Sorbonne Universite

Master 1 - Quantum Information

2021/2022

Lecture notes
-
Quantum Kinematic

Contents

1 Introduction

Physical system which has $d \in \mathbb{N}$ possible distinguishable 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:

$$\langle\psi|\varphi\rangle = \begin{bmatrix} \psi_1^* \cdots \psi_d^* \end{bmatrix} \begin{bmatrix} \varphi_1 \\ \vdots \\ \varphi_d \end{bmatrix} = \psi_1^* \varphi_1 + \cdots + \psi_d^* \varphi_d \tag{4}$$

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

1.2 Measurement in a basis B

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

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

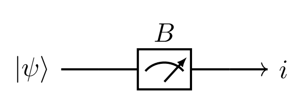

Figure 1: Circuit representation of the measurement of the state $|\psi\rangle$ in the basis B.

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".

Qubit

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

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

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

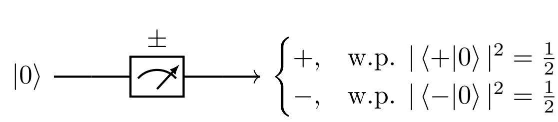

Figure 2: Measure of the state $|0\rangle$ in the basis $|\pm\rangle$

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 → 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 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.

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

T is linear.

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

T acts like an unitary operator. T corresponds to a complex matrix U: $T(|\varphi\rangle) = U|\varphi\rangle$, $U \in \mathbb{C}^{n\times n}$, such that $U^\dagger U = Id$. In the basis $\{|i\rangle\}_{i=0}^n$, which is the computational basis, $\langle T(|\psi\rangle)|T(|\psi\rangle)\rangle = \langle i|j\rangle = \delta_{i,j}$

We have :

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

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

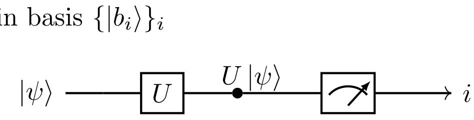

Figure 3: Circuit representation of the measurement unitary exptected behavior

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

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

Indeed, if $U = \sum_i |i\rangle \langle b_i|$ then $U^\dagger = \sum_i |b_i\rangle \langle i|$, that implies $U^\dagger |i\rangle = \big(\sum_j |b_j\rangle \underbrace{\langle j| \big) |i\rangle}_{\delta_{i,j}} = |i\rangle$.

Is U an unitary ?

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

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

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

and $|\varphi\rangle_{AB} \in \mathscr{H}_{AB}$. $|\varphi\rangle_{AB}$ 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 Partial measurement

Case of the 2-qubits state

Let $|\psi\rangle = \alpha |00\rangle + \beta |01\rangle + \delta |10\rangle + \gamma |11\rangle$. If we consider not the measurement of the two qubits but only the measurement of, for this example, the first qubit, the probablilies of having 0 or 1 as outcome are simply given by:

$$\begin{aligned} \mathbb{P}(|0\rangle) &= |\alpha|^2 + |\beta|^2 \\ \mathbb{P}(|1\rangle) &= |\delta|^2 + |\gamma|^2 \end{aligned} \tag{21}$$

We can rewrite $|\psi\rangle = |0\rangle (\alpha |0\rangle + \beta |1\rangle) + |1\rangle (\delta |0\rangle + \gamma |1\rangle)$, hence we deduce that the final state after the measurement is $\frac{\alpha|0\rangle + \beta|1\rangle}{\sqrt{|\alpha|^2+|\beta|^2}}$ if the measurement outcome was $|0\rangle$, and $\frac{\delta|0\rangle + \gamma|1\rangle}{\sqrt{|\delta|^2+|\gamma|^2}}$ if the measurement outcome was $|1\rangle$.

As a matter of intution, imagine that we separate both qubits of the system by a long distance, then acting on the qubit we measure should not do anything on the other, hence we juste need to sum the probabilities.

3.2 No cloning theorem

Theorem 1 *There is no unitary* U *such that* $\forall |\psi\rangle \in \mathscr{H}, U|\psi\rangle = |\psi\rangle \otimes |\psi\rangle \in \mathscr{H} \otimes \mathscr{H}$.

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

$$\forall |\psi\rangle, U|\psi\rangle \overset{\text{def}}{=} |\psi\rangle|\psi\rangle \tag{22}$$

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

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

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

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

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

3.3 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
$\|00\rangle$	I	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}} = \|\varphi^+\rangle$
$\|01\rangle$	Z	$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}} = \|\varphi^-\rangle$
$\|10\rangle$	X	$\frac{\|10\rangle+\|01\rangle}{\sqrt{2}} = \|\psi^+\rangle$
$\|11\rangle$	Y	$\frac{\|01\rangle-\|10\rangle}{\sqrt{2}} = \|\psi^-\rangle$

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

3.4 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:

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

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

$$\text{Shape of } O \ : \begin{pmatrix} o_1 & 0 & \cdots & 0 \\ 0 & o_2 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & a_d \end{pmatrix} \tag{31}$$

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

$$\mathbb{P}(i) = \langle\psi|\Pi_i|\psi\rangle \tag{32}$$

Expectation value and standard deviation

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

$$\begin{aligned} \langle O\rangle &= \sum_i o_i \mathbb{P}(i\,|\psi\rangle) \\ &= \sum_i o_i \|\Pi_i\,|\psi\rangle\,\|^2 \\ &= \sum_i o_i \langle\psi|\Pi_i|\psi\rangle \\ &= \langle\psi| \sum_i o_i \Pi_i\,|\psi\rangle \\ &= \langle\psi|O|\psi\rangle \end{aligned} \tag{33}$$

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

$$\Delta^2 O = \langle (O - \langle O\rangle)^2\rangle = \langle O^2\rangle - \langle O\rangle^2 \tag{34}$$

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

$$\begin{aligned} \langle O\rangle &= \langle\psi|O|\psi\rangle \\ &= \langle\psi|\lambda|\psi\rangle \\ &= \lambda\,\langle\psi|\psi\rangle \\ &= \lambda \end{aligned} \tag{35}$$

And:

$$\begin{aligned} O\,|\psi\rangle = \langle O\rangle\,|\psi\rangle &\Rightarrow \Delta^2 O = (\lambda^2 - \lambda^2) = 0 \\ &\Rightarrow \Delta O = 0 \end{aligned} \tag{36}$$

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

$$[A, B] := AB - BA \tag{37}$$

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.)

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

$$\Delta A \Delta B \geq \frac{1}{2} \big|\,\langle\psi|[A, B]|\psi\rangle\,\big| \tag{38}$$

Anti-commutator

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

$$\{A, B\} = AB + BA \tag{39}$$

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

$$\begin{aligned} \langle X\rangle_{|\theta\rangle} &= \langle\theta|X|\theta\rangle \\ &= [\cos\theta \sin\theta] \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \cos\theta \\ sin\theta \end{bmatrix} \\ &= 2\sin\theta\cos\theta \\ &= \sin(2\theta) \end{aligned} \tag{40}$$

4.3 Generalized measurements

A generalized measurement is defined by

$$\{K_i\}_i \text{ such that } \sum_i K_i^\dagger K_i = Id \tag{41}$$

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 probability p_j, I measure $\{\Pi_{ij}\}_i$ (with $\sum_i \Pi_{ij} = Id$) and I measure U_j on the output state. The probability of getting ij as measurement outcome is given by:

$$\begin{aligned} \mathbb{P}(ij) &= p_j \langle\psi|\Pi_{ij}U^\dagger U\Pi_{ij}|\psi\rangle \\ &= p_j \langle\psi|\Pi_{ij}|\psi\rangle \end{aligned} \tag{42}$$

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

$$\begin{aligned} \sum_{ij} K_{ij}^\dagger K_{ij} &= \sum_{ij} p_j \Pi_{ij} U^\dagger U \Pi_{ij} \\ &= \sum_j p_j \sum_i \Pi_{ij} \\ &= \sum_j p_j \\ &= Id \end{aligned} \tag{43}$$

Can we associate each set $\{K_i\}_i$ with a U and a $\{\Pi_i\}_i$?
$\forall i$, the output state of the system is

$$(I_o \otimes |i\rangle_M \langle i|)U|\psi\rangle \otimes |0\rangle_A = |i\rangle_M \langle i|U|0\rangle_A |\psi\rangle_I \tag{44}$$

Assume $K_i =_M \langle i|U|0\rangle_A$. With (44), we deduce that the output state is $K_i|\psi\rangle$, w.p. $\langle\psi|K_i^\dagger K_i|\psi\rangle$.

