Notes of introduction to information processing

Dario Marcone

Samedi 08 novembre 2025

Table des matières

1 Linear algebra in Dirac notation

- A **Hilbert space** is a vector space on complex numbers with an inner product stucture.
- $\mathcal{H}$, $dim\mathcal{H} = d$, colon vectors : $\vec{\psi} = \begin{pmatrix} \psi_1 \\ \dots \\ \psi_d \end{pmatrix}$, $\psi \in \mathbb{C}$, line vectors : $\vec{\psi}^{T,*} = (\psi_1^*, \psi_2^*, \dots, \psi_d^*)$,
  scalar product : $\vec{\phi}^{T,*} \cdot \vec{\psi} = \sum_{i=1}^{d} \phi_i^* \psi_i$.
  (means conjugate)*

1.1 Dirac notation

Ket : $\vec{\psi} = |\psi\rangle$, Bra : $\vec{\psi}^{T,*} = \langle\psi|$, $\implies$ braket : $\vec{\phi}^{T,*}\vec{\psi} = \langle\phi|\psi\rangle$.

1.2 Propreties of Dirac

- **Linearity :** $\left(\alpha^* \langle\psi_1| + \beta^* \langle\psi_2|\right)|\phi\rangle = \alpha^* \langle\psi_1|\phi\rangle + \beta^* \langle\psi_2|\phi\rangle$.
- **Dirac conjugate :** $(|\phi\rangle)^{T,*} = \langle\phi|$.
- **Skew symmetry :** $\langle\phi|\psi\rangle^* = \langle\psi|\phi\rangle$.
- **Norm :** $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$ with properties :
  1. $\|\psi\| \geq 0, \|\psi\| = 0 \leftrightarrow |\psi\rangle = 0$,
  2. $\|\psi_1\| - \|\psi_2\| \leq ||\psi_1\rangle + |\psi_2\rangle| \leq \|\psi_1\| + \|\psi_2\|$,
  3. $|\langle\phi|\psi\rangle| \leq \|\phi\| \cdot \|\psi\|$.
- **Basis :**
  1. Orthonormal Basis : $\{|v_1\rangle, |v_2\rangle, \dots, |v_d\rangle\}$, then $\langle v_i|v_j\rangle = \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$.
  2. Other basis : $\frac{|0\rangle+|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv |+\rangle$, $\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \equiv |-\rangle$.
- **Tensor product :**
  Linear : $(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) = \alpha\gamma|0\rangle\otimes|0\rangle + \alpha\delta|0\rangle\otimes|1\rangle + \beta\gamma|1\rangle\otimes|0\rangle + \beta\delta|1\rangle\otimes|1\rangle$.

Example

Let $\mathcal{H} = \mathbb{C}^2$, $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, then

$$|0\rangle \otimes |0\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \; |0\rangle \otimes |1\rangle = |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|1\rangle \otimes |0\rangle = |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \; |1\rangle \otimes |1\rangle = |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

-

- **Matrices :**
  - Dagger : $A^{T,*} = A^\dagger$, $(A|\psi\rangle)^{T,*} = (A|\psi\rangle)^\dagger = (|\psi\rangle)^\dagger A^\dagger = |\psi\rangle A^\dagger$.
  - Notation : Let $\{|v_1\rangle, \dots, |v_3\rangle\}$ an orthonormal basis and $A_{ij} = \langle v_i| A |v_j\rangle$ ((i,j)th element of the matrice), then $A = \sum_{i,j=1}^{d} A_{ij} |v_i\rangle \langle v_j|$.
  - Hermitian matrices : $A^\dagger = A$ (self-adjoint), i.e. $\begin{pmatrix} 1 & i \\ -i & 0 \end{pmatrix}$.
  - Unitary matrices : $U^\dagger U = UU^\dagger = \mathbb{1}$, $U^\dagger = U^{-1}$, with properties :
    1. $\|U|\psi\rangle\| = \||\psi\rangle\|$,
    2. $\left(\langle\phi| U^\dagger\right)(U|\psi\rangle) = \langle\phi|\psi\rangle$.

2 5 principles of quantum mechanics

2.1 State of a system

The state of an **isolated** system is a vector $|\phi\rangle \in \mathcal{H}$ in Hilbert space $\mathcal{H}$ w.r.t the normalization condition $\langle\phi|\phi\rangle = 1$.

Remarque

$|\phi\rangle$ and $e^{i\lambda}|\phi\rangle, \lambda \in \mathbb{R}$ are physically equivalent.

Examples

1. Let $\mathcal{H} = \mathbb{C}^2 = \{\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \mid \alpha, \beta \in \mathbb{C}\}$ (qubit space), then $\mathbb{C} \implies |\psi\rangle = \alpha|0\rangle + \beta|1\rangle,\ |\alpha|^2 + |\beta|^2 = 1 = \alpha\alpha^* + \beta\beta^*$,
2. Physical system : Mach-Zehnder interferometer
3. Let $\mathcal{H} = \mathbb{C}^d$, $\begin{pmatrix}\alpha_1\\ \dots\\ \alpha_d\end{pmatrix} = |\psi\rangle = \sum_{i=1}^d \alpha_i |i\rangle,\ \sum_{i=1}^d (\alpha_i)^2 = 1$, (qudit space).

-

2.2 States evolve with time

As follows : $|\psi_t| = U_t|\psi_0\rangle$ where U_t is unitary matrix.

Example

We can desribe the transformation of the state of a particle by a prefecting reflecting mirror ($|H\rangle \to |V\rangle$ and $|V\rangle \to |H\rangle$), by

$$U = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\ |H\rangle = \begin{pmatrix}1\\ 0\end{pmatrix},\ |V\rangle = \begin{pmatrix}0\\ 1\end{pmatrix},$$

$$\implies U(\alpha|H\rangle + \beta|V\rangle) = \beta|H\rangle + \alpha|V\rangle.$$

-

2.3 Observable quantities

Quantities that we measure : "observables" are given by Hermitian matrices of dimension $\mathcal{H} \cdot \mathcal{H}$

Example

Observable for 1 qubit $(\mathbb{C}^2)$:

$$A = a\mathbb{1} + bX + cY + dZ,\ A = a^\dagger \implies a, b, c, d \in \mathbb{R}$$

$$\mathbb{1} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}, Z = \begin{pmatrix}1 & 0\\ 0 & -i\end{pmatrix}.$$

-

2.4 Measurement give probability outcome

When observable A is measured, the outcome is a random eigenvalue of A, call it $\lambda_i, i = 1, \ldots, d = dim\mathcal{H}$, the original state before measure $|\psi\rangle$ becomes after measurement an output state $|v_i\rangle$ with eigenvalues corresponding to λ_i. The probability distributioin associated to the output $\lambda_i, |v_i\rangle$ is $prob\,(i) = |\langle v_i|\psi\rangle|^2 \leftarrow$ **BORN RULE**.

- Results of the measurement are eigenvalues λ_i of observable A,
- Every eigenvalue is associated to an eigenvector $|v_i\rangle$,
- If the system is in the original state $|\psi\rangle$, the probability to obtain λ_i is

$$P\,(\lambda_i) = |\langle v_i|\psi\rangle|^2\,,$$

- After the measurement, the state collapse on the eigenvector : $|\psi\rangle \to |v_i\rangle$.

