PLAN C.I. 4 - INTRICATION QUANTIQUE

- Rappels : produit tensoriel de qubits ; portes quantiques à 1 qubit et 2 qubits
- États à 2 qubits, états intriquées (enchevêtrés)
- Application - la téléportation quantique
- Théorème de non-clonage quantique
- Calcul quantique, quelques généralités

rappels:

Produit tensoriel et qubits

Représentation matricielle des qubits:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$

$$|\psi\rangle \longrightarrow \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

cas particuliers:

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

produit tensoriel de matrices:

$$A \otimes B := \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mm}B \end{pmatrix}$$

produit tensoriel de qubits

Exo.: Calculer les produits tensoriels des états $|0\rangle$ et $|1\rangle$.

$$|00\rangle \equiv |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|01\rangle \equiv |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle \equiv |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle \equiv |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

} états produit

Remarque: On peut factoriser des états produit d'autres

Rappels : portes quantiques

Portes quantiques : famille continue de transformations
- toute **matrice unitaire** est susceptible de représenter une porte logique à 1 qubit.

Exemples

- la porte X (opérateur NOT)

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathcal{M}_{2,2}(\mathbb{C})$$

$\Rightarrow X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$

- la porte Y

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

$\Rightarrow Y|0\rangle = i|1\rangle$, $Y|1\rangle = -i|0\rangle$

- la porte Z (opérateur de flip)

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$\Rightarrow Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$

- la porte ϕ

$$R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

$\Rightarrow R_\phi|0\rangle = |0\rangle$, $R_\phi|1\rangle = e^{i\phi}|1\rangle$

Remarque : $Z = R_\pi$ (car $e^{i\pi} = -1$)

- la porte de Hadamard

$$H = \frac{1}{\sqrt{2}}(X+Z) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$\Rightarrow H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$H\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = |0\rangle$ (effet analogue à l'interférence d'ondes)

porte à 2 qubit

porte CNOT

E	S
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

L'INTRICATION QUANTIQUE

caractère subtile et paradoxal de la méca q. (1964)
- paradoxe EPR (inégalités de Bell (1935) expériences d'Aspect ('82))

États à 2 qubits

ts qubit A : $|0_A\rangle$ et $|1_A\rangle$
— qubit B : $|0_B\rangle$ et $|1_B\rangle$
états du système AB : $\underbrace{|0_A\rangle|0_B\rangle, |0_A\rangle|1_B\rangle, |1_A 0_B\rangle, |1_A 1_B\rangle}_{\text{base}}$.

chaque qubit se trouve dans un état de superposition :

qubit A : $|\psi_A\rangle = \alpha|0_A\rangle + \beta|1_A\rangle$
— B : $|\psi_B\rangle = \gamma|0_B\rangle + \delta|1_B\rangle$

système AB : $|\psi_A\rangle|\psi_B\rangle = \alpha\gamma|0_A\rangle|0_B\rangle + \alpha\delta|0_A\rangle|1_B\rangle +$
$+ \beta\gamma|1_A\rangle|0_B\rangle + \beta\delta|1_A\rangle|1_B\rangle$ (1)

notation : les états $|0_A 0_B\rangle \equiv |00\rangle$, $|0_A 1_B\rangle \equiv |01\rangle$, $|1_A 0_B\rangle \equiv |10\rangle$, $|1_A 1_B\rangle \equiv |11\rangle$

La mécanique quantique nous dit (1er postulat)
ue tout état à 2 qubits se décompose :

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle, \quad (2)$$

avec $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 = \sum_{ij=0}^{1} |\alpha_{ij}|^2$.

l'état $|\psi_A\rangle|\psi_B\rangle$ de l'éq. (1) est un état factorisé

$$(|\psi_A\rangle|\psi_B\rangle = |\psi_A\rangle \otimes |\psi_B\rangle)$$

Il existe des états qui ne se factorisent pas
u un produit d'états à 1 qubit — états intriqués
(ou états enchevêtrés) (anglais : entangled states)
états spécifiques de la description quantique ;
ls engendrent entre les particules des corrélations fortes
qui sont à la base des différents protocoles et
algo de l'info quantique.
important : dans ces états, l'état individuel d'un qubit
n'est pas défini — c'est le système qui est dans un
état défini (qui évolue avec le temps

x. d'état intriqué - le 1er état de Bell :

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Tant qu'aucune mesure n'est effectué sur le système, l'état de chaque qubit n'est pas défini.

