Calcul Quantique et Algorithmes

- Introduction au calcul quantique du point de vue *théorique* !
- Comparaison avec le calcul classique
- *Bonus* : notation graphique pour les tenseurs

Partie 2 : factorisation des entiers,
transformée de Fourier quantique, ...

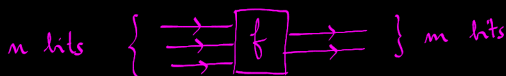
I) Calcul classique

- Bit : 0 <u>ou</u> 1 $\longrightarrow$ "circuit électrique"

- n bits $\longleftrightarrow$ $\{0,1\}^n$ $\longleftrightarrow$ nombres entiers entre 0 et $2^n - 1$

  2 bits : 00, 01, 10, 11

- Porte logique : $f : \{0,1\}^n \longrightarrow \{0,1\}^m$



<u>Exemple</u> :

$n = m = 1$

$i \longrightarrow \boxed{\text{Not}} \longrightarrow j$

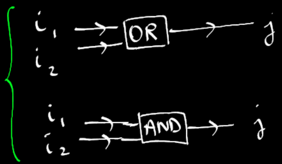
i	j
0	1
1	0

$i \longrightarrow j$

i	j
0	0
1	1

$n = 2$

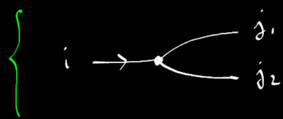
$m = 1$



i_1	i_2	OR	AND	XOR
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

$n = 1$

$m = 2$



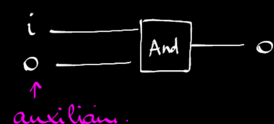
i	j_1	j_2
0	0	0
1	1	1

Théorème.

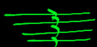
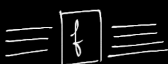
> Toute fonction $\{0,1\}^n \longrightarrow \{0,1\}^m$ peut être construite avec les portes , AND, XOR et NOT ainsi que des bits auxiliaires préparés dans des états spécifiques

Exemple : $f : \{0,1\} \longrightarrow \{0,1\}$

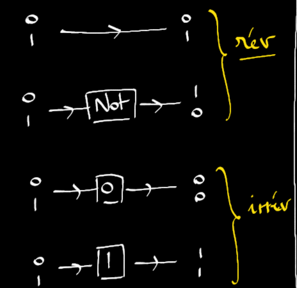
$x \longmapsto 0$



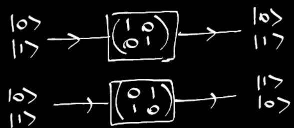
II) Calcul Quantique

Bit $\in \{0,1\}$	Qubit : $\lvert\psi\rangle = a\lvert 0\rangle + b\lvert 1\rangle$ avec $\lvert a\rvert^2 + \lvert b\rvert^2 = 1$
$\longrightarrow$	$\longrightarrow$ $\quad \lvert\psi\rangle \in \mathcal{H} = \mathrm{Vect}_{\mathbb{C}}(\lvert 0\rangle, \lvert 1\rangle)$
n-bits $\in \{0,1\}^n$	n-qubits : élément de $\underbrace{\mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{n \text{ facteurs}} = \mathrm{Vect}_{\mathbb{C}}\begin{pmatrix} \lvert 00\ldots 0\rangle \\ \lvert 00\ldots 1\rangle \\ \vdots \\ \lvert 11\ldots 1\rangle \end{pmatrix}$
	
Porte	Porte quantique : $n\left\{ \equiv \boxed{U} \equiv \right\}n$
	avec $U : \mathcal{H}^{\otimes n} \longrightarrow \mathcal{H}^{\otimes n}$ $\quad \nearrow$ Réversible
$\{0,1\}^n \longrightarrow \{0,1\}^m$	opérateur $\boxed{\text{unitaire}}$ $\quad UU^\dagger = U^\dagger U = \mathbb{1}$.
	linéaire

Portes $n = m = 1$.



Portes $n = 1$ $\quad \mathcal{H} \xrightarrow{U} \mathcal{H}$ $\quad U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$

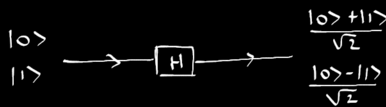


4 paramètres réels.

Porte de Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Impossible d'effectuer des opérations non réversibles !

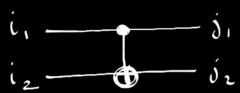


Portes à $n = 2$.

i_1 i_2	j_2
0 0	0
0 1	1
1 0	1
1 1	0

Porte $\boxed{\text{CNOT}}$

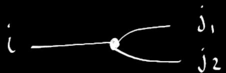
"Control-NOT"



$i_1 i_2$	$j_1 j_2$
0 0	0 0
0 1	0 1
1 0	1 1
1 1	1 0

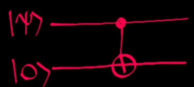
Matrice dans $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



i	j_1	j_2
0	0	0
1	1	1

"Pas de clonage en mécanique quantique"



$|0\rangle$ $|1\rangle$

$|0\rangle$ $|1\rangle$

$\uparrow$ si $|\psi\rangle = |0\rangle$ $\quad\uparrow$ si $|\psi\rangle = |1\rangle$

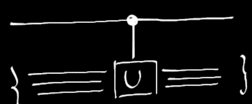
ne fonctionne pas !