Théorème 1

Spectral Theorem :
Let A be an hermitian matrice $A = A^\dagger$ and let $A\,|v_i\rangle = \lambda_i\,|v_i\rangle\,, i = 1, \ldots, d = dim\mathcal{H}$

- $\lambda_i \in \mathbb{R}$,
- $|v_1\rangle\,, \ldots, |v_d\rangle$ *form an orthogonal basis,*

$$\implies A = \sum_{i=1}^{d} \lambda_i\,|v_i\rangle\,\langle v_i| = \begin{pmatrix} \lambda_1 & \ldots & 0 \\ & \ldots & \\ 0 & \ldots & \lambda_d \end{pmatrix}.$$

- Lemma : $\sum_{i=1}^{d} |\langle v_i|\psi\rangle|^2 = 1$, because $\|\psi\| = 1$.
- Property :
  - $E\,(A) = \sum_{i=1}^{d} \lambda_i\,|\langle v_i|\psi\rangle|^2 = \langle\psi|\,A\,|\psi\rangle$
  - $\mathrm{Var}(A) = \langle\psi|\,A^2\,|\psi\rangle - \langle\psi|\,A\,|\psi\rangle^2$

2.5 Composite system and entanglement

The composite system of $\mathcal{H}_A$ and $\mathcal{H}_B$ is equal to $\mathcal{H}_{A\cup B} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Remarque

$$dim\,(\mathcal{H}_A \otimes \mathcal{H}_B) = (dim\mathcal{H}_A)\,(dim\mathcal{H}_B).$$

Example

$$\mathcal{H}_A = \mathbb{C}^2,\ \mathcal{H}_B = \mathbb{C}^2,\ \mathbb{C}^2 \otimes \mathbb{C}^2 = \begin{cases} |00\rangle = |0\rangle \otimes |0\rangle \\ |01\rangle = |0\rangle \otimes |1\rangle \\ |10\rangle = |1\rangle \otimes |0\rangle \\ |11\rangle = |1\rangle \otimes |1\rangle \end{cases}$$

-

Product states : $|\psi\rangle = |\phi_A\rangle \otimes |\chi_B\rangle\,,\ \psi \in \mathcal{H}_A \otimes \mathcal{H}_B,\ \phi \in \mathcal{H}_A,\ \chi \in \mathcal{H}_B$.

Entangled states : $\nexists$ a factorisation of the state.

Example

$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$.

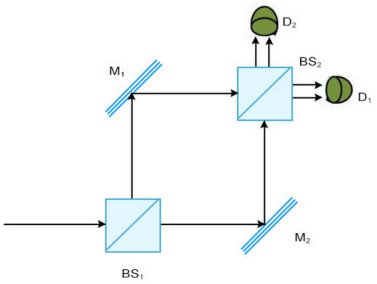
-

Apparté

Bloch sphere of a qubit state vector :
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$.

3 Applications of principles

3.1 Mach-Zehnder interferometer



- **Space :** $\mathcal{H} = \mathbb{C}^2 = \{\begin{pmatrix}\alpha\\ \beta\end{pmatrix},\ \alpha\beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1\}$.
- **Basis :** $\begin{pmatrix}1\\0\end{pmatrix} = |H\rangle$, $\begin{pmatrix}0\\1\end{pmatrix} = |V\rangle$, $\alpha|H\rangle + \beta|V\rangle = |\psi\rangle$.
- **Beam splitter :** $U = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ (Hadamard matrix).
- **State after the beam splitter :** $U|H\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$.

Remarque

It's a very srange state that is at the same time horizontal and vertical. If it wasn't a qubit, it would either be completely reflected or it would go through.

- **Perfect mirror :** $R = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, $RR^\dagger = R^\dagger R = 1$ (**important condition !**), $R^\dagger = R$ (coincidence).
- **State after the perfect mirror :** $RU|H\rangle = \frac{1}{\sqrt{2}}(R|H\rangle + R|V\rangle) = \frac{1}{\sqrt{2}}(|V\rangle + |H\rangle)$.
- **State after the second beam splitter :** $URU|H\rangle = \frac{1}{\sqrt{2}}(U|V\rangle + U|H\rangle)$.
- **State before the detector :** $\psi_{\text{before detector}} = 2 \cdot \frac{1}{2}|H\rangle = |H\rangle$.
- **Measurement :** model with orthogonal basis of $\mathcal{H} = \mathbb{C}^2 = \{|H\rangle \text{ and } |V\rangle\}$:
  At the end of the interferometer, we measure state $|H\rangle$ or state $|V\rangle$,
  if we measure $|H\rangle \implies$ clic in $D_1 \implies$ register $+1$,
  if we measure $|V\rangle \implies$ clic in $D_1 \implies$ register -1.
  By the Born rule :

$$prob\,(+1) = |\langle H|\psi_{\text{before detector}}\rangle|^2 = 1$$
$$prob\,(-1) = |\langle V|\psi_{\text{before detector}}\rangle|^2 = 0$$

  If we follow the 4^{th} *principle*, then we know that $|H\rangle$ and $|V\rangle$ are the eigenvectors of our observable and $(+1)$ and (-1) are the eigenvalues of our observable.

  By spectral theorem, we define our observable : $(+1)|H\rangle\langle H| + (-1)|V\rangle\langle V| = \begin{pmatrix}+1 & 0\\ 0 & -1\end{pmatrix} = Z$.

Expectated value of (Z) : $\langle\psi_{\text{before detector}}| Z |\psi_{\text{before detector}}\rangle = \langle H| \{(+1) |H\rangle \langle H| + (-1) |V\rangle \langle V|\} |H\rangle = (+1) \langle H|H\rangle \langle H|H\rangle + (-1) \langle H|V\rangle \langle H|V\rangle = (+1)$.
Var(Z) : $\langle\psi| Z^2 |\psi\rangle - \langle\psi| Z |\psi\rangle^2 = 0$.

3.2 Photon polarization

- **Classical electro-magnetic waves :**

$$\text{Linear polarization : } \vec{E} \propto \vec{E}_0 \begin{pmatrix} \cos\theta \\ \sin\theta \\ 0 \end{pmatrix} e^{i\omega t} e^{i\frac{2\pi}{\lambda}z},$$

$$\text{Circular polarization : } \vec{E} \propto \vec{E}_0 \begin{pmatrix} 1 \\ i \\ 0 \end{pmatrix} e^{i\omega t} e^{i\frac{2\pi}{\lambda}z}.$$

Remarque

The polarization of an electro-magnetic wave indicate how the electrique field oscillate in space and time (it shows the direction).

- **Photon quantum particles :** Photon quantum particles that carry electro-magnetic energy have a polarization state :
Linear polarization state : $|\theta\rangle = \cos\theta |x\rangle + \sin\theta |y\rangle$, $|\theta_\perp\rangle = -\sin\theta |x\rangle + \cos\theta |y\rangle$.
Circular polarization state : $|\circlearrowleft\rangle = \frac{1}{\sqrt{2}} (|x\rangle + i |y\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$, $|\circlearrowright\rangle = \frac{1}{\sqrt{2}} (|x\rangle - i |y\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}$.

Remarque

A classical electro-magnetic wave can be viewed as a collective state of many photons, each having the same polarization state. This photon polarization state determine the direction and the form of oscillation of the electric field in the corresponding classical wave.

4 Quantum key distribution (QKD)

Classical protcols rely on some mathematicals problems believed to be hard, but one day, if there is some strong enough computer, the security wouldn't be assured. QKD rely on physics ! So it doesn't have this problem, the disavantage is that you should have a quantum channel.

4.1 Key distribution

1. Suppose Alice wants to send $\vec{m}$. She encodes it as $\vec{m} \oplus \vec{x} = \vec{z}$.
2. Bob receives $\vec{z}$. He adds $\vec{x} \implies \vec{z} \oplus \vec{x} = (\vec{m} \oplus \vec{x}) \oplus \vec{x} = \vec{m} \oplus (\vec{x} \oplus \vec{x}) = \vec{m}$.