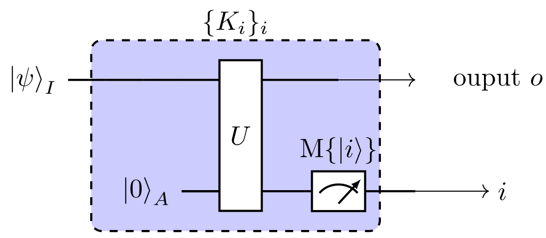

Figure 4: Circuit representation of such U and $\{\Pi_i\}_i$.
Note: $\mathscr{H}_A \otimes \mathscr{H}_I = \mathscr{H}_O \otimes \mathscr{H}_M$

Is $\{K_i\}_i$ a valid set of operators ?

$$\begin{aligned}\sum_i K_i^\dagger K_i &= \sum_i \big({}_A\langle 0| \otimes I_I\big)U^\dagger\big(|i\rangle_M \otimes I_O\big)\big(I_O \otimes_M \langle i|\big)U\big(I_I \otimes |0\rangle_A\big)\\ &= ({}_A\langle 0| \otimes I_I)\,U^\dagger \underbrace{(\underbrace{\underbrace{\sum_i |i\rangle_M}_{=I_M} \otimes I_O)}_{=I_{OM}}(I_O \otimes_M \langle i|)}_{=I_{OA}}(I_I \otimes |0\rangle_A)\\ &= ({}_A\langle 0| \otimes I_I)I_{OA}(I_I \otimes |0\rangle_A)\\ &= I_O \qquad \{K_i\}_i \text{ is a valid set.}\end{aligned} \tag{45}$$

$\{K_i\}_i \rightarrow$ **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

$$U|\psi\rangle \otimes |0\rangle_A = \sum_i K_i |\psi\rangle \otimes |i\rangle \tag{46}$$

And then

$$\begin{aligned}{}_A\langle 0|U^\dagger U|0\rangle_A &= {}_A\langle 0|\,(\sum_i |0\rangle_{AM}\langle i|\,K_i^\dagger \cdot \sum_j K_j\,|j\rangle_{AM}\langle 0|)\,|0\rangle_A\\ &= \underbrace{{}_A\langle 0|0\rangle_A}_{=1} \cdot \sum_{ij}({}_M\langle i| \otimes K_i^\dagger)(|j\rangle_M \otimes K_j)\underbrace{{}_A\langle 0|0\rangle_A}_{=1}\\ &= \sum_{ij}\underbrace{\langle i|j\rangle}_{\delta_{ij}} K_i^\dagger K_j\\ &= \sum_i K_i^\dagger K_i\\ &= Id\end{aligned} \tag{47}$$

4.4 POVMs

POVMs means Projective Operator Valued Measure: differently from the projective measurements, the POVM does not define the post-measurement state.
Recall that the probability of getting i, when the state is $|\psi\rangle$ is

$$\langle\psi|K_i^\dagger K_i|\psi\rangle \tag{48}$$

Then let $E_i = K_i^\dagger K_i$.
POVMs are then defined by the set $\{E_i\}_i$, such that

$$\sum_i E_i = Id, \quad E_i \geq 0 \tag{49}$$

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.

4.5 The global phase

Lemma 1 *The global phase is irrelevant.*

Of couse, the state $|\psi\rangle$ is different from the state $e^{i\varphi}|\psi\rangle$, but there is no way to measure the factor $e^{i\varphi}$.

Proof: First, we have

$$|\langle\psi|e^{i\varphi}|\psi\rangle|^2 = |e^{i\varphi}|^2 = 1 \tag{50}$$

Using the generalized measurements $\{K_i\}_i$ such that $\sum_i K_i^\dagger K_i = Id$
Then, since $e^i\varphi \in \mathbb{C}$, it commutes with K_i:

$$K_i e^{i\varphi}|\psi\rangle = e^{i\varphi}K_i|\psi\rangle \tag{51}$$

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

$$\|K_i e^{i\varphi}|\psi\rangle\|_2^2 = \begin{cases} \|K_i|\psi\rangle\|_2^2 & = \sqrt{\mathbb{P}(i\,|\psi\rangle)} \\ \|e^{i\varphi}K_i|\psi\rangle\|_2^2 & = \sqrt{\mathbb{P}(i|e^{i\varphi}|\psi\rangle)} \end{cases} \tag{52}$$

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.

$$\frac{1}{\sqrt{2}}(|0\rangle + \underbrace{e^{i\varphi}}_{\text{relative phase}}|1\rangle) \tag{53}$$

For example the Z gates changes the relative phase and $HZH|0\rangle = |1\rangle \neq HH|0\rangle = |0\rangle$ due to the relatve phase added by Z.

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 $\mathscr{H}$:

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

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

$$|\theta,\varphi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{54}$$

5 Bloch sphere

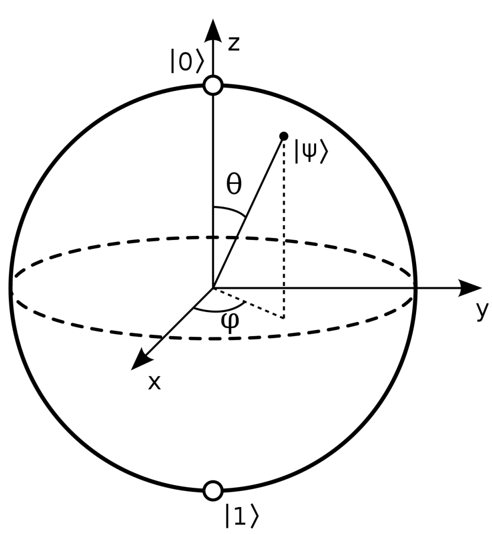

Figure 5: Graphical representation of a quantum state in the Bloch sphere

We will denote $|\psi\rangle$ as the vector $\vec{m}$

$$\vec{m} = \begin{bmatrix} u \\ v \\ w \end{bmatrix} \text{ such that } u^2 + v^2 + w^2 = 1 \tag{55}$$

whose cartesian coordinates are

$$\vec{m} = \begin{bmatrix} \sin\theta\cdot\cos\varphi \\ \sin\theta\cdot\sin\varphi \\ \cos\theta \end{bmatrix} \tag{56}$$

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

$$\begin{aligned}
\langle m|-m\rangle &= \langle \theta,\varphi|\pi-\theta,\varphi+\pi[2\pi]\rangle \\
&= \Big(\cos\frac{\theta}{2}\langle 0| + e^{i\varphi}\sin\frac{\theta}{2}\langle 1|\Big)\Big(\underbrace{\cos(\frac{\pi}{2}-\frac{\theta}{2})}_{\sin\frac{\theta}{2}}|0\rangle + e^{i(\varphi+\pi)}\underbrace{\sin(\frac{\pi}{2}-\frac{\theta}{2})}_{\cos\frac{\theta}{2}}|1\rangle\Big) \\
&= \cos\frac{\theta}{2}\sin\frac{\theta}{2}\langle 0|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}(-e^{i\varphi})\cos\frac{\theta}{2}\langle 1|1\rangle \\
\langle m|-m\rangle &= 0
\end{aligned} \tag{57}$$

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

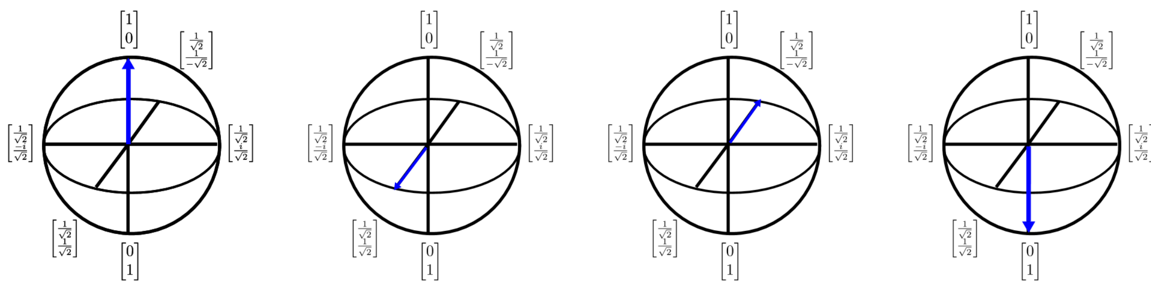

Figure 6: Example of states in the Bloch sphere.

