \cdot & e^{i\omega\frac{t}{2}}\end{bmatrix} \tag{66}$$

By measuring the hamiltonian over time on the general state $|\theta, \varphi\rangle$, we get that

$$
\begin{aligned}
U(t)\,|\theta,\varphi\rangle &= e^{-i\frac{\omega t}{2}} \cos\frac{\theta}{2} + e^{+i(\frac{\omega t}{2}+\varphi)} \sin\frac{\theta}{2}\,|1\rangle \\
&= e^{-i\frac{\omega t}{2}} \Big(\cos\frac{\theta}{2}\,|0\rangle + e^{i(\omega t+\varphi)} \sin\frac{\theta}{2}\,|1\rangle \Big) \\
&= e^{-i\frac{\omega t}{2}}\,|\theta, \varphi+\omega t\rangle
\end{aligned}
\tag{67}
$$

From (67), we can deduce that

$$
e^{-i\frac{\omega t}{2}\sigma_z} = R_z(\omega t)\cdot e^{-i\frac{\omega t}{2}} \qquad \text{with } R_z(\omega t) = \begin{bmatrix} 1 & \cdot \\ \cdot & e^{i\omega t} \end{bmatrix}
\tag{68}
$$

Note: The relative phase from $R_z(\omega t)$ and $U(t)$ are equal.
From the previous results, we can express an arbitrary rotation matrix $R_{\vec{m}}$ up to a global phase.

$$
\begin{aligned}
R_{\vec{m}}(\alpha) &= e^{-i\frac{\alpha}{2}\sigma_{\vec{m}}} \\
&= \sum_{k=0}^{\infty} \frac{(-i\frac{\alpha}{2}\sigma_{\vec{m}})^k}{k!} \\
&= \sum_{q=0}^{\infty} \Big(\frac{(-i)^{2q}(\frac{\alpha}{2})^{2q}}{(2q)!} I + \frac{(-i)^{2q+1}(\frac{\alpha}{2})^{2q+1}}{(2q+1)!} \sigma_{\vec{m}} \Big) \\
&= \cos\frac{\alpha}{2} I - i \sin\frac{\alpha}{2}\sigma_{\vec{m}}
\end{aligned}
\tag{69}
$$