4.2 BB84 protocol

For quantum key distribution protocols, we assume that :

- A, B share a public classical channel that is not spoofable.
- A, B share a public quantum channel that is spoofable.

Setting : Alice has generated ($\vec{x} \in \{0,1\}$) and wants to share it with Bob.

1. Alice encodes $\vec{x}$ as a quantum state of qubit.
2. Bob decodes the q-state back into qbitstring.
3. Public communication phase (through the classical channel).
4. Generation of the common secret key + security check.

1. **Step Encoding :**
   Alice encodes each $x \in \{0,1\}$ in a random basis (either X or Z basis) :
   - Z basis : $|0\rangle, |1\rangle, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
   - X basis : $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, |+\rangle \frac{|0\rangle + |1\rangle}{\sqrt{2}}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

x_1	**Z basis**
0	$\|0\rangle$
1	$\|1\rangle$
	X basis
0	$\|+\rangle$
1	$\|-\rangle$

   Let define H such that : $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$.
   Alice sends $|0\rangle |+\rangle |-\rangle |0\rangle |1\rangle |1\rangle |+\rangle$, so she sends :

$$|\psi_{x_1}\rangle = H^{ei}|x_1\rangle \text{ where ei} \sim \text{Unif } \{0,1\} \implies |\psi_{\vec{x}}\rangle = \bigoplus_{j=1}^{m} H^{ei}|x_j\rangle .$$

2. **Step Decoding :**
   Bob recieves $|\psi_{\vec{x}}\rangle = \bigoplus_{j=1}^{m} H^{ei}|x_j\rangle$, he chooses a random basis to measure it. If Bob know the basis, he can decode easily, he doesn't !
   - Case 1 : Bob measure in the same basis chosen by Alice → prob(decoding correctly)=1.
   - Case 2 : Bob measures in the wrong basis → prob(decoding correctly)=$\frac{1}{2}$.

   $\implies$ prob(decoding correctly)=$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$.
3. **Step Public communication :**
   Alice has $\vec{x}$: original bitstring, $\vec{e}$: original choice of basis.
   Bob has $\vec{y}$: decoded bitstring, $\vec{f}$: Bob's choice of basis.
   They publish over the classical channel their choice of $\vec{e}, \vec{f}$, and for each bit, if the base agree they keep the bit, otherwise they discard it. At the end, Alice has $\widetilde{x} \subset \vec{x}$ and Bob has $\widetilde{y} \subset \vec{y}$.
4. **Step Security check :**
   Let $\widetilde{x}, \widetilde{y}$ be of length k. Alice and Bob pick a subset of k bits to "sacrifice" them : they exchange the bits over the public channel,
   - if they match, we can exclude that there is an eavesdropper,
   - otherwise we can conclude that there is an eavesdropper so we abort the protocol.

Remarque

When the eavesdropper look at a qubit on the quantum channel, he has to measure the qubit $\implies$ the state of the particle collapse. So if Alice and Bob have the same basis, but not the same bit, they can assume that an eavesdropper has intercepted and measured a qubit in the wrong basis, and then sent a modified state to Bob.

Let now see what is the probability that Alice and Bob have the same bit knowing that an eavesdropper (Eve) intercept it.

$$\text{prob(Eve's measured bit agrees)} = \begin{cases} \text{case 1 : correct base} \implies \text{prob(correct)} = 1 \\ \text{case 2 : wrong base} \implies \text{prob(correct)} = \frac{1}{2} \end{cases}$$

$$\implies \text{prob(Eve's measured bit agrees)} = \frac{3}{4}.$$

$$\text{prob(Bob correct} \mid \text{Eve's intercepted)} = \begin{cases} \text{case 1 : Eve was correct} \implies \frac{3}{4} \cdot \frac{3}{4} = \frac{9}{16} \\ \text{case 2 : Eve was wrong} \implies \frac{1}{4} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{16} \end{cases}$$

$$\implies \text{prob(Bob correct} \mid \text{Eve intercepted)} = \frac{9}{16} + \frac{1}{16} = \frac{5}{8}.$$

Maybe sometimes bits of Alice and Bob can disagree not because of an eavesdropper but because of **noise**! To deal with noise we can use some classical error connection.

Example

Repetition code : Suppose noise flips with probability $\frac{1}{3}$. If i want to send a bit b over a noisy channel instead i'll send $bb\bar{b}$.

- Binary linear code : $C \subset \mathbb{F}_2^m$, $|C| = 2^k, [m, k, d]$ with
  - m : length of the codeword,
  - k : actual of bits of information per codeword,
  - d : minimum distance of the code (minimum number of bits differing between 2 vectors in C, in general d=m).

-

In the BB84 protocol, we can apply this by supposing that we expect ϵ fraction of bits to differ between $\widetilde{x}$ and $\widetilde{y}$ because of noise.

- After step 3, Alice chooses an ECC C that corrects ϵ' fraction of the bits and compute $\vec{c}$ $(\epsilon' > \epsilon)$.
- She sends $m = \widetilde{x} \oplus \vec{c}$ to Bob over the classical channel.
- Bob compute $\vec{c}\,' = \widetilde{y} \oplus m = (\widetilde{x} \oplus \widetilde{y}) \oplus \vec{c}$, where $\widetilde{x} \oplus \widetilde{y} =$ errors.
- Then because $\vec{c}\,' = \vec{c} \oplus$errors, Bob can recover $\vec{c}$ with the ECC and compute $m \oplus \vec{c} = (\widetilde{x} \oplus \vec{c}) \oplus \vec{c} = \widetilde{x}$.

5 Entanglement

Let be 2 parts : AB, $\mathcal{H}_{\text{total}} = \mathcal{H}_A \otimes \mathcal{H}_B$, then there is two types of states :

product states : $|\psi\rangle = |\phi_A\rangle \otimes |\chi_B\rangle$,
entangled states : $|\psi\rangle$ such that $\nexists$ a factorization into tensor product.

Example

Let $\mathcal{H}_{\text{total}} = \mathbb{C}^2 \otimes \mathbb{C}^2$, $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, $|ab\rangle = |a\rangle \otimes |b\rangle$, $a_{ij} \in \mathbb{C}$, $\sum_{i,j=(0,0)}^{(1,1)} |\alpha_{ij}|^2 = 1$, $\langle\psi|\psi\rangle = 1$.
Product state :
$|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$ such that $\alpha_{00} = \alpha\gamma, \alpha_{01} = \alpha\delta, \alpha_{10} = \beta\gamma, \alpha_{11} = \beta\delta$.

$$\det\begin{pmatrix} \alpha_{00} & \alpha_{01} \\ \alpha_{10} & \alpha_{11} \end{pmatrix} = det\,(\alpha)_{ij} = \alpha_{00}\alpha_{11} - \alpha_{01}\alpha_{10} = \alpha\gamma\beta = -\alpha\delta\beta = 0.$$

$$|\psi\rangle \textbf{ is a product state} \iff \det\begin{pmatrix} \alpha_{00} & \alpha_{01} \\ \alpha_{10} & \alpha_{11} \end{pmatrix} = 0.$$

-

Entangled state :
We will use the Bell states :

- $|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- $|B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
- $|B_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
- $|B_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

Properties :

1. They form an orthonormal basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$
$$\langle B_{ij}|B_{ij}\rangle = 1,\ \langle B_{ij}|B_{kl}\rangle,\ (ij) \neq (kl).$$
2. "Rotation invariance" : $|B_{00}\rangle = \frac{1}{\sqrt{2}}(|\theta\rangle \otimes |\theta\rangle + |\theta_\perp\rangle \otimes |\theta_\perp\rangle)\ \forall\theta$.