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:

$$\forall i \in \{1,2,3\} f \quad \sigma_i^\dagger \sigma_i = \sigma_i^2 = Id \tag{58}$$

- braket decomposition

$$\begin{aligned}
\sigma_x &= |0\rangle\langle 1| + |1\rangle\langle 0| \\
\sigma_y &= -i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0| \\
\sigma_z &= |0\rangle\langle 0| - |1\rangle\langle 1|
\end{aligned} \tag{59}$$

- commutation relation

$$[X,Y] = 2iZ; \quad [Y,Z] = 2iX; \quad [Z,X] = 2iY \tag{60}$$

  and more generally:

$$[\sigma_i,\sigma_j] = 2i\varepsilon_{ikj}\sigma_k \quad \text{with } \varepsilon_{123} = 1 \text{ and } \varepsilon_{jik} = -\varepsilon_{ijk} \tag{61}$$

Expectation values of the operators

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

$$\begin{aligned}
\langle \sigma_z\rangle &= \langle \theta,\varphi|Z|\theta,\varphi\rangle \\
&= \frac{1}{2} + \frac{1}{2}\cos\theta - \frac{1}{2} + \cos\theta \\
&= \cos\theta = w \text{ (the } w \text{ component of } \vec{m})
\end{aligned} \tag{62}$$

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

$$\begin{aligned}
\langle \sigma_x\rangle &= \langle \theta,\varphi|X|\theta,\varphi\rangle \\
&= \Big(\cos\frac{\theta}{2}\langle 0| + e^{-i\varphi}\sin\frac{\theta}{2}\langle 1|\Big) + \underbrace{\Big(\cos\frac{\theta}{2}|1\rangle + e^{i\varphi}\sin\frac{\theta}{2}|0\rangle\Big)}_{=X|\theta,\varphi\rangle} \\
&= \cos\frac{\theta}{2}\sin\frac{\theta}{2}\Big(\underbrace{e^{i\varphi}+e^{-i\varphi}}_{=2\cos\varphi}\Big) \\
&= \sin\theta\cos\varphi = u \text{ (the } u \text{ component of } \vec{m})
\end{aligned} \tag{63}$$

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

$$\begin{aligned}\langle\sigma_y\rangle &= \Big(\cos\frac{\theta}{2}\langle 0| + e^{-i\varphi}\sin\frac{\theta}{2}\langle 1|\Big)\Big(-i|0\rangle\langle 1| + i|1\rangle\langle 0|\Big)\Big(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\Big)\\ &= \Big(-i\cos\frac{\theta}{2}\langle 1| + ie^{-i\varphi}\sin\frac{\theta}{2}\langle 0|\Big)\Big(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\Big)\\ &= -i\sin\frac{\theta}{2}\cos\frac{\theta}{2}\underbrace{(e^{i\varphi} - e^{-}i\varphi)}_{i\sin\varphi}\\ &= \sin\theta\sin\varphi = v\end{aligned} \tag{64}$$

Note: The average value corresponds to the associated coordinates: $\vec{m} = \begin{bmatrix}\langle X\rangle\\ \langle Y\rangle\\ \langle Z\rangle\end{bmatrix}$. The set (X,Y,Z) is tomographically complete.

Pauli matrices as unitary

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

$$\begin{aligned}\sigma_z|\theta,\varphi\rangle &= \cos\frac{\theta}{2}|0\rangle - e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\\ &= \cos\frac{\theta}{2}|0\rangle + e^{i(\varphi+\pi)}\sin\frac{\theta}{2}|1\rangle\\ &= |\theta,\varphi+\pi\rangle\\ &= R_z(\pi)|\theta,\varphi\rangle\end{aligned} \tag{65}$$

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

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

$$\begin{aligned}\sigma_x|\theta,\varphi\rangle &= e^{i\varphi}\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle\\ &= e^{i\varphi}\cos\frac{\pi-\theta}{2}|0\rangle + e^{-i\varphi}\sin\frac{\pi-\theta}{2}|1\rangle\\ &= e^{i\varphi}|\pi-\theta,-\varphi\rangle\\ &= R_x(\pi)|\theta,\pi\rangle\end{aligned} \tag{66}$$

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

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

Pauli Group

The Pauli group is defined by the set $G_1 = \{\eta I, \eta\sigma_x, \eta\sigma_y, \eta\sigma_z\}_{\eta\in\{\pm 1,\pm i\}}$.

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

7 Generic observable

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

Following the definition (56) of the vector $\vec{m}$, we can define a projector onto the vector $\vec{m}$ for any arbitrary state $|\theta, \varphi\rangle$.

$$\begin{aligned} |\vec{m}\rangle\langle\vec{m}| &= \cos^2\frac{\theta}{2}|0\rangle\langle 0| + \sin^2\frac{\theta}{2}|1\rangle\langle 1| + \cos\frac{\theta}{2}\sin\frac{\theta}{2}\Big(e^{i\varphi}|1\rangle\langle 0| + e^{i\varphi}|0\rangle\langle 1|\Big) \\ &= \underbrace{\frac{1}{2}(1+\cos\theta)|0\rangle\langle 0| + \frac{1}{2}(1-\cos\theta)|1\rangle\langle 1|}_{\text{diagonal}} + \underbrace{\frac{1}{2}\sin\theta\Big(e^{i\varphi}|1\rangle\langle 0| + e^{-i\varphi}|0\rangle\langle 1|\Big)}_{\text{anti-diagonal part}} \\ &= \frac{1}{2}\Big(I + \cos\theta\sigma_z + \sin\theta\cos\varphi\sigma_x + i\sin\theta\cos\varphi\sigma_y\Big) \\ &= \frac{1}{2}\Big(I + u\sigma_x + v\sigma_y + w\sigma_z\Big) \\ &= \frac{1}{2}(I + \vec{m}\vec{\sigma}) \quad \text{considering } \vec{\sigma} = \begin{bmatrix}\sigma_x & \sigma_y & \sigma_z\end{bmatrix} \end{aligned} \tag{68}$$

Note: Hence we can also express the projector onto $\vec{m}$ with

$$|\vec{m}\rangle\langle\vec{m}| = \frac{1}{2}\begin{bmatrix} 1+w & u-iw \\ u+iw & 1-w \end{bmatrix} \tag{69}$$

but the result found on (68) is a more convinient notation.

7.2 Generic observable

Let $\sigma_{\vec{m}} := 1\,|\vec{m}\rangle\langle\vec{m}| - 1\,|-\vec{m}\rangle\langle-\vec{m}|$. (recall from (57), $\vec{m}$ and $-\vec{m}$ are orthogonal).

$$\begin{aligned} \sigma_{\vec{m}} &= |\vec{m}\rangle\langle\vec{m}| - |-\vec{m}\rangle\langle-\vec{m}| \\ &= \frac{1}{2}(I + \vec{m}\vec{\sigma} - I - (-\vec{m}\vec{\sigma})) \\ &= \vec{m}\vec{\sigma} \end{aligned} \tag{70}$$

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

$$\begin{aligned} \sigma_{\vec{m}}^2 &= (u\sigma_x + v\sigma_y + w\sigma_z)(u\sigma_x + v\sigma_y + w\sigma_z) \\ &= (u^2+v^2+w^2)I + uv(\sigma_x\sigma_y + \sigma_y\sigma_x) + uw(\sigma_x\sigma_z + \sigma_z\sigma_x) + \cdots \\ &= \underbrace{(u^2+v^2+w^2)}_{=1(\text{by def. }56)}I + \underbrace{uv\{\sigma_x;\sigma_y\}}_{=0} + \underbrace{uw\{\sigma_x,\sigma_z\}}_{=0} \\ &= I \end{aligned} \tag{71}$$

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

Example

$$\sigma_{\frac{1}{\sqrt{2}}\left[\begin{smallmatrix}1\\0\\1\end{smallmatrix}\right]} = H = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\end{bmatrix} \tag{72}$$

7.3 Arbitrary rotation

The Pauli matrices X, Y and Z are so-called because when they are exponentiated, they give rise to the *rotation operators*, which rotate the Bloch vector $\vec{m}$ around the x, y and z axis:

$$\begin{aligned} R_x &\equiv e^{-i\frac{\theta}{2}X} \\ R_y &\equiv e^{-i\frac{\theta}{2}Y} \\ R_z &\equiv e^{-i\frac{\theta}{2}Z} \end{aligned} \tag{73}$$

Example

The hamiltonian of a system is given by the formula

$$H = \frac{\hbar\omega}{2}\sigma_z \tag{74}$$

And we can build an unitary that express the hamiltonian

$$U(t) = e^{-\frac{i}{\hbar}Ht} = e^{-i\frac{\omega t}{2}\sigma_z} = \begin{bmatrix} e^{i\omega\frac{t}{2}} & \cdot \\ \cdot & e^{i\omega\frac{t}{2}} \end{bmatrix} \tag{75}$$

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

$$\begin{aligned} U(t)\,|\theta,\varphi\rangle &= e^{-i\frac{\omega t}{2}}\cos\frac{\theta}{2} + e^{+i(\frac{\omega t}{2}+\varphi)}\sin\frac{\theta}{2}\,|1\rangle \\ &= e^{-i\frac{\omega t}{2}}\Big(\cos\frac{\theta}{2}\,|0\rangle + e^{i(\omega t+\varphi)}\sin\frac{\theta}{2}\,|1\rangle\Big) \\ &= e^{-i\frac{\omega t}{2}}\,|\theta,\varphi+\omega t\rangle \end{aligned} \tag{76}$$

From (76), we can deduce that

$$e^{-i\frac{\omega t}{2}\sigma_z} = R_z(\omega t)\cdot e^{-i\frac{\omega t}{2}} \qquad \text{with } R_z(\omega t) = \begin{bmatrix} 1 & \cdot \\ \cdot & e^{i\omega t} \end{bmatrix} \tag{77}$$

