

# Informatique quantique

*Basé sur le cours de Sébastien DESIGNOLLE  
Notes prises par Hugo SALOU*



*11 septembre 2025*

# Table des matières

<b>1</b>	<b>Introduction.</b>	<b>4</b>
1.1	Calculabilité. . . . .	4
1.1.1	Objectifs de ce cours. . . . .	4
<b>2</b>	<b>Modélisation d'un système quantique.</b>	<b>5</b>
2.1	Bit probabiliste. . . . .	5
2.2	Bit quantique. . . . .	6
2.3	Plusieurs qubits. . . . .	7
2.4	Notation de Dirac. . . . .	8

Le cours aura lieu de 8h à 10h (sauf pour quelques exceptions, indiquées sur le *pad*). Les TDs seront le vendredi de 10h15 à 12h15. Il y aura des devoirs, un partiel le 6/11 et un examen le 15/12.

# 1 Introduction.

## 1.1 Calculabilité.

Un ordinateur manipule des *bits* (0 ou 1) via des *opérations* (des programmes). Un résultat (c'est plus une hypothèse) est la thèse de Church-Turing étendue :

Tout calcul réaliste peut être efficacement simulée par une machine de Turing.

L'intuition est que les systèmes physiques sont simulables en temps polynomial. Le contre-exemple est la physique quantique.

### 1.1.1 Objectifs de ce cours.

Ce qui est dans ce cours sera :

- ▷ les bases du formalisme quantique ;
- ▷ le calcul algorithmes principaux ;
- ▷ la communication avec les protocoles principaux,

mais il ne sera pas :

- ▷ un cours de physique ;
- ▷ un cours sur les avancées récentes.

# 2 Modélisation d'un système quantique.

## 2.1 Bit probabiliste.

On considère un système physique  $X$  avec des niveaux distinguables<sup>1</sup> dans  $\Sigma = \{0, 1\}$ . L'état de connaissance de ce système est un vecteur

$$v = \begin{pmatrix} a \\ b \end{pmatrix},$$

où  $a$  représente la probabilité que l'on ait un 0, et  $b$  la probabilité que l'on ait un 1. Ceci implique que l'on ait  $a, b \in \mathbb{R}^+$  et  $a + b = 1$ .

On peut considérer des *transformations du système*  $X$ , passant d'un état à un autre :

- ▷  $\text{INIT}_0 : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  qui initialise à l'état 0 ;
- ▷  $\text{INIT}_1 : \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix}$  qui initialise à l'état 1 ;
- ▷  $\text{NOT} : \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  qui inverse l'état.

On demande que ces opérations soient *linéaires* :

$$\text{NOT} \begin{pmatrix} a \\ b \end{pmatrix} = a \text{NOT} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \text{NOT} \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

---

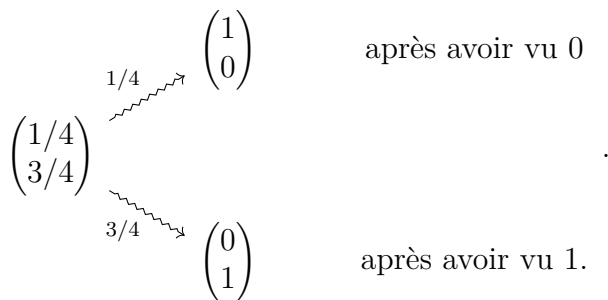
1. On peut distinguer de l'état physique deux états : un état 0 (par exemple, pas de courant), et un état 1 (par exemple, avoir du courant)

On peut représenter une telle opération par une matrice stochastique : c'est une matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

telle que  $a, b, c, d \geq 0$  et  $a + c = b + d = 1$ . Ainsi,  $\text{INIT}_0$  et  $\text{INIT}_1$  ne sont pas des transformations valides.

Lorsqu'on « observe » le système  $X$ , on change l'état de nos connaissances :



## 2.2 Bit quantique.

On considère un système physique  $X$  avec des niveaux distinguables dans  $\Sigma = \{0, 1\}$ . L'état de connaissance de ce système est un vecteur

$$v = \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

où  $\alpha, \beta \in \mathbb{C}$  sont les *amplitudes* et vérifient  $|\alpha|^2 + |\beta|^2 = 1$ .

Les transformations de  $X$  sont des opérations linéaires en  $v$  et préservent la norme, représentations les matrices *unitaires*, c'est-à-dire des matrices  $U^\dagger U = \mathbf{1}$ ,<sup>2</sup> qui généralise les matrices orthogonales pour les matrices complexes. Quelques exemples de matrices unitaires sont :

▷ la matrice identité  $\mathbf{1}_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  ;

---

2. L'opération  $-\dagger$  est la *transconjugaison* qui correspond à la transposée de la conjugaison composante par composante.