Si $|\psi\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$ alors l'état final est : $\dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$

$\neq$

$|\psi\rangle|\psi\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$

Si Condition, faire f.



Control - U

III) Notation tensorielle

<u>Idée</u> : faire de l'algèbre linéaire avec des dessins.

- <u>Application linéaire</u>.

$$
\begin{array}{ccc}
M : \mathbb{R}^n & \longrightarrow & \mathbb{R}^m \\
\uparrow & & \uparrow \\
\text{base } (e_1, \dots, e_n) & & \text{base } (f_1, \dots, f_m)
\end{array}
$$

$$u \in \mathbb{R}^n, \quad M(u) = M(u^i e_i) = M(e_i)\, u^i = f_j \underbrace{M^j{}_i}_{\text{coefficient de } M(e_i) \text{ sur } f_j} u^i$$

coefficient de $M(e_i)$ sur f_j

$$\boxed{M(u)^j = M^j{}_i\, u^i}$$

$$i \longrightarrow \boxed{M} \longrightarrow j$$

Produit de matrices = composition d'applications linéaires

$$(MN)^k{}_i = M^k{}_j\, N^j{}_i \qquad\qquad i \longrightarrow \boxed{N} \xrightarrow{\;j\;} \boxed{M} \longrightarrow k$$

• <u>Vecteurs</u> : $v \in \mathbb{R}^n$ $\quad v = v^i e_i$ $\quad \boxed{v} \longrightarrow i$

<u>Covecteur</u> = forme linéaire = $\mathbb{R}^n \longrightarrow \mathbb{R}$. $\quad i \longrightarrow \boxed{\lambda}$

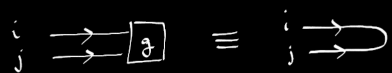
$$\lambda = \lambda_i (e^*)^i$$

$$\lambda(v) = \boxed{v} \longrightarrow \boxed{\lambda}$$

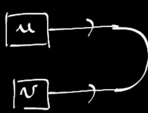
• <u>Tenseurs</u> . $T : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}^n$

$$T^k{}_{ij}$$

<u>Exemple</u> : métrique g_{ij}



Produit scalaire de deux vecteurs

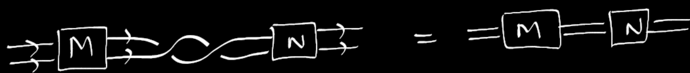


← besoin de la métrique g_{ij}

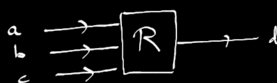
trace d'une application linéaire :

$M^i{}_i$

Remarques. Les fils ne peuvent pas se tresser :



Exemples. Géométrie riemannienne, tenseur $R^{d}{}_{abc}$:



Tenseur de Ricci :

Scalaire de Ricci :

IV) Calcul sur 1 qubit

$U = \begin{pmatrix} \vdots & \vdots \end{pmatrix}$ unitaire.

Exemples :

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ analogue quantique de NOT

$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\quad |0\rangle \to |0\rangle$, $\quad |1\rangle \to -|1\rangle$

$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ création d'états "superposés" $\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$

$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$ $\qquad R_3 = T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = $ "$\frac{\pi}{8}$"

$\vdots$

L'ensemble des opérations unitaires forme le groupe de Lie $U(2)$ qui est infini, non dénombrable.

Théorème.

Toute $U \in U(2)$ peut être approximée avec une précision arbitraire avec seulement H et R_3

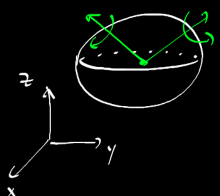
Preuve (idée)

- On mesure l'erreur avec $E(U,V) = \max_{\substack{|\psi\rangle \\ \langle\psi|\psi\rangle=1}} \left| (U-V)\,|\psi\rangle \right|$.

  Si $E(U,V)$ est petit, alors V approxime bien U.

- Géométriquement, R_3 = rotation d'angle $\pi/4$ autour de z

  HR_3H = ______________________ x.



Combine les deux : rotation autour de $\vec{n}\left(\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8}\right)$ d'angle θ tel que $\cos(\theta/2) = \cos^2(\pi/8)$.

Lemme : $\frac{\theta}{\pi} \notin \mathbb{Q}$.