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

$$\begin{aligned} R_{\vec{m}}(\alpha) &= e^{-i\frac{\alpha}{2}\sigma_{\vec{m}}} \\ &= \sum_{k=0}^{\infty}\frac{(-i\frac{\alpha}{2}\sigma_{\vec{m}})^k}{k!} \\ &= \sum_{q=0}^{\infty}\Big(\frac{(-i)^{2q}(\frac{\alpha}{2})^{2q}}{(2q)!}I + \frac{(-i)^{2q+1}(\frac{\alpha}{2})^{2q+1}}{(2q+1)!}\sigma_{\vec{m}}\Big) \\ &= \cos\frac{\alpha}{2}I - i\sin\frac{\alpha}{2}\sigma_{\vec{m}} \end{aligned} \tag{78}$$

8 Density matrix and density operator

Until this part, we were using pure state, i.e. states $|\psi\rangle \in \mathscr{H}$. In this part, we will study convexe mixtures/ensembles of pure states, denoted by

$$\{p_i, |\psi_i\rangle\}_i \tag{79}$$

It corresponds to a set of states $|\psi_i\rangle$ that are associated to a probability p_i. The density operator for the system is defined by the equation

$$\rho \equiv \sum_i p_i \underbrace{|\psi_i\rangle\langle\psi_i|}_{\text{density matrix}} \tag{80}$$

The mean value of an observable O can be expressed by the density operator ρ:

$$\begin{aligned} \langle O\rangle_{p_i,\{\psi_i\}} &= \sum_i p_i \underbrace{\langle\psi_i|O|\psi_i\rangle}_{\in\mathbb{R}} \\ &= \sum_i p_i \mathrm{tr}\,(\langle\psi_i|O|\psi_i\rangle) \\ &= \sum_i p_i \mathrm{tr}\,(O\,|\psi_i\rangle\langle\psi_i|) \qquad \text{as } \mathrm{tr}(AB){=}\mathrm{tr}(BA) \\ &= \mathrm{tr}\,\Big(\sum_i p_i O\,|\psi_i\rangle\langle\psi_i|\Big) \\ &= \mathrm{tr}\,(O\rho) = \mathrm{tr}\,(\rho O) \end{aligned} \tag{81}$$

Suppose, for example, that the evolution of a closed quantum system is described by the unitary operator U. If the system was initially in the state $|\psi_i\rangle$, with probability p_i then afer the evolution has occured the system will be in the state $U|\psi_i\rangle$ with probability p_i. Thus, the evolution of the density operator is described by the equation

$$\rho = \sum_i p_i\,|\psi_i\rangle\langle\psi_i| \xrightarrow{U} \sum_i p_i U\,|\psi_i\rangle\langle\psi_i|\,U^\dagger = U\rho U^\dagger \tag{82}$$

Generalized measurements are also described with the density operator. Suppose we perform a measurement described by the measurements operators $\{K_m\}_m$. If the initial state was $|\psi_i\rangle$, then the probability if getting result m is

$$\begin{aligned} \mathbb{P}(m|i) &= \langle\psi_i|K_m^\dagger K_m|\psi_i\rangle \\ &= \mathrm{tr}(K_m^\dagger K_m\,|\psi_i\rangle\langle\psi_i|) \end{aligned} \tag{83}$$

We can interpret this formula as the mean value of the operator K_m over the subspace associated to m, and conclude using (81).

Hence, by the law of total probabilities, the probability of obtaining the result m is

$$\begin{aligned} \mathbb{P}(m) &= \sum_i p_i \mathbb{P}(m|i) \\ &= \sum_i p_i \mathrm{tr}\ (K_m^\dagger K_m |\psi_i\rangle \langle\psi_i|) \\ &= \mathrm{tr}\ (K_m^\dagger K_m \rho) \end{aligned} \tag{84}$$

If the initial state was $|\psi_i\rangle$ then the state after obtaining the result m is

$$|\psi_i^m\rangle = \frac{K_m |\psi_i\rangle}{\sqrt{\langle\psi_i|K_m^\dagger K_m|\psi_i\rangle}} = \frac{K_m |\psi_i\rangle}{\| K_m |\psi_i\rangle \|_2} \tag{85}$$

Example

$$\{(p, |0\rangle), (1-p, |1\rangle)\} \tag{86}$$

Does it exists a state $|\psi\rangle$ representing this ? Recall that for an observable O

$$\langle O\rangle = \sum_i p_i \langle\psi_i|O|\psi_i\rangle \tag{87}$$

Then

$$\begin{aligned} \langle X\rangle &= p\langle 0|X|0\rangle + (1-p)\langle 1|X|1\rangle = 0 = \langle Y\rangle \\ \langle Z\rangle &= p\underbrace{\langle 0|Z|0\rangle}_{=1} + (1-p)\underbrace{\langle 1|Z|1\rangle}_{=-1} = 2p-1 \end{aligned} \tag{88}$$

We see that there is no intersection on the sphere. This implies that there is no $|\psi\rangle$ representing this mixture.

Peculiar density matrices

$$|0\rangle\langle 0| + |1\rangle\langle 1| = |+\rangle\langle +| + |-\rangle\langle -| = Id \tag{89}$$

8.1 Properties of the density operator

In the case of a pure state, a system can be described both by a density operator and by a state vector: with (80), we can easily see that the states $|\psi\rangle$ and $e^{i\varphi}|\psi\rangle$ have the same density operator, hence they describe the same physical state. The density operator therefore has the benefit of removing the arbitrary global phase of a state, that we saw in section 4.5 (p.8) that it was irrelevant.
Other interesting properties of the density operator that come from its definition:

- the density operator is hermitian
$$\rho = \rho^\dagger \tag{90}$$
- semi definite positive, hence its eigenvalues are greater or equal to zero.
$$\forall |\psi\rangle, \langle\psi|\rho|\psi\rangle \geq 0 \tag{91}$$
- tr(ρ) ≤ 1
- tr(ρ^2)=tr(ρ)=1 if and only if the state is pure.
- ρ is diagonalizable, i.e. $\exists \lambda_i \geq 0 : \rho = \sum_i \lambda_i |e_i\rangle\langle e_i|$. And $\{e_i\}_i$ is the cannonical basis: $\forall i, j : \langle e_i|e_j\rangle = \delta_{ij}$

To any ρ such that $\rho = \rho^\dagger$, $\rho \geq 0$ and tr(ρ)=1 corresponds a matrix, since $\rho = \rho^\dagger$, there exists a set $\{|\psi_i\rangle\}$ that form a basis such that $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$.

8.2 Bloch sphere for mixed states

Using the def. (56) of the vector $\vec{m}$ and the def. (68) of the projector onto this vector $\vec{m}$, we have

$$\rho = \sum_i p_i |\vec{m}_i\rangle\langle\vec{m}_i| = \frac{1}{2}\left(Id + \vec{\sigma}\cdot\sum_i p_i \vec{m}_i\right) \tag{92}$$

Any measurement on ρ leads to the same statistics independant of the mixture.
In `BB84`: $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = 2Id = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$

8.3 Composition

As seen previouly, the state $|\psi\rangle_{AB} \in \mathscr{H}_A \otimes \mathscr{H}_B$. From the fact that

$$|\psi'\rangle_{AB} = \sum_{\psi,\varphi} |\psi_A\rangle \otimes |\varphi_B\rangle \neq \Big(\sum_{\psi} |\psi\rangle_A\Big) \otimes \Big(\sum_{\varphi} |\varphi\rangle_B\Big) \tag{93}$$

We can see that the density operator for the composition is defined by

$$\begin{aligned} \rho_{AB} &\equiv \sum_{\psi} |\psi'\rangle_{AB} \langle\psi'|_{AB} \neq \sum \rho_A \otimes \rho_B \\ &\equiv \sum_{\psi,\psi',\varphi,\varphi'} |\psi\rangle_A \langle\psi'| \otimes |\varphi\rangle_B \langle\varphi'| \end{aligned} \tag{94}$$

Criterion to decide if a state is mixed or pure: Let ρ to be in its diagonal form (as ρ hermitian, if not diagonal, it is diagonalizable). Then

$$\begin{aligned} \text{tr } \rho^2 &= \text{tr } \left(U \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_d \end{bmatrix}^2 U^\dagger \right) \\ &= \text{tr } \left(U \begin{bmatrix} \lambda_1^2 & & \\ & \ddots & \\ & & \lambda_d^2 \end{bmatrix} U^\dagger \right) \\ &= \sum_i \lambda_i^2 \\ &= 1 \qquad \text{if and only if } \rho \text{ is pure} \end{aligned} \tag{95}$$

Note: From that we can express by $1 - \text{tr } \rho^2$ the notion of purity of a state.