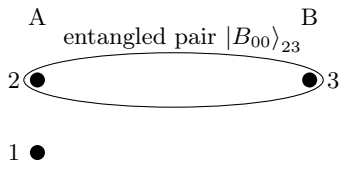
-

5.1 Teleportation

The goal of teleportation is to teleport a quantum state or some information from A to B without physically transporting any qubit, we will however send classical messages

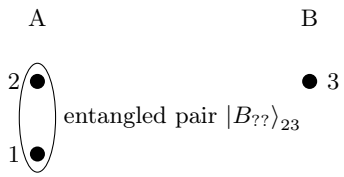
- **Initial situation :**

$$\overbrace{\mathbb{C}^2_1 \otimes \mathbb{C}^2_2}^{Alice} \otimes \overbrace{\mathbb{C}^2_3}^{Bob},\ |\phi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1,\ |B_{00}\rangle_{23} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$



- **Final situation :**

$$|B_{??}\rangle_{12},\ |\phi\rangle_3 = \alpha|0\rangle_2 + \beta|1\rangle_3.$$



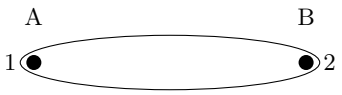
- **Protocol steps :**
  1. Alice does a Bell basis measurement in her lab, so her qubits collapse into one of the fourth possible Bell states, the total state becomes
  $$\left(|B_{ij}\rangle_{12}\langle B_{ij}|_{12} \otimes \mathbb{1}_3\right)|\phi\rangle_1 \otimes |B_{00}\rangle_{23} = |B_{ij}\rangle_{12} \otimes |\widetilde{\phi}\rangle_3.$$
  2. Alice sends two classical bits of information to Bob : 00, 01, 10, 11.

3. Bob receives a classical message $ij \in \{00, 01, 10, 11\}$ and does the following :

$$
\begin{aligned}
&00 \to \text{Bob applies } \mathbb{1} \text{ on his qubit,} \\
&01 \to \text{Bob applies } X_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ on his qubit,} \\
&10 \to \text{Bob applies } Z_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ on his qubit,} \\
&11 \to \text{Bob applies } Z_3 X_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ on his qubit,}
\end{aligned}
$$

5.2 Dense coding

The goal is to send two classical bits from A to B of information by one use of quantum channel.



Protocol :
If Alice wants to encode

$$
\begin{aligned}
&00 \to \text{she applies } \mathbb{1}_1 \otimes \mathbb{1}_2 \left|B_{00}\right\rangle_{12} = \left|B_{00}\right\rangle_{12}, \\
&01 \to \text{she applies } X_1 \otimes \mathbb{1}_2 \left|B_{00}\right\rangle_{12} = \left|B_{01}\right\rangle_{12}, \\
&10 \to \text{she applies } Z_1 \otimes \mathbb{1}_2 \left|B_{00}\right\rangle_{12} = \left|B_{10}\right\rangle_{12}, \\
&11 \to \text{she applies } Z_1 X_1 \otimes \mathbb{1}_2 \left|B_{00}\right\rangle_{12} = \left|B_{11}\right\rangle_{12},
\end{aligned}
$$

Then she sends her obtained qubit so Bob have both qubit $\to$ the total state. So he knows which bits Alice encoded.

6 Bell inequalities

The goal here will be to ensure that A B share an entangles Bell state (inequality) and as a consequence are able to produce common random secret strings of bits (Ekert 91 QKD protocol).

Let

measure the qubit.

- basis : $\{|\alpha\rangle, |\alpha_\perp\rangle$,
  record $a = \pm 1$.
- basis $\{|\alpha'\rangle, |\alpha'_\perp\rangle$,$\}$
  record $a' = \pm 1$.

pairs of photons
with pol. state.
$i = 1, \ldots, N$.

measure the qubit.

- basis : $\{|\beta\rangle, |\beta_\perp\rangle$,
  record $b = \pm 1$.
- basis $\{|\beta'\rangle, |\beta'_\perp\rangle$,$\}$
  record $b' = \pm 1$.

There is four possible measure settings for A and B : $1 = (\alpha, \beta), 2 = (\alpha', \beta), 3 = (\alpha, \beta'), 4 = (\alpha', \beta')$.
A and B meet or communcate classically and compute so-called correlation coefficient :

$$
X_{exp} = \frac{1}{N_1} \sum_{i_1} a_{i1} b_{i1} + \frac{1}{N_2} \sum_{i_2} a'_{i2} b_{i2} + \frac{1}{N_3} \sum_{i_3} a_{i3} b'_{i3} + \frac{1}{N_4} \sum_{i_4} a'_{i4} b'_{i4}
$$

Classical prediction ($X_{\text{class. th}}$) :

We assume a locality of measurement result, which means that $p_A(a)$ depends only of Alice's angle and $p_B(b)$ depends only of Bob's angle,

$$\implies p(a,b|\alpha,\beta,\lambda) = p_A(a|\alpha,\lambda)\, p_B(b|\beta,\lambda) \text{ with } \lambda = \text{ random variable with distribution } h(\lambda)\, d\lambda.$$

Lemma :

$$-2 \leq X_{\text{class. th.}} \leq 2 \text{ for } N \to +\infty.$$

Quantum theory :

$$X_{\text{th. quant.}} = \langle B_{00}| A \otimes B |B_{00}\rangle + \langle B_{00}| A' \otimes B |B_{00}\rangle - \langle B_{00}| A \otimes B' |B_{00}\rangle + \langle B_{00}| A' \otimes B' |B_{00}\rangle .$$

Observables :

$$A = (+1)\,|\alpha\rangle\langle\alpha| + (-1)\,|\alpha_\perp\rangle\langle\alpha_\perp|\,,\ B = (+1)\,|\beta\rangle\langle\beta| + (-1)\,|\beta_\perp\rangle\langle\beta_\perp|\,,$$

$$\text{with } |\alpha\rangle = \cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle\,,\ |\alpha_\perp\rangle = -\sin\alpha\,|0\rangle + \cos\alpha\,|1\rangle \text{ and same for } \beta.$$

$$\implies X_{\text{th. quant.}} = \cos(2(\alpha-\beta)) + \cos(2(\alpha'-\beta)) - \cos(2(\alpha-\beta')) + \cos(2(\alpha'-\beta'))\,.$$

Entanglement induces non-locality, so according to QM :

$$p(a,b|\alpha,\beta) = |\langle \text{state after meas.}|B_{00}\rangle|^2 = \frac{1}{4}\left(1 + ab\cos(2(\alpha-\beta))\right) \neq p_A(a|\alpha)\, p_B(b|\beta)\,.$$

If we choose angles when $X_{\text{th. quant.}}$ is maximal $\left(\beta = \frac{\pi}{8},\ \alpha = 0,\ \beta' = -\frac{\pi}{8},\ \alpha' = -\frac{\pi}{8}\right)$, then $X_{\text{th. quant.}} = 2\sqrt{2} > \mathbf{2}$**! It violates the Lemma!**

If source distribute tensor product state $|\phi_A\rangle \otimes |\phi_B\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ then :

$$p(a,b|\alpha,\beta) = |\langle \text{state after meas.}|\left(|\phi_a\rangle \otimes |\phi_B\rangle\right)\rangle|^2$$

$$= \underbrace{\left(\left(\frac{1+a}{2}\right)|\langle\alpha|\phi_A\rangle|^2 \left(\frac{1-a}{2}\right)|\langle\alpha_\perp|\phi_A\rangle|^2\right)}_{p_A(a|\alpha)} \underbrace{\left(\left(\frac{1+b}{2}\right)|\langle\beta|\phi_B\rangle|^2 \left(\frac{1-b}{2}\right)|\langle\beta_\perp|\phi_B\rangle|^2\right)}_{p_B(b|\beta)}.$$

If the pair is a product state it can't be greater than 2, $\implies$ if the result violates the Bell inequality it's an entangled state!

