Summary 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

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

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

- **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

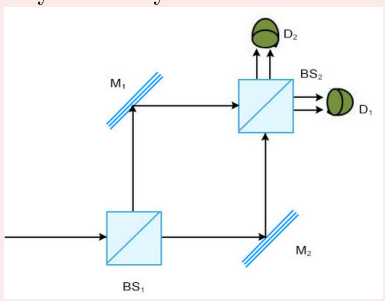
The state of an **isolated** system is a vector $|\phi\rangle \in \mathcal{H}$ in Hilbert space $\mathcal{H}$ w.r.t the normalization condition $\langle\phi|\phi\rangle = 1$.

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 $\left(\mathbb{C}^2\right)$:

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

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

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

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

- 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

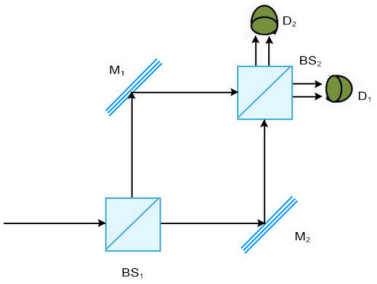
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle).$$

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 $\rightarrow$ prob(decoding correctly)=1.
   - Case 2 : Bob measures in the wrong basis $\rightarrow$ 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 $\widetilde{x}, \widetilde{y}$ 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 $\Longrightarrow$ 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.