On peut donc construire une approximation de $\boxed{R_{\vec{n}}(\alpha)}$ pour tout α, arbitrairement bonne.

$$R_{\vec{m}}(\alpha) = H \, R_{\vec{n}}(\alpha) \, H \quad \text{avec} \quad \vec{m} = \left(\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8}\right)$$

<u>Lemme</u>. On peut écrire toute $U \in U(2)$ sous la forme

$$U = e^{i\alpha} R_{\vec{n}}(\beta) \, R_{\vec{m}}(\gamma) \, R_{\vec{n}}(\delta) \quad \text{avec} \quad \alpha, \beta, \gamma, \delta \in \mathbb{R}.$$

V) Calcul Quantique universel

But : montrer qu'il suffit d'exhiber un opérateur unitaire pour dire qu'il existe un algorithme quantique réalisable avec quelques portes de base.

↳ Transformée de Fourier quantique ⇝ Algorithme de Shor pour la factorisation.

Théorème.

$$\boxed{\text{Toute } U : \mathcal{H}^{\otimes n} \longrightarrow \mathcal{H}^{\otimes n} \text{ unitaire peut être exprimée de façon \underline{exacte} à l'aide de CNOT et de portes à 1 qubit et de \underline{qubits auxiliaires}}}$$

Preuve (idée).

① Une matrice unitaire $D \times D$ peut s'écrire comme produit de matrices de la forme :

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & a & \cdots & b & \\ & & & \vdots & 1 \ddots 1 & \vdots & \\ & & & c & \cdots & d & \\ & & & & & & 1 \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{pmatrix} \begin{array}{l} \\ \\ \\ 01001 \\ \\ 11101 \\ \\ \\ \\ \end{array} = M .$$

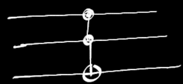
← il suffit de savoir faire cela.

Preuve par récurrence sur D.

② Soit $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $\tilde{M} = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & U \end{pmatrix} \begin{array}{l} \\ \\ \\ 11\ldots10 \\ 11\ldots11 \end{array}$. Il existe des combinaisons de portes X et CNOT telles que

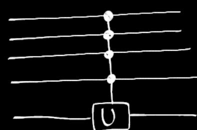
$$\boxed{M} = (X, \mathrm{Cnot}) \; \boxed{\tilde{M}} \; (X, \mathrm{Cnot})$$

③ On peut construire à l'aide de CNOT et R_3 une porte de "Toffoli" :

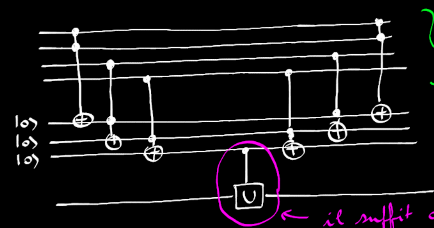


(admis) (pas besoin d'auxiliaires)

$\tilde{M}$ =



=

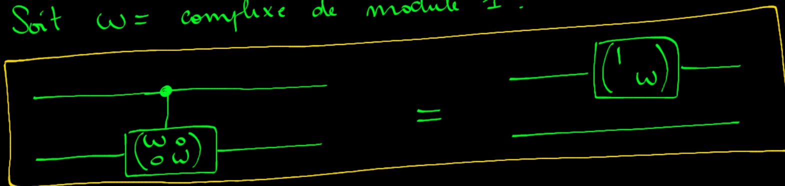


!!

← il suffit de faire ça

<u>Remarque</u> : Parfois, la mécanique quantique est contre-intuitive !

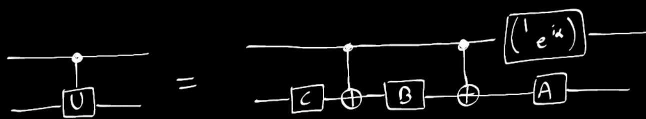
Soit ω = complexe de module 1.



$$|0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle = |0\rangle|0\rangle$$
$$|0\rangle|1\rangle \longrightarrow |0\rangle|1\rangle = |0\rangle|1\rangle$$
$$|1\rangle|0\rangle \longrightarrow |1\rangle\,\omega|0\rangle = \omega|1\rangle|0\rangle$$
$$|1\rangle|1\rangle \longrightarrow |1\rangle\,\omega|1\rangle = \omega|1\rangle|1\rangle$$

(4) **Lemme :** Tout $U \in U(2)$ peut se décomposer en $U = e^{i\alpha} AXBXC$ avec $\alpha \in \mathbb{R}$, $A, B, C \in U(2)$, et $ABC = id$.

Alors on a :



$$|0\rangle|\psi\rangle \longrightarrow |0\rangle|\psi\rangle$$
$$|1\rangle|\psi\rangle \longrightarrow e^{i\alpha}|1\rangle\, AXBXC|\psi\rangle = |1\rangle\, U|\psi\rangle.$$

A suivre : QFT, Shor...

Comment exploiter un algo quantique

Comment faire des mesures ?