6.1 Ekert 91

Let

measure in possible basis :

- $\alpha_1 = -\frac{\pi}{4}$,
- $\alpha_2 = -\frac{\pi}{8}$,
- $\alpha_3 = 0$,

EPR pairs, $|B_{00}\rangle$.

measure in possible basis :

- $\beta_1 = -\frac{\pi}{8}$
- $\beta_2 = 0$
- $\beta_3 = \frac{\pi}{8}$

A and B exchange the basis choices at each $1, \ldots, N$ and compute X_{Bell} using the bits among (x_i, y_i) only those corresponding to CSHS basis choice, $|X_{Bell}| \approx 2\sqrt{2}$, otherwise there is an eavesdropper.

Common key one time pad is given by x_i and y_i such that A and B choose the same basis, (α_3, β_2) or (α_2, β_1). In this case $x_i = y_i$.

7 Density matrix

There is two situations where density matrix are useful :

1. Statistical mixtures.
2. Physical systems that are not isolated.

7.1 Statistical mixture

A statistical mixture is a system of N degrees of freedom (quantum particles), where

$$\begin{aligned}&\text{fraction } p_1 \text{ of degree of freedom is in state } |\phi_1\rangle \in \mathcal{H},\\ &\text{fraction } p_2 \text{ of degree of freedom is in state } |\phi_2\rangle \in \mathcal{H},\\ &\qquad\dots\\ &\text{fraction } p_k \text{ of degree of freedom is in state } |\phi_k\rangle \in \mathcal{H},\end{aligned}$$

$$0 \leq p_i \leq 1, \sum_{i=1}^{k} p_i = 1.$$

Convenient useful description is through the density matrix : $\rho = \sum_{i=1}^{k} p_i \left|\phi_i\right\rangle \left\langle\phi_i\right|$

Remarque

Density matrix is a convex linear combination of projections : $\left|\phi_i\right\rangle \left\langle\phi_i\right| = \pi_i,\ \pi_i \left|\psi\right\rangle = \left|\phi_i\right\rangle \left\langle\phi_i|\psi\right\rangle,\ \pi_i^{+} = \pi_i,\ \pi_i^2 = \pi_i.$

From a statistical mixture, we get a state $|\phi_i\rangle$ with probability p_i, then we measure $|\phi_i\rangle$, what's the expectation of A ?

Remarque

Cyclicity of Trace :

$$Tr\left(AB\right) = Tr\left(BA\right),\ Tr\left(ABC\right) = Tr\left(CAB\right) = Tr\left(BCA\right).$$

Expectated value of A notated <A> :

$$\sum_{i=1}^{k} p_i \left\langle\phi_i\right| A \left|\phi_i\right\rangle = \sum_{i=1}^{k} p_i Tr\left(A \left|\phi_i\right\rangle \left\langle\phi_i\right|\right) = Tr\{\sum_{i=1}^{k} p_i A \left|\phi_i\right\rangle \left\langle\phi_i\right|\} = TrA\left(\sum_{i=1}^{k} p_i \left|\phi_i\right\rangle \left\langle\phi_i\right|\right) = Tr\left(A\rho\right).$$

$$< A >= Tr\left(A\rho\right) = Tr\left(\rho A\right), \quad Var\left(A\right) =< A^2 > - < A >^2 = Tr\left(A^2\rho\right) - \left(Tr\left(A\rho\right)\right)^2.$$

Théorème 2

1. *A density matrix satisfies* $\rho^{\dagger} = \rho,\ \rho \geq 0,\ Tr\rho = 1.$
2. *Vice-versa any matrix satisfying these 3 proposition is a density matrix.*

7.2 Partial trace

M acts on $\mathcal{H}_1 \otimes \mathcal{H}_2$, orthonormal basis can be $|v_i\rangle \otimes |w_j\rangle$ with $i = 1 \dots dim\mathcal{H}_1$ and $j = 1 \dots dim\mathcal{H}_2$.

$$M = \sum_{ij;kl} M_{ij;kl} \left(\left|v_i\right\rangle \otimes \left|w_j\right\rangle\right) \left(\left|v_k\right\rangle \otimes \left|w_l\right\rangle\right), \quad M_{ij;kl} = \left(\left|v_i\right\rangle \otimes \left|w_j\right\rangle\right) M \left(\left|v_k\right\rangle \otimes \left|w_l\right\rangle\right).$$

Full trace : $TrM = \sum_{ij} M_{ij;ij}$, partial trace : $Tr_{\mathcal{H}_1} M = \sum_{j;l} \left(\sum_i M_{ij;il}\right) \overbrace{\left|w_j\right\rangle \left\langle w_l\right|}^{dim\mathcal{H}_2 \cdot dim\mathcal{H}_2}$.

Remarque

You can vizualize this by thinking that M like a big matrice of size $(dim\mathcal{H}_1 dim\mathcal{H}_2) \cdot (dim\mathcal{H}_1 dim\mathcal{H}_2)$ and that the partial trace correspond to slice this matrice in blocs corresponding to $\mathcal{H}_1$ and compute the trace on these blocs.

Properties :

- $Tr_{\mathcal{H}_1} Tr_{\mathcal{H}_2} M = \overbrace{Tr_{\mathcal{H}_1 \mathcal{H}_2}}^{\text{full trace}} M = Tr_{\mathcal{H}_2} Tr_{\mathcal{H}_1} M$,
- In special case $A \otimes B$:

$$Tr_{\mathcal{H}_1}(A \otimes B) = (Tr_{\mathcal{H}_1} A) B, \;\; Tr_{\mathcal{H}_2}(A \otimes B) = A (Tr_{\mathcal{H}_2} B), \;\; Tr_{\text{full}} A \otimes B = (Tr_{\mathcal{H}_1} A)(Tr_{\mathcal{H}_2} B).$$

7.3 Partial density matrix

Let ρ be a full system $\mathcal{H}_{\text{full}} = \mathcal{H}_A \otimes \mathcal{H}_B$, then the local description of system A is given by

$$Tr_{\mathcal{H}_B} \rho \equiv \rho_A.$$

When you have a non-isolated system S, it means that the system interact with an environement E, and $|\psi\rangle \in \mathcal{H}_S \otimes \mathcal{H}_E$, $\rho_{S \cup E} = |\psi\rangle \langle\psi|$. Then to compute the state of the sub-system S, you have to compute

$$\rho_S = Tr_E |\psi\rangle \langle\psi|.$$

Therefore, the general state of a non-isolated systemn is a density matrix !

Computation :

1. Choose an orthonormal basis on B : $\{|i_B\rangle\}$, $i_B \in \{0,1\}^{n_B}$.
2. $\rho_A = \sum_{i_B} (\mathbb{1}_A \otimes \langle i_B|) \rho_{AB} (\mathbb{1}_A \otimes |i_B\rangle)$.

Properties :

- If $M = A \otimes B$ thne $M_B = Tr(A) \cdot B$,
- If M a density matrix $= \rho_A \otimes \rho_B$ then $M_B = \underbrace{Tr(\rho_A)}_{=1} \rho_B = \rho_B$.

8 Von Neumann entropy

8.1 Classical entropy

For a random variable X, the entropy of X, $H(X) \approx$ amount of uncertainty :

$$H(X) := -\sum_i p_i \log(p_i).$$

$H(X)$ is maximized for the distribution over X that puts equal probabilities for all outcomes and is minimized if all its probability is on a single outcome.