8.4 Partial trace

Consider a two physical systems $A \in \mathscr{H}_A$ and $B \in \mathscr{H}_B = \mathscr{H}_{AB}$. The space associated to the global system is $\mathscr{H}_A \otimes \mathscr{H}_B$. Let $\{|\psi_i\rangle_A\}_i$ be a basis of A and $\{|\psi_i\rangle_B\}_i$ a basis of B. $\{|\psi_i\rangle_A |\psi_i\rangle_B\}$ is a basis of $\mathscr{H}_{AB}$. The density operator ρ_{AB} acts on the whole system. We are going to define, starting form ρ_{AB}, an operator ρ_A (or ρ_B) that acts only on A (or B).

The reduced density operator for the system A is ρ_A

$$\rho_A \equiv \sum_k \langle\psi_k|_B \, \rho \, |\psi_k\rangle_B \tag{96}$$

ρ_A is obtained from ρ by computing the partial trace on the system B

$$\rho_A \equiv \text{tr}_B(\rho_{AB}) \tag{97}$$

We can deduce from the definitions of ρ_{AB}, ρ_A and ρ_B, that

$$\text{tr}(\rho) = \text{tr}_A(\text{tr}_B\rho) = \text{tr}_B(\text{tr}_A\rho) \tag{98}$$

The trace of the state density operator acting on the system AB is then

$$\text{tr}\rho_{AB} = \sum_{i,k} \big(\langle\psi_i|_A \langle\psi_k|_B \big) \rho_{AB} \big(|\psi_i\rangle_A |\psi_k\rangle_B \big) \tag{99}$$

9 Tomography

9.1 Case of the qubit

We start with $p^{\otimes n}$, that is, n copies of an unknown state p. We suppose, for simplicity, that all of these states are the same. The goal is to write the state p, or any complete description of the state p. The procedure is the following:

1. Split the n copies of the state into 3 sets of size $\frac{n}{2}$
2. Measure X, Y, Z on each set
3. Then deduce the average values of the opertors

$$\langle X\rangle \approx \frac{1}{n/3}\sum_{i=1}^{n/3} x_i \qquad \langle Y\rangle \approx \frac{1}{n/3}\sum_{i=1}^{n/3} y_i \qquad \langle Z\rangle \approx \frac{1}{n/3}\sum_{i=1}^{n/3} z_i \tag{100}$$

4. Finally

$$\rho = \frac{1}{2}\Big(Id + \langle X\rangle X + \langle Y\rangle Y + \langle Z\rangle Z\Big) \tag{101}$$

Exemple of problem

We could get something like $\langle X \rangle = \langle Z \rangle = 1$ as outcome of the measurement. This is physically impossible but could occur due to bad measurement devices.

9.2 Tomography of qubits

For a system of dimension d, it is needed to have a tomographically complete set of observables, which is a basis for the matrices verctor space. The inner product in a matrices vector space can be defined as

$$< A, B >= \mathrm{tr}(A^\dagger B) \tag{102}$$

and is called the Hilbert-Schmidt inner product.
For instance if $d = 2$, then we can use the basis $\mathscr{B} = \left\{ \frac{I}{\sqrt{2}}, \frac{X}{\sqrt{2}}, \frac{Y}{\sqrt{2}}, \frac{Z}{\sqrt{2}} \right\}$ where we have

$$\forall \sigma_i, \sigma_j \in \mathscr{B}, < \sigma_i, \sigma_j >= \delta_{ij} \tag{103}$$

More generally, $\forall d \in \mathbb{N}$, such a basis can be defined by

$$\mathscr{B} = \underbrace{\{ |i\rangle \langle i| \}_i^d}_{\mathbb{1}_d} \cup \underbrace{\{ \frac{|i\rangle \langle j| + |j\rangle \langle i|}{\sqrt{2}} \}_{i<j}^d}_{\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}} \cup \underbrace{\{ \frac{i\,|i\rangle \langle j| - i\,|j\rangle \langle i|}{\sqrt{2}} \}_{i<j}^d}_{\frac{i}{\sqrt{2}}\begin{bmatrix} 1 & \cdots & \cdots & 1 \\ -1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & 1 \\ -1 & \cdots & -1 & 1 \end{bmatrix}} \tag{104}$$

Where $\forall M \in \mathscr{B}, M^\dagger = M$ i.e each matrix of $\mathscr{B}$ is hermitian, and $|\mathscr{B}| = d^2$.
The basis of a matrix vector space is indeed an orthonormal basis, then

$$\begin{aligned} \rho &= \sum_{\sigma \in \mathscr{B}} < \sigma, \rho > \cdot \sigma \\ &= \sum_{\sigma \in \mathscr{B}} \mathrm{tr}(\sigma^\dagger \rho) \cdot \sigma && \text{using eq. (102)} \\ &= \sum_{\sigma \in \mathscr{B}} \mathrm{tr}(\sigma \rho) \cdot \sigma && \text{since } \sigma \in \mathscr{B} \text{ is hermitian} \\ &= \sum_{\sigma \in \mathscr{B}} \langle \sigma \rangle_\rho \cdot \sigma \end{aligned} \tag{105}$$

Hence to reconstruct ρ we only need to measure the average $\langle \sigma \rangle_\rho$ for all σ. Since $|\mathscr{B}| = d^2$ and knowing $\mathrm{tr}(\rho) = 1$, we need $d^2 - 1$ average measurements to reconstruct ρ :

number of qubits in ρ	1	2	3	5
average measurements needed	3	15	63	1023

Table 1: Number of average measurements needed for a n-qubits state reconstruction

The number of average measurement grows very fast, hence we need a more clever way than *brute force*, like compressed sensing (signal processing technique for efficiently acquiring and reconstructing a signal), A.I, etc...

10 Purification

Schmidt decomposition: Suppose $|\psi\rangle_{AB}$ is a pure state of a bipartite system, AB. Then there exist orthonormal states $|e_i\rangle_A$ for system A, and $|e_i\rangle_B$ for system B such that

$$|\psi\rangle = \sum_i \lambda_i |e_i\rangle_A |e_i\rangle_B \tag{106}$$

where $\lambda_i \in \mathbb{R}^+$ and are satisfying $\sum_i \lambda_i = 1$, and $\forall i, j \langle e_i | e_j \rangle = \delta_{ij}$.

The purification of a given density matrix ρ is the process of getting the associated quantum state. In other word it is the converse operation of the trace: since given a state $|\psi\rangle_{AB}$, taking the trace of the state gives us the density matrix ρ_{AB}, purifying the density matrix ρ_{AB} gives us the quantum state $|\psi\rangle_{AB}$.
The natural question that comes is: for all density matrix ρ_A does it exist a pure state $|\psi\rangle_{AB}$ such that $\mathrm{tr}_B |\psi\rangle_{AB} = \rho_B$? The answers is yes and the proof follows.

From section (8.1), any density matrix ρ_A is hermitian and semi-definite positive, i.e $\rho_A = \rho_A^\dagger$ and $\rho_A \geq 0$, and ρ_A is diagonalizable. From theses properties, one can express $|\psi\rangle_{AB}$ in the cannonical basis $\{e_i\}_i$

If $\dim \mathscr{H}_B \geq r$, then the state $|\psi\rangle_{AB}$ can be written

$$|\psi\rangle_{AB} = \sum_{i=0}^{r} \sqrt{\lambda_i}\, |e_i\rangle_A \, |b_i\rangle_B \tag{107}$$

where $\{b_i\}_i$ is an orthonormal basis of $\mathscr{H}_B$

11 Entanglement and Bell inequalities

Consider being in the situation described in Fig. (7), where to parts `A` and `B` are sharing a qubit of the state $|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, where `A` makes its measurement with an angle α and `B` measure with an angle β.