- ▷ la matrice **NOT**  $:= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ;
- ▷ la matrice de Hadamard  $\mathbf{H} := \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$ ;
- ▷ la matrice  $\mathbf{Y} := \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$ ;
- ▷ la matrice de rotation  $\mathbf{R}_\theta := \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ ;
- ▷ mais les matrices des opérations  $\text{INIT}_i$  ne sont pas unitaires.

Lorsqu'on « observe » le système  $X$  (que l'on appellera une *mesure*), on change l'état de nos connaissances :

$$\begin{array}{ccc}
 \frac{1}{2} = \left| -\frac{1}{\sqrt{2}} \right|^2 & \xrightarrow{\text{~~~~~}} & \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \text{après avoir vu 0} \\
 \begin{pmatrix} -1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} & & & \\
 \frac{1}{2} = \left| \frac{1}{\sqrt{2}} \right|^2 & \xrightarrow{\text{~~~~~}} & \begin{pmatrix} 0 \\ 1 \end{pmatrix} & \text{après avoir vu 1.}
 \end{array}$$

## 2.3 Plusieurs qubits.

On considère deux systèmes  $X_1, X_2$  avec 4 niveaux  $\Sigma = \{00, 01, 10, 11\}$ . On peut distinguer un vecteur probabiliste « classique » et un état quantique :

$$\begin{pmatrix} 1/8 \\ 1/2 \\ 0 \\ 3/8 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ -1/2 \\ 1/2 \end{pmatrix}.$$

Un système à  $n$  qubits sera représenté par un espace à  $2^n$  dimensions.

L'opération importante est le *produit tensoriel*. Si l'on a deux matrices  $A \in \mathbb{C}^{k \times \ell}$  et  $B \in \mathbb{C}^{m \times n}$  alors on a une matrice  $A \otimes B \in \mathbb{C}^{km \times \ell n}$ .

**Définition 2.1 (Construction du produit tensoriel).** Si on a :

- ▷ un espace vectoriel  $V$  avec une base  $\{e_1, \dots, e_n\}$  ;
- ▷ un espace vectoriel  $V'$  avec une base  $\{e'_1, \dots, e'_m\}$  ;

alors l'espace vectoriel  $V \otimes V'$  a pour base

$$\{e_i \otimes e'_j \mid i \in \llbracket 1, n \rrbracket \text{ et } j \in \llbracket 1, m \rrbracket\}.$$

Ainsi,

$$V \otimes V' = \text{vect}\{v \otimes v' \mid v \in V \text{ et } v' \in V'\}.$$

On a quelques propriétés sur le produit tensoriel.

**Proposition 2.1.** On a :

- ▷  $\lambda \otimes A = \lambda A$  où l'on identifie  $\mathbb{C}^{1 \times 1}$  et  $\mathbb{C}$  ;
- ▷  $(A \otimes B) \otimes C = A \otimes (B \otimes C)$  ;
- ▷  $(A \otimes B)(C \otimes D) = AC \otimes BD$  ;
- ▷  $A \otimes (B + C) = A \otimes B + A \otimes C$ .

On suppose ici que les matrices respectent les bonnes conditions de dimension pour que ces opérations aient du sens.  $\square$

**Attention !** En général, on a  $A \otimes B \neq B \otimes A$ .

## 2.4 Notation de Dirac.

On adopte les notations suivantes :

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

que l'on appelle *ket*  $|-\rangle$ . Cette notation est linéaire dans le sens où l'on a

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha |0\rangle + \beta |1\rangle.$$



L'écriture des produits tensoriels est plus simple  $|0\rangle \otimes |0\rangle = |00\rangle$ .  
L'avantage est que l'on peut écrire

$$\frac{1}{\sqrt{2}}|0000\rangle + \frac{1}{\sqrt{2}}|1111\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ \vdots \\ 0 \\ 1/\sqrt{2} \end{pmatrix}.$$

On a la notion de *dualité* :  $|\psi\rangle \leftrightarrow \langle\psi| = (|\psi\rangle)^\dagger$ .

Avec  $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$  et  $|\varphi\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$ , on peut définir des notations sympathiques :

$$\langle\varphi|\psi\rangle = \begin{pmatrix} \bar{\gamma} & \bar{\delta} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\bar{\gamma} + \beta\bar{\delta} = \langle\varphi|\psi\rangle.$$

On peut aussi définir  $|- \rangle \langle -|$ . On peut ainsi interpréter  $|\psi\rangle \langle\psi|$  comme la projection sur vect  $|\psi\rangle$ .