8.2 Quantum entropy

Let ρ be a density matrix, its Von Neumann entropy is

$$S(\rho) := -Tr(\rho \log(\rho)).$$

Remarque

Diagonal elements of ρ are a classical probability distribution, $Tr(\rho \log \rho)$ means :

- write ρ in its eigenbasis : $\rho = \sum_i \lambda_i |i\rangle \langle i|$,
- $-Tr(\rho \log \rho) = -\sum_{n=1}^{d} \lambda_i \log(\lambda_i)$.

Properties :

- $S(\rho) \geq 0$,
- $S(\rho)$ is maximal for $\rho = \frac{\mathbb{1}}{d} = \begin{pmatrix} \frac{1}{d} & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & \frac{1}{d} \end{pmatrix}$,
- $S(\rho) = 0 \iff \rho$ is a pure state $\iff \rho = |\psi\rangle\langle\psi|$,
- Concavity : $S(\alpha\rho_1 + (1-\alpha)\rho_2) \geq \alpha S(\rho_1) + (1-\alpha) S(\rho_2)$.

8.3 Entropy of a single qubit

For a single qubit, the density matrix is

$$\rho = \frac{1}{2}(\mathbb{1} + \vec{a}\cdot\vec{\sigma}) = \frac{1}{2}\begin{pmatrix} \mathbb{1} + a_z & a_x + ia_y \\ a_x - ia_y & \mathbb{1} - a_z \end{pmatrix}, \quad \|\vec{a}\| < 1,\ \vec{\sigma} = [\sigma_x\ \sigma_y\ \sigma_z].$$

Then we can do a basis change $\rho \to \rho'$ such that $S(\rho) = S(\rho')$ but $S(\rho')$ is much easier to calculate. For this case, the basis change is

$$\rho' = \begin{pmatrix} \frac{1+\|\vec{a}\|}{2} & 0 \\ 0 & \frac{1+\|\vec{a}\|}{2} \end{pmatrix}.$$

because $\lambda_{1,2} = \frac{1\pm\|\vec{a}\|}{2}$.

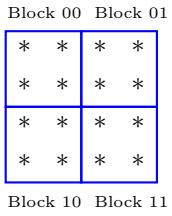
$$\implies S(\rho) = S(\rho') = H\left(\frac{1+\|\vec{a}\|}{2}, \frac{1-\|\vec{a}\|}{2}\right).$$

8.4 Compute a partial density matrix

If overall state $\in \mathcal{H}_{AB}$ is ρ_{AB} with n_A =qubits in A and n_B =qubits in B, then

$$\rho_A = \sum_{i\in\{0,1\}^{n_B}} (I_A \otimes \langle i|_B)\,\rho_{AB}\,(I_A \otimes |i\rangle_B),$$
$$\rho_B = \sum_{i\in\{0,1\}^{n_A}} (\langle i|_A \otimes I_B)\,\rho_{AB}\,(|i\rangle_A \otimes I_B).$$

Special case : $n_A = n_B = 1$, $\rho_{AB} =$



Then

$$\rho_A = \begin{pmatrix} * & * \\ * & * \end{pmatrix} = \begin{pmatrix} Tr\,(\text{Block 00}) & Tr\,(\text{Block 01}) \\ Tr\,(\text{Block 10}) & Tr\,(\text{Block 11}) \end{pmatrix}.$$

This only works if we adopt the convention $A \otimes B = \begin{pmatrix} A_{00}B & A_{01}B \\ A_{10}B & A_{11}B \end{pmatrix}$.

Example

Let $\rho_{AB} = |\psi_{Ab}\rangle \langle \psi_{AB}|$, where $|\psi_{AB}\rangle = |0\rangle_A \otimes |+\rangle_B$. Then

$$\rho_{AB} = \sigma_A \otimes \sigma_B \implies Tr_B(\rho_{AB}) = \sigma_A.$$

Let's compute :

$$|\psi_{AB}\rangle = \begin{pmatrix}1\\0\end{pmatrix}_A \otimes \frac{1}{\sqrt{2}} \begin{pmatrix}1\\1\end{pmatrix}_B$$

$$\rho_{AB} = \begin{pmatrix}1\\1\\0\\0\end{pmatrix} \begin{pmatrix}1 & 1 & 0 & 0\end{pmatrix} \cdot \frac{1}{2}$$

$$= \frac{1}{2} \left(\begin{array}{cc|cc} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

By doing the trace of each block :

$$\rho_A = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} = |0\rangle \langle 0|_A = \begin{pmatrix}1\\0\end{pmatrix} \begin{pmatrix}0 & 0\end{pmatrix}.$$

-

8.5 Entanglement entropy

Entanglement entropy answers the question : "How much entanglement is in this quantum state ?", this is the von Neumann entropy of a reduced density matrix.

We already know a definition of entanglement, but there is another one that use von Neumann entropy.

If you look at the reduced density matrix of a product state $|\phi\rangle_{AB} = |\alpha\rangle_A \otimes |\beta\rangle_B$ then you obtain $\rho_A = |\alpha\rangle \langle \alpha|_A$ which is a pure state $\iff S(\rho_A) = 0$.

So a general state $|\psi\rangle_{AB}$ is entangled $\iff S(\rho_A) \neq 0$.

Théorème 3

If ρ_A and ρ_B come from a pure state, $S(\rho_A) = S(\rho_B)$.

Examples

1. **Product state :**

$$|\psi\rangle = |\alpha\rangle_A \otimes |\phi\rangle_B\,, \quad \rho_A = |\alpha\rangle\langle\alpha|_A\,, \quad \rho_B = |\phi\rangle\langle\phi|_B\,,$$

$$S(\rho_A) = S(\rho_B) \implies \text{theorem is correct.}$$

2. **Bell state :**
this state is famous being "maximally entangled". State on 2 qubits :

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\,, \text{ let's check if the definition hold :}$$

$$\rho_A = Tr_B(|\psi\rangle\langle\psi|) = Tr\left(\frac{1}{2}\begin{pmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{pmatrix}\right) = \frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}.$$

$\implies S(\rho_A) = 1$, this Bell state is entangled, this is a maximally entangled state !

-

Remarque

A unique thing about quantum mechanics is that there existe some ρ_{AB} such that $S(\rho_{AB}) < S(\rho_A)$. For example : $\rho_{AB} = |B_{00}\rangle\langle B_{00}|$.

Théorème 4

The Schmidt decomposition theorem *says that any state* $|\psi\rangle_{AB}$ *can be express as*

$$\sum_i p_i |\phi_A\rangle_i \otimes |\phi_B\rangle_i\,, \quad p_i \geq 0.$$

$\{|\phi_A\rangle_i\}$ *is orthonormal for* A *and* $\{|\phi_B\rangle_i\}$ *is orthonormal for* B*, but they don't need to form a basis.*

Remarque

If $r = 1$, then $|\phi\rangle_{AB}$ is factorizable !

Now, let's prove that : *first definition of entanglement* $\iff$ *second definition of entropy*.