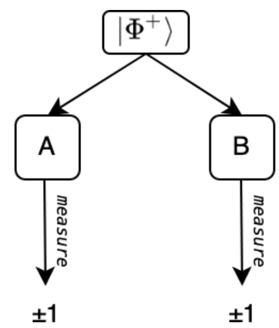

Figure 7: State sharing between `A` and `B`

The observables related to their own measurement are respectively Z_α and Z_β, hence the observable related to the measurement of the global state $|\varphi^+\rangle$ is $Z_\alpha \otimes Z_\beta$, where

$$\begin{aligned}\langle Z_\alpha \otimes Z_\beta\rangle &= \cos\alpha\cos\beta\,\langle Z \otimes X\rangle \\ &+ \sin\alpha\sin\beta\,\langle X \otimes X\rangle \\ &+ \cos\alpha\sin\beta\,\langle Z \otimes X\rangle \\ &+ \sin\alpha\cos\beta\,\langle X \otimes Z\rangle\end{aligned} \tag{108}$$

and

- $\langle\psi^+|Z \otimes X|\psi^+\rangle = \langle\psi^+|\,\frac{1}{\sqrt{2}}\big(Z \otimes X\,|00\rangle + Z \otimes X\,|11\rangle\,\big) = \langle\varphi^+|\,\big(\,|01\rangle - |10\rangle\,\big) = 0$
- $Z \otimes Z\,|00\rangle = |00\rangle$ and $Z \otimes Z\,|11\rangle = |11\rangle \Rightarrow Z \otimes Z\,|\varphi^+\rangle = |\varphi^+\rangle$ hence $\langle\psi^+|Z \otimes Z|\psi^+\rangle = 1$
- $X \otimes X\,|00\rangle = |11\rangle$ and $X \otimes X\,|11\rangle = |00\rangle \Rightarrow X \otimes X\,|\varphi^+\rangle = |\varphi^+\rangle$ hence $\langle\psi^+|X \otimes X|\psi^+\rangle = 1$
- $\langle\psi^+|X \otimes Z|\psi^+\rangle = \langle\psi^+|\,\frac{1}{\sqrt{2}}\big(X \otimes Z\,|00\rangle + X \otimes Z\,|11\rangle\,\big) = \langle\varphi^+|\,\big(\,|10\rangle - |01\rangle\,\big) = 0$

hence

$$\langle Z_\alpha \otimes Z_\beta\rangle = \cos\alpha\cos\beta + \sin\alpha\sin\beta = \cos(\alpha - \beta) \tag{109}$$

The expectation value of the measurement of the shared state φ^+ depends only on the difference of the two angle.

11.1 Local hidden variable theory (LHV)

We now consider that a parameter λ is associated to the starting state $|\varphi^+\rangle$, and that this parameter could be used on the measurement of the state such that the outcome of `A`'s and `B`'s measurements are now functions of λ. Note that no information is sent between `A` and `B`.

Example of LHV

Let λ to be an angle, and the measure along α gives as outcome $+1$ if $|\lambda - \alpha| < \frac{\Pi}{2}$ and -1 if $|\lambda - \alpha| \geq \frac{\pi}{2}$. Given φ^+ choose $\lambda \in [0, 2\pi[$ and set $\lambda_{\mathtt{A}} = \lambda_{\mathtt{B}} = \lambda$. Hence we have

$$\begin{aligned}\langle Z_\alpha \otimes Z_\beta\rangle_{LHV} &= \int \mathbb{P}(\lambda)\cdot Z_\alpha(\lambda)\cdot Z_\beta(\lambda)d\lambda \\ &= \frac{2\big(\pi - |\alpha - \beta|\big) + 2|\alpha - \beta|}{2\pi}\end{aligned} \tag{110}$$

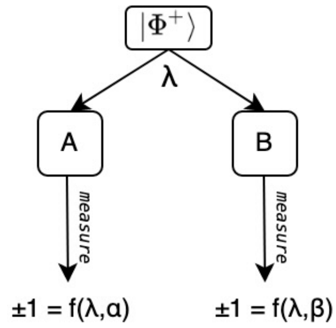

Figure 8

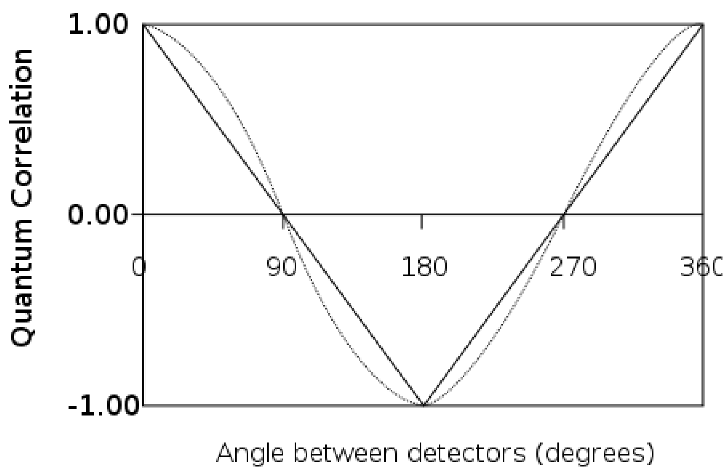

Figure 9: The realist prediction (solid lines) for quantum correlation when there are no non-detections. The quantum-mechanical prediction is the dotted curve.

CHSH test

Choose $\alpha_0, \alpha_1, \beta_0, \beta_1$ such that :

$$S = Z_{\alpha_0} Z_{\beta_0} - Z_{\alpha_0} Z_{\beta_1} + Z_{\alpha_1} Z_{\beta_0} + Z_{\alpha_1} Z_{\beta_1} \tag{111}$$

Classical prediction

Let's assume LHV :

$$\langle S \rangle_{LVH} = \int \mathbb{P}(\lambda) S(\lambda) d\lambda \tag{112}$$

where, from eq. 111 (**note :** all Z depends on λ), we have :

$$S(\lambda) = \underbrace{(Z_{\alpha_0} + Z_{\alpha_1})}_{\oplus} \underbrace{Z_{\beta_0}}_{\pm 1} + \underbrace{(Z_{\alpha_1} - Z_{\alpha_0})}_{\ominus} \underbrace{Z_{\beta_1}}_{\pm 1} \tag{113}$$

and

$$\begin{aligned} Z_{\alpha_1} = \pm Z_{\alpha_0} \Rightarrow & \begin{cases} \oplus = 2, \ominus = 0 & \text{if } Z_{\alpha_1} = Z_{\alpha_0} \\ \oplus = 0, \ominus = 1 & \text{if } Z_{\alpha_1} = -Z_{\alpha_0} \end{cases} \\ & \Rightarrow |S(\lambda)| = 2 \\ & \Rightarrow -2 \le \langle S \rangle_{LHV} \le 2 \end{aligned} \tag{114}$$

From that we obtain the CHSH Inequality :

$$|\langle S \rangle_{LVH}| \le 2 \qquad ; \qquad |\langle S \rangle_Q| \le 2\sqrt{2} \tag{115}$$

11.2 Theories beyond Q : no-signalling

If a state is shared between $\mathtt{A}$ and $\mathtt{B}$, no action of $\mathtt{B}$ changes the measurement statistics of $\mathtt{A}$. Let

$$|\varphi^+\rangle_{\mathtt{AB}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle) \tag{116}$$

On the one hand, if Bob measures Z with the set $\left\{\frac{1}{2}|00\rangle\langle 00|, \frac{1}{2}|11\rangle\langle 11|\right\}$, then the state of Alice is

$$\rho_{\mathtt{A|B}\ \mathrm{m}.Z} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \tag{117}$$

On the other hand, if Bob measures X with $\left\{\frac{1}{2}\left|++\right\rangle\left\langle ++\right|, \frac{1}{2}\left|--\right\rangle\left\langle --\right|\right\}$, then Alice's state is

$$\rho_{\mathtt{A}|\mathtt{B}\ \mathrm{m}.X} = \frac{1}{2}\left|+\right\rangle\left\langle +\right| + \frac{1}{2}\left|-\right\rangle\left\langle -\right| \tag{118}$$

which is the same as the state given that Bob measures Z. All of this implies, for example, that if Bob measures $Z = 0$, then Alice has the state $\left|0\right\rangle_{\mathtt{A}}$ w.p. 1.

Let $x, y \in \{0, 1\}, a, b\{-1, +1\}$, such that $\forall x, y, a, b : \mathbb{P}(a, b|x, y) \geq 0$ and $\forall x, y : \sum_{a,b} \mathbb{P}(a, b|x, y) = 1$.

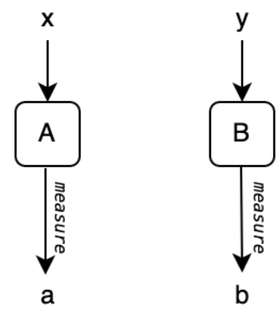

Figure 10: Scheme of the no-signalling setup.

In the case of the no-signalling theory:

$$\mathbb{P}(a|x, y = 0) = \mathbb{P}(a|x, y = 1) = \sum_b \mathbb{P}(a, b|x, y = 0) \tag{119}$$

Hence, again from eq. 111

$$|S_{NS}| \leq 4 \tag{120}$$

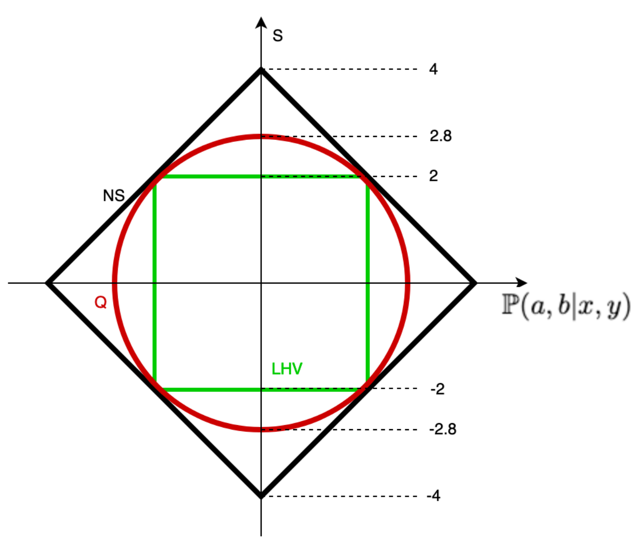

Figure 11: Summary of the presented results

12 Entanglement witnesses and entanglement measures

A much better explanation of entanglement witnesses can be found on the paper of D. Bruss https://arxiv.org/pdf/quant-ph/0110078.pdf

12.1 Easy case: bipartite entanglement of pure states

The question we ask is : given $|\psi\rangle_{AB}$, is it an entangled state ? Where an entangled state is a state that is not separable, and, in the case of pure states, a separable state is a product state: $|\psi\rangle_{AB} \in SEP$ if and only if $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$.