Si nous mesurions le 1er qubit et nous trouvons l'état $|0\rangle$, alors l'état $|\beta_{00}\rangle$ est projeté sur l'état $|00\rangle$, ce qui entraîne que le 2ème qubit est forcement lui aussi dans l'état $|0\rangle$.

État de Bell $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

On suppose qu'il existe α_i, β_i, $i=0,1$. t.q.

$$|\beta_{00}\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle)(\beta_0|0\rangle + \beta_1|1\rangle) \Leftrightarrow$$

$$\Leftrightarrow \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$$

$$\Rightarrow \alpha_0\beta_0 = \frac{1}{\sqrt{2}} = \alpha_1\beta_1 \Rightarrow \alpha_0, \beta_0, \alpha_1, \beta_1 \neq 0 \;/\Rightarrow$$

$$\alpha_0\beta_1 = 0 = \alpha_1\beta_0$$

$\Rightarrow$ contradiction $\Rightarrow$

$\Rightarrow$ l'état de Bell ne se factorise pas !

(———) ——— est un état intriqué)

Mesure d'un état à 2 qubits

D'après la méca. Q. (d'après le postulat de la mésure), si on mesure l'état de 2 qubits, le système est projeté dans l'un des états de base

$|00\rangle, |01\rangle, |10\rangle$ ou $|11\rangle$

avec une probabilité $|\alpha_{ij}|^2$.

Mesure partielle : on mesure uniquement un des 2 qubits

La mesure va fixer l'état du qubit mesuré — l'état du système sera une superposition des états de base compatibles, et dans laquelle le qubit mesuré aura une valeur fixée

Ex.: Si on mesure le 1er qubit du système de l'état (2) et on trouve $|0\rangle$, le système est projeté ds. l'état:

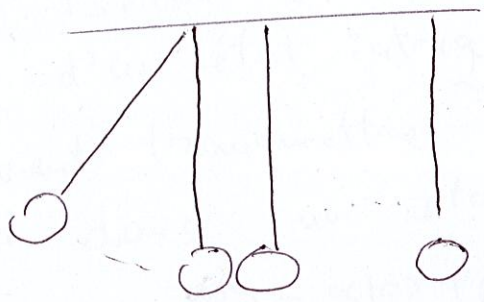
$$|\tilde{\psi}\rangle = \frac{\alpha_{00}}{\sqrt{|\alpha_{00}|^2+|\alpha_{01}|^2}}|00\rangle + \frac{\alpha_{01}}{\sqrt{|\alpha_{00}|^2+|\alpha_{01}|^2}}|01\rangle.$$

Rq.: $\dfrac{|\alpha_{00}|^2}{(|\alpha_{00}|^2+|\alpha_{01}|^2)} + \dfrac{|\alpha_{01}|^2}{|\alpha_{00}|^2+|\alpha_{01}|^2} = 1.$ ✓

Téléportation quantique

téléportation d'état quantique, pas
le —— " —— de système physique porteur de l'état !

analogie :



ici, c'est la quantité de mouvement (l'impulsion) qui se téléporte, pas la bille
(pas de transport de matière !)

Pour réaliser la téléportation quantique, il faut une paire de particules intriquées.

Rq : L'état initial, qui est téléporté, est détruit !
cela est une différence avec le clonage quantique.

Illustration : comment transmettre d'un point A (Anne) à un point B (Benoît) le contenu inconnu d'un qubit (i.e. un état quantique)?
(le système physique porteur du qubit n'est pas transporté !)

- Anne et Benoit se sont offert antérieurement un des 2 qubits d'un état intriqué de Bell $|\beta_{00}\rangle$
- Anne veut transmettre à Benoît le contenu d'un qubit dans un état

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

que Anne ne connait pas.

- système à 3 qubits:

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle) =$$

$$= \frac{1}{\sqrt{2}}(\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle)$$

ordre de qubits:
1. A - le qubit inconnu
2. B - le 1er qubit de la paire intriquée (obtenu par Anne)
3. C - le 2nd ——— , ——— (——— , ——— Benoît)

Anne réalise les opérations suivantes:

1.) elle réalise un CNOT sur la paire (A,B);
— o — obtient:

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha(|000\rangle + |011\rangle) + \beta(|110\rangle + |101\rangle)\right]$$

2.) — o — envoie le 1er qubit sur une porte de Hadamard; l'état du système devient:

$$|\Psi_2\rangle = \frac{1}{2}\left[\alpha(|000\rangle + |100\rangle + |011\rangle + |111\rangle) + \beta(|010\rangle - |110\rangle + |001\rangle - |101\rangle)\right] =$$

$$= \frac{1}{2}\left(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\right)$$

} Exo.