- **Definition 1** $\implies$ **definition 2 :**
If $|\psi\rangle_{AB}$ can be factorized, then $S(\rho_A)$. So by contraposition, definition 1 $\implies$ definition 2.
- **Definition 2** $\implies$ **definition 1 :**
We can reformulize : if $\nexists$ a factorization then $S(\rho) > 0$.
So by the Schmidt theorem, we can assume that : if $\nexists$ a way to write $|AB\rangle_{AB} = |\phi\rangle_A \otimes |\sigma\rangle_B \implies r > 1$. So $|\psi\rangle_{AB} = p_1|\phi_1\rangle_A \otimes |\phi_1\rangle_B + p_2|\phi_2\rangle_A \otimes |\phi_2\rangle_B + \dots$
Then $p_1 > 0,\ p_2 > 0 \implies \rho_A = p_1^2|\phi_1\rangle\langle\phi_1| + p_2|\phi_2\rangle\langle\phi_2| + \dots$ because $\rho_A = \sum_i (\mathbb{1}_A \otimes |\alpha_i\rangle_B)|\psi\rangle\langle\psi|_{AB}(\mathbb{1}_A \otimes |\alpha_i\rangle_B)$ with $\{|\alpha\rangle_i\}\{|\phi_B\rangle_i\}$.
You can get then $\rho_A = \sum_{i=1}^r p_i^2|\phi_i\rangle\langle\phi_i|_A\,,\ \rho_B = \sum_{i=1}^r p_i^2|\phi_i\rangle\langle\phi_i|_B$.
Then $S(\rho_A) = -\sum_i p_i^2 \log(p_i^2) = -p_1^2\log(p_1^2) - p_2^2\log(p_2^2) - \dots > 0$.

9 Quantum error correction

Why do we use quantum error correction ? Classical computers have some errors but quantum computers have much higher rates of errors (noise).

9.1 Classical error correction

One solution is **redundancy** : you encode n bits of information in m bits (m > n).

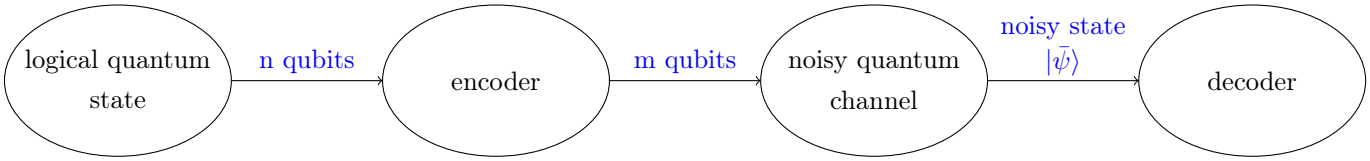
Example

Let's suppose I want to send 1 bit over a noisy channel.
Encoding :

$$1 \to 111$$
$$0 \to 000.$$

Here $n = 1$ and $m = 3$.
Decoding :
Majority vote, $\bar{m} = abc \to$ output, whichevere bit is in the majority.

9.2 Model of quantum communication



9.3 Types of (single-qubit) quantum errors

- **X = bit flip error :**

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle, \quad X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle.$$

- **Z = phase flip error :**

$$Z|0\rangle = |0\rangle, \quad Z|1\rangle = -|1\rangle, \quad Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle.$$

- R_θ **= Phase rotation :**

$$R_\theta = \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

How des quantum error correction differ form classical error correction :

- The no-cloning theorem forbids copying information.
- We can't look at quantum states and figure out which copy is wrong.
- There are infinately many types of quantum errors. For example

$$R_\theta, \quad \theta \sim [0, 2\pi[\quad \to \quad \text{continuous}$$

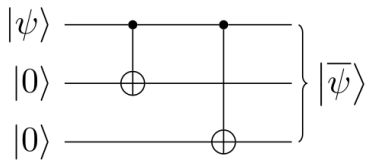
- We have Y errors on top of X and Z errors. Recall :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

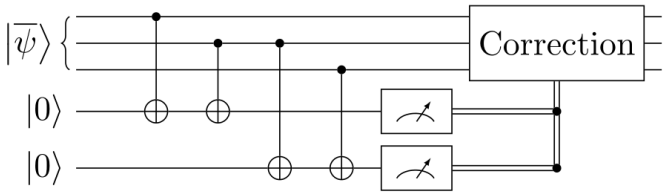
9.4 Detection and correction of bitflip errors

Encoding : Quantum repetition code

$$\begin{aligned} |0\rangle &\rightarrow |000\rangle\,, \\ |1\rangle &\rightarrow |000\rangle\,, \\ |\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle &\rightarrow \alpha\,|000\rangle + \beta\,|111\rangle\,. \end{aligned}$$



Decoding : The idea is to check parity of every neibhouring pair



We assume that there was at most one error.

a	**b**	which qubit had error
0	0	none
0	1	3
1	0	1
1	1	2

But at the end, this QECC is not satisfying, because

- It only handles one error out of 3 possible error locations.
- You use 3 qubits to protect one 1 qubit (inefficient).
- It only works for one type of error (bitflip).

To counter the third point, we will see phaseflip code a 9-qubit Shor code.

9.5 Detection and correction of phaseflip errors

The key fact in phaseflip detection and correction error is that phaseflip is a bitflip in a different basis.

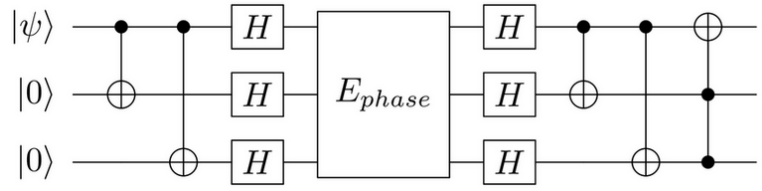
We already seen the effect of Pauli's matrices X and Z on base $\{|0\rangle\,;|1\rangle\}$, now let's see the effect on Hadamard basis $\{|+\rangle\,;|-\rangle\}$:

- $X\,|+\rangle = X\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) = \frac{|1\rangle+|0\rangle}{\sqrt{2}} = |+\rangle$,
- $X\,|-\rangle = X\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) = \frac{|1\rangle-|0\rangle}{\sqrt{2}} = -\,|-\rangle$,
- $Z\,|+\rangle = Z\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) = \frac{|0\rangle-|1\rangle}{\sqrt{2}} = |-\rangle$,
- $Z\,|-\rangle = Z\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) = \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle$,

Phaseflip error is a bitflip error in Hadamard basis !

Let H be the change matrice between $|0\rangle / |1\rangle$ basis and $|+\rangle / |-\rangle$ basis, then

- $H|0\rangle = |+\rangle$,
- $H|1\rangle = |-\rangle$,
- $H|+\rangle = |0\rangle$,
- $H|-\rangle = |1\rangle$,
- $HXH = Z$,
- $HZH = X$.



E_{phase} = phase where phaseflip error occurs.
Explanation : The idea here is to apply bitflip encoding circuit, then change in Hadamard basis before the error phase, change in normal basis and apply bitflip decoding circuit.

But what if we have both bitflip and phaseflip errors at the same time ?