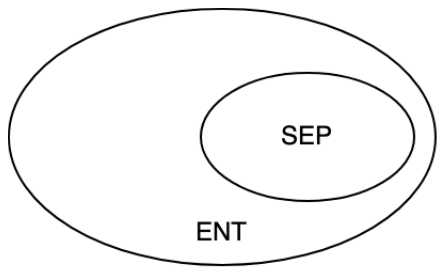

Figure 12: Space of entangled and separable quantum states.

Theorem 2 *For all $|\psi\rangle_{AB} : |\psi\rangle_{AB} \in SEP \Leftrightarrow tr_B[\rho_{AB}]$ is pure.*

Proof: Let $\rho_{AB} = |\psi\rangle_{AB} \langle\psi|_{AB}$ to be the density matrix of $|\psi\rangle_{AB}$.

($\Rightarrow$) If $|\psi\rangle_{AB}$ is separable, then $\exists\, |\psi\rangle_A, |\psi_B\rangle$ such that $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$, which implies that the trace of ρ_{AB} over B is $|\psi\rangle_A$, which is a pure state :

$$\mathrm{tr}_B[\rho_{AB}] = \rho_A \tag{121}$$

($\Leftarrow$) $\mathrm{tr}_B[\rho_{AB}] = |\psi\rangle_A \langle\psi|$. Let us write ρ_{AB} in a basis where $|\psi\rangle_A$ is the first vector. Let $\{|i\rangle_B\}$ to be a basis of $\mathscr{H}_A$, $\{|j\rangle_B\}$ to be a basis of $\mathscr{H}_B$.

$$\rho_{AB} = \sum_{i,j,k,l} \rho_{AB}^{ij,kl} |i\rangle_A |j\rangle_B \langle k|_A \langle l|_B \tag{122}$$

And the trace over B is :

$$\begin{aligned}\mathrm{tr}_B[\rho_{AB}] &= \sum_{i,j,k,l,m} \langle m|_B \rho_{AB}^{ij,kl} |i\rangle_A |j\rangle_B \langle k|_A \langle l|_B |m\rangle_B \\ &= \sum_{i,k,m} \rho_{AB}^{im,km} |i\rangle_A \langle k| \\ &= |\psi\rangle_A \langle\psi| \\ &= |1\rangle_A \langle 1| \quad \text{, since } |\psi\rangle_A \text{ is the first vector of the basis.}\end{aligned} \tag{123}$$

...

Finally, $\mathrm{tr}_B[\rho_{AB}]$ is pure $\Rightarrow \rho_{AB} = |\psi\rangle_A \langle\psi| \otimes |\psi\rangle_B \langle\psi|$

If $\mathrm{tr}_B[\rho_{AB}] = \mathrm{tr}\big[\,|\varphi\rangle_{AB} \langle\varphi|\,\big]$, then $\exists U_B$ such that $|\varphi\rangle_{AB} = Id_A \otimes U_B |\psi\rangle_{AB}$. Hence

$$\mathrm{tr}_B\big[\rho_{AB}\big] = |\psi\rangle_A \langle\psi| = \mathrm{tr}_B\big[\,|\psi\rangle_A |1\rangle_B \otimes \langle 1|_B \langle\psi|_A\,\big] \tag{124}$$

And

$$|\psi\rangle_{AB} = Id_A \otimes U_B\big(\,|\psi\rangle_A \otimes |1\rangle_B\,\big) = |\psi\rangle_A \otimes \underbrace{U_B |1\rangle_B}_{=|\varphi\rangle_B} \tag{125}$$

Hence $|\psi\rangle_{AB}$ is separable.

For pure states, all entanglement measures are equivalent, they are monotonous functions of $S(\mathrm{tr}_B[\rho_{AB}])$ where S is the entropy of entanglement, which is defined as

$$S(\mathrm{tr}_B[\rho_{AB}]) = \sum_i -p_i \log_2 p_i \leq \log_2 \dim \mathscr{H}_A \tag{126}$$

12.2 Bipartite mixed states

We still have the entangled states defined as state that are not separable (i.e. not in SEP), but in the case of mixed states $SEP \supsetneq PROD$ where $PROD$ is the space of product states, i.e there exists mixed states that can not be written as product states, but are still separable states. The space SEP is now defined as :

$$SEP = \big\{\rho_{AB} | \exists \{p_i, \sigma_i, \tau_i\} : \rho_{AB} = \sum_i p_i(\sigma_i \otimes \tau_i)\big\} \tag{127}$$

where σ_i and τ_i are density matrices, and p_i is a probability.

Examples of mixed entangled states :

- $\rho_{AB}^{(1)} = \frac{1}{2}\underbrace{|00\rangle\langle 00|}_{|0\rangle\langle 0|\otimes|0\rangle\langle 0|} + \frac{1}{2}\underbrace{|11\rangle\langle 11|}_{|1\rangle\langle 1|\otimes|1\rangle\langle 1|} \neq \sigma\otimes\tau$ for some σ, τ

- $\rho_{AB}^{(2)} = \frac{1}{2}\varphi^+ + \frac{1}{2}\varphi^-$, where $\varphi^\pm = \begin{bmatrix} 1 & \cdot & \cdot & \pm 1 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \pm 1 & \cdot & \cdot & 1 \end{bmatrix}$

and one can notice that $\mathrm{tr}[\rho_{AB}^{(1)}] = \mathrm{tr}[\rho_{AB}^{(2)}]$

12.3 Entanglement witnesses

Let W to be an entanglement witness, such that $\rho \in SEP \Rightarrow W(\rho) \geq 0$. We do not have $W(\rho) \geq 0 \Rightarrow \rho \in SEP$: if we only have $W(\rho) \geq 0$, we do not know is ρ is entangled or separable. Hence $W(\rho) < 0 \Rightarrow \rho$ is entangled.
W is often linear in ρ : $W(\rho) = \mathrm{tr}[W\rho]$.

Example of entanglement witness : Bell inequalities

The CHSH test is an entanglement witness : $S_{CHSH} \geq 2 \Rightarrow \rho$ is entangled. With that one can define $W_{CHSH} = 2 - S_{CHSH}$. By taking Werner states, let's use W_{CHSH} on it to see if it's entangled. Recall : A Werner state, which is a mixture of Bell state and the identity, is defined as

$$\rho_W(p) = p \cdot \varphi^+ + (1-p)\frac{Id}{4} \tag{128}$$

where $\varphi^+ = |\varphi^+\rangle\langle\varphi^+|$ and $p \in [0,1]$. By using the previouly defined entanglement witness, and $S_{CHSH}(\rho_W) = p \cdot 2\sqrt{2} + (1-p)0$, we obtain

$$W_{CHSH}(\rho_W) = 2 - p2\sqrt{2} \tag{129}$$

This implies that if $p > \frac{1}{\sqrt{2}}$, the state is entangled. In other words, any density matrix that is close enough to the identity is separable.

12.4 Partial transpose

The partial transpose is defined as follows :

$$|ij\rangle\langle kl| \xrightarrow{\Gamma} |kj\rangle\langle il| \tag{130}$$

In other words, if $\rho_{AB} = \sum \rho_{ijkl}|ij\rangle\langle kl|$ then then partial transpose of ρ_{AB} is $\rho_{AB}^\Gamma = \sum \rho_{kjil}|ij\rangle\langle kl|$. The partial transpoe can be seen as the following operation on the matrix elements :

$$\begin{bmatrix} \swarrow\!\!\!\nearrow & \cdots & \swarrow\!\!\!\nearrow \\ \vdots & \ddots & \vdots \\ \swarrow\!\!\!\nearrow & \cdots & \swarrow\!\!\!\nearrow \end{bmatrix} \tag{131}$$

Where $\swarrow\!\!\!\nearrow$ acts on the two by two inner matrices of the main matrix as follow :

$$\swarrow\!\!\!\nearrow \; : \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \longrightarrow \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix} \tag{132}$$

Hence we see that the partial transpose conserves the trace, since the diagonal stays the same, but the eigenvalues are changes.

Exemple 1

$$\varphi^- = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{\quad\Gamma\quad} \varphi^{-\Gamma} = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{133}$$

Where the *central* elements of the partial transpose can be recognized as being $-\sigma_x$, whose eigenvalues are 1 and -1. Hence the eigenvalues of $\varphi^{-\Gamma}$ are $Sp(\varphi^{-\Gamma}) = \{\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\}$. The sum of the four eigenvalues is indeed 1, but there are three probabilities of $\frac{1}{2}$, and one of $-\frac{1}{2}$ which does not make sense. Hence the state is entangled.

Example 2

Let $\rho_W = p \cdot \varphi^+ + (1-p)\frac{Id}{4}$ where $\varphi^+ = |\varphi^+\rangle\langle\varphi^+|$ and $p \in [0,1]$, it's a Werner state.

$$\rho_W = \begin{bmatrix} \frac{1+p}{4} & 0 & 0 & \frac{p}{2} \\ 0 & \frac{1-p}{4} & 0 & 0 \\ 0 & 0 & \frac{1-p}{4} & 0 \\ \frac{p}{2} & 0 & 0 & \frac{1+p}{4} \end{bmatrix} \Rightarrow \rho_W^\Gamma = \begin{bmatrix} \frac{1+p}{4} & 0 & 0 & 0 \\ 0 & \frac{1-p}{4} & \frac{p}{2} & 0 \\ 0 & \frac{p}{2} & \frac{1-p}{4} & 0 \\ 0 & 0 & 0 & \frac{1+p}{4} \end{bmatrix} \tag{134}$$

We easily get two of the four eigenvalues, that are, $\frac{1+p}{4}$. In order to get the two others, we just caculate

$$\begin{aligned} &\det \begin{bmatrix} \frac{1-p}{4}-\lambda & \frac{p}{2} \\ \frac{p}{2} & \frac{1-p}{4}-\lambda \end{bmatrix} = 0 \\ \Rightarrow &\Big(\frac{1-p}{4} - \lambda\Big)^2 = \Big(\frac{p}{2}\Big)^2 \\ \Rightarrow &\frac{1-p}{4} - \lambda = \pm\frac{p}{2} \\ \Rightarrow &\begin{cases} \lambda_+ = \frac{1+p}{4} \\ \lambda_- = \frac{1-3p}{4} \end{cases} \end{aligned} \tag{135}$$

hence the two other eigenvalues are $\lambda_+ = \frac{1+p}{4}$ and $\lambda_- = \frac{1-3p}{4}$. And $\lambda_- = \frac{1-3p}{4} < 0 \Rightarrow p > \frac{1}{3}$. This implies that ρ_W is entangled if $p > \frac{1}{3}$.

Note : The partial transpose is a positive map but not a completely positive map. A map $f : \rho \mapsto f(\rho)$ is completely positive if and only if $(f \otimes Id)(\rho_{AB}) \geq 0$ if $\rho_{AB} \geq 0$. Since ρ_{AB} is a density matrix then it is a positive semi-definite hermitian matrix. But as we saw ρ_{AB}^Γ does not always has positive eigenvalues, and since is ρ_{AB}^Γ symmetric in the example, ρ_{AB}^Γ is not always positive definite.

12.5 Entanglement measure

Let E be an entanglement measure :

$$\begin{aligned} \forall \rho \quad & E(\rho) \in \mathbb{R}^+ \\ \forall \varphi \in SEP \quad & E(\varphi) = 0 \end{aligned} \tag{136}$$

E is *entanglement monotone*, that means E can't increase entanglement. Let `LOOC` to be a Local Operation and Classical Communication. Let P to be an arbitrary `LOCC` operation then

$$E(\rho) \geq E(P(\rho)) \tag{137}$$

Example of entanglement monotone

Let $\mathscr{N}$ be the negativity : based on the partial transpose, it is the sum of the negative eigenvalues. If $Sp(\rho_{AB}^\Gamma) = \{\lambda_i\}_i$ then

$$\begin{aligned} \mathscr{N}(\rho_{AB}^\Gamma) &= \sum_{\lambda_i \leq 0} \lambda_i \\ &= \sum_{\lambda_i \leq 0} |\lambda_i| + \sum_{\lambda_i > 0} \frac{|\lambda_i| - \lambda_i}{2} \\ &= \sum_{\lambda_i} \frac{|\lambda_i| - \lambda_i}{2} \\ &= \frac{||\rho_{AB}^\Gamma||_1 - 1}{2} \qquad \text{since } \mathrm{tr}[\rho_{AB}^\Gamma] = \mathrm{tr}[\rho_{AB}] = 1 \end{aligned} \tag{138}$$

Where $||\rho_{AB}^\Gamma||_1 = \sum_i |\lambda_i| = \mathrm{tr}[\rho] = \mathrm{tr}\big[\sqrt{\rho + \rho}\big]$ denotes the trace norm.

12.5.1 Log-Negativity

The log-negativity is defined as

$$E_{\mathscr{N}} = \log_2 ||\rho_{AB}^\Gamma||_1 = \begin{cases} 0 & \text{for all states with positive partial transpose} \\ > 0 & \text{else} \end{cases} \tag{139}$$

$E_{\mathscr{N}}$ is additive on tensor product and it is an upper bound on the entangled entropy, which is defined in eq. (126). It is related to the negativity as follows:

$$E_{\mathscr{N}} := \log_2(2\mathscr{N} + 1) \tag{140}$$

13 Appendix

13.1 Non-orthogonal quantum states

Distinguish non-orthogonal states

Theorem 3 *Non-orthogonal states can not be reliably distinguish*

Considering two non-orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$, there exist no quantum measurement that can distingxuish reliably between those two states, i.e. there can not exist a pair of operators E_1, E_2 such that

$$\langle\psi_1|E_1|\psi_1\rangle = 1 \quad \langle\psi_2|E_2|\psi_2\rangle = 1 \tag{141}$$

Since $\sum_i E_i = Id$ it follows that $\sum_i \langle\psi_1|E_i|\psi_1\rangle = 1$, and since $\langle\psi_1|E_1|\psi_1\rangle = 1$ we must have $\langle\psi_1|E_2|\psi_1\rangle = 0 \Rightarrow \sqrt{E_2}\,|\psi_1\rangle = 0$.
We can decompose $|\psi_2\rangle$ as

$$|\psi_2\rangle = \alpha\,|\psi_1\rangle + \beta\,|\varphi\rangle \tag{142}$$

where $\langle\psi_1|\varphi\rangle = 0$, $|\alpha|^2 + |\beta|^2 = 1$, and $|\beta| < 1$ as $|\psi_1\rangle$ and $|\psi_2\rangle$ are not orthogonal. Based on our assumption, we have

$$\sqrt{E_2}\,|\psi_1\rangle = 0 \Rightarrow \sqrt{E_2}(|\psi_2\rangle - \beta\,|\varphi\rangle) = 0 \Rightarrow \sqrt{E_2}\,|\psi_2\rangle = \beta\sqrt{E_2}\,|\varphi\rangle \tag{143}$$

which implies that

$$\langle\psi_2|E_2|\psi_2\rangle = |\beta|^2\,\langle\varphi|E_2|\varphi\rangle \leq |\beta|^2 \leq 1 \tag{144}$$

where we used

$$\langle\varphi|E_2|\varphi\rangle \leq \sum_i \langle\varphi|E_i|\varphi\rangle = \langle\varphi|\varphi\rangle = 1 \tag{145}$$

Therefore our assumption contradicts the property of non-orthonormality of the states ($|\beta| < 1$) and can not be true. Thus, one can't reliably distinguish non-orthogonal states.

13.2 Perpendicular state

Given a vector $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, the perpendicular vector $|\psi^\perp\rangle$ is:

$$|\psi^\perp\rangle = -\beta^*\,|0\rangle + \alpha^*\,|0\rangle \tag{146}$$

as can be seen by multiplying the two vectors

$$\begin{aligned}\langle\psi^\perp|\psi\rangle &= (-\beta\,\langle 0| + \alpha\,\langle 1|)(\alpha\,|0\rangle + \beta\,|1\rangle) \\ &= -\beta\alpha + \alpha\beta = 0\end{aligned} \tag{147}$$

13.3 Relation between Bell states

Given a Bell state separated between two parties A and B, it is possible to change the shared state to an other one of the Bell basis with only `LOOC` following this procedure :

$$\begin{tikzcd}
|\phi^+\rangle \arrow[r, leftrightarrow, "\sigma_z^A \text{ or } \sigma_z^B"] \arrow[d, leftrightarrow, "\sigma_x^A \text{ or } \sigma_x^B"'] & |\phi^-\rangle \arrow[d, leftrightarrow, "\sigma_x^A \text{ or } \sigma_x^B"] \\
|\psi^+\rangle \arrow[r, leftrightarrow, "\sigma_z^A \text{ or } \sigma_z^B"] & |\psi^-\rangle
\end{tikzcd}$$

Figure 13: Switching between Bell states with LOOC