9.6 9-qubit Shor code

9-qubit Shor code is just a code concatenation :
Phaseflip encoding :

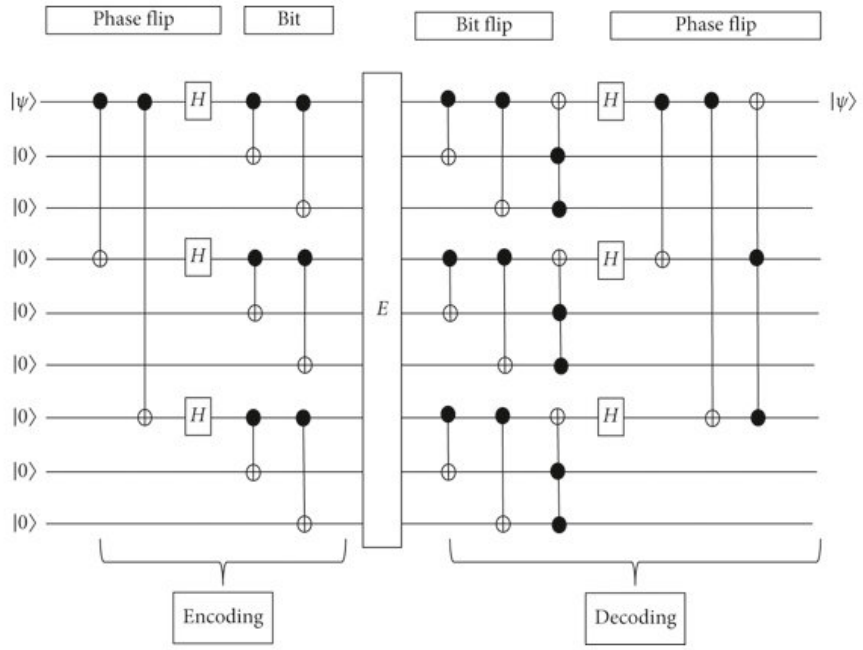
$$|0\rangle \to |+++\rangle\,,$$
$$|1\rangle \to |---\rangle\,.$$

Bitflip encoding :

$$|0\rangle \to |000\rangle\,,$$
$$|1\rangle \to |111\rangle\,.$$

Shor encoding :

$$|0\rangle \to |000\rangle \to |+++\rangle \to \frac{1}{\sqrt{8}}\left(|000\rangle + |111\rangle\right)^{\otimes 3}\,,$$
$$\underbrace{|1\rangle \to |111\rangle \to |---\rangle}_{\text{Phaseflip encoding}} \to \underbrace{\frac{1}{\sqrt{8}}\left(|000\rangle - |111\rangle\right)^{\otimes 3}}_{\text{Bitflip encoding}}\,.$$



Apparté

Something important in QECC, is that quantum errors can be discretized, it means that : **correcting X,Y,Z** errors suffices to correct all quantum errors (though there are infinitely many).

Proof by example of Shor code :
Suppose we had $R_{\theta \text{ error}} = \cos\theta - i\sin\theta Z$, then errored encoded state : $|\tilde{\psi}\rangle = R_\theta |\bar{\psi}\rangle = \cos\theta |\bar{\psi}\rangle - i\sin\theta Z |\bar{\psi}\rangle$.
After applying the Shor code detection circuit :

$$\cos\theta |\bar{\psi}\rangle |I\rangle_{\text{SYN}} - i\sin\theta Z |\bar{\psi}\rangle |Z\rangle_{\text{SYN}} \to \text{meas. syndrome register} \to = \begin{cases} |\bar{\psi}\rangle |I\rangle_{\text{SYN}} & \text{if } = \cos^2 \\ Z |\bar{\psi}\rangle |Z\rangle_{\text{SYN}} & \text{if } = \sin^2 \end{cases}$$

Note : now the syndrome register is entangled with the system registers.

Decoder :
Let

$$|0\rangle \to |+++\rangle \to \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}} \right)^{\otimes 3} = |\bar{0}\rangle ,$$
$$|1\rangle \to |---\rangle \to \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}} \right)^{\otimes 3} = |\bar{1}\rangle .$$

1. Suppose that only one bitlflip happened, then the bitlfip decoder will decode as usual.
2. Suppose that only one phaseflip happened, then errored state is

$$\frac{1}{\sqrt{8}} (|000\rangle + |111\rangle) (|000\rangle - |111\rangle) (|000\rangle - |111\rangle) ,$$

and the U decoder will decode with "parity comparison for signs" between the blocks. It will result as

$$|+\rangle |0\rangle |0\rangle \text{ for the first block, } |-\rangle |0\rangle |0\rangle \text{ for the second and } |-\rangle |0\rangle |0\rangle \text{ for the third.}$$

3. Suppose that both X_1 and Z_1 happened, the errored state is

$$(|100\rangle + |011\rangle) (|000\rangle - |111\rangle) (|000\rangle - |111\rangle) ,$$

- Check for bitflip error →correct the bitflip error : $(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$.
- Check for phaseflip error →correct the phaseflip error.

The Shor code can also decode **some** 2-qubit errors, consider now this 2 qubits errors X_1, X_2. I claim there is no way to correct this error, why ?

It works with $|\bar{0}\rangle$ because : $\underbrace{(|110\rangle + |001\rangle)}_{\text{it will think error is on } X_3} \xrightarrow{\text{after correction}} (|111\rangle + |000\rangle) = (|000\rangle + |111\rangle)$,

but not on $|\bar{1}\rangle$ because : $\underbrace{(|110\rangle - |001\rangle)}_{\text{it will think error is on } X_3} \xrightarrow{\text{after correction}} (|111\rangle - |000\rangle) = -|\bar{1}\rangle = e^{i\phi}$ if $\phi = \pi, |\bar{1}\rangle \equiv |\bar{1}\rangle$,

$$\text{BUT } \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle \neq \alpha|\bar{0}\rangle - \beta|\bar{1}\rangle.$$

9.7 Quantum code distance

Recall :

The classical code distance is the minimum number of bits you need to flip to get from any codeword to any other codeword. Code distance relates to how many bitflip errors a classical code can correct $\Longrightarrow \lfloor \frac{\text{disance } -1}{2} \rfloor$.

Example

$\{000, 111\} \implies$ number of correctable errors $= 1$,

$000 \xrightarrow{2 \text{ errors}} 011$ will be closer to 111.

-

The Pauli weight is the number of positions where the is a non-I Pauli matrice $\sim$ quantum analog of the number of bitlfips.
e.g. $XIX \rightarrow$ weight $= 2$.

If $|\bar{\psi_1}\rangle$, $|\bar{\psi_2}\rangle$ are two encoded statesw in the same code and $\exists$ Pauli P s.t. $|\bar{\psi_1}\rangle = P|\bar{\psi_2}\rangle$, then Pauli P is **uncorrectable** because it looks just like "no error on $|\bar{\psi_1}\rangle$".

$$\text{Quantum code distance } := \text{ min weight}(P) \text{ s.t. } P|\bar{\psi_1}\rangle = |\bar{\psi_2}\rangle,$$
$$P = \text{ some Pauli string, } |\bar{\psi_1}\rangle, |\bar{\psi_2}\rangle \text{ any two orthogonal code.}$$

Analogous to classical code distance, quantum code with distance d can correct Pauli errors of weights at most $\lfloor \frac{d-1}{2} \rfloor$.

Example

- $n = \#$ of physical qubits (n-qubit codeword),
- $k = \#$ of logical qubits (to encode a k-qubit quantum state),
- d : code distance.

$$\mathcal{H}_k \rightarrow \text{ ENC } \rightarrow \mathcal{H}_n,$$

Shor's 9-qubit encode a single qubit into 9 qubit so it's a $\underbrace{[[n, k, d]]}_{9,1,3}$,

that's why it can correct **all** errors of Pauli weight $\lfloor \frac{3-1}{2} \rfloor$.

-

What properties we want of a good QECC :

- make d as large as possible,
- $\frac{k}{n}$ as large as possible,
- fast encoding (decoding).

Let (U, Σ) be a QECC where $U : \mathcal{H}_K \to \mathcal{H}_N$ a map and Σ is a set of correctable errors s.t. $\forall E \in \Sigma, \forall |\psi\rangle \in \mathcal{H}_K$, there is a decoding map that restores the errored state : $D\left(EU |\psi\rangle \langle\psi| U^\dagger E^\dagger\right) \propto |\psi\rangle \langle\psi|$.

Théorème 5

If (U, Σ) is a QECC then $(U, span(\Sigma))$ is also a QECC. Then, to correct arbitrary errors like $\alpha E + \beta F$, it suffices to correct E, F $\implies$ ***quantum errors can be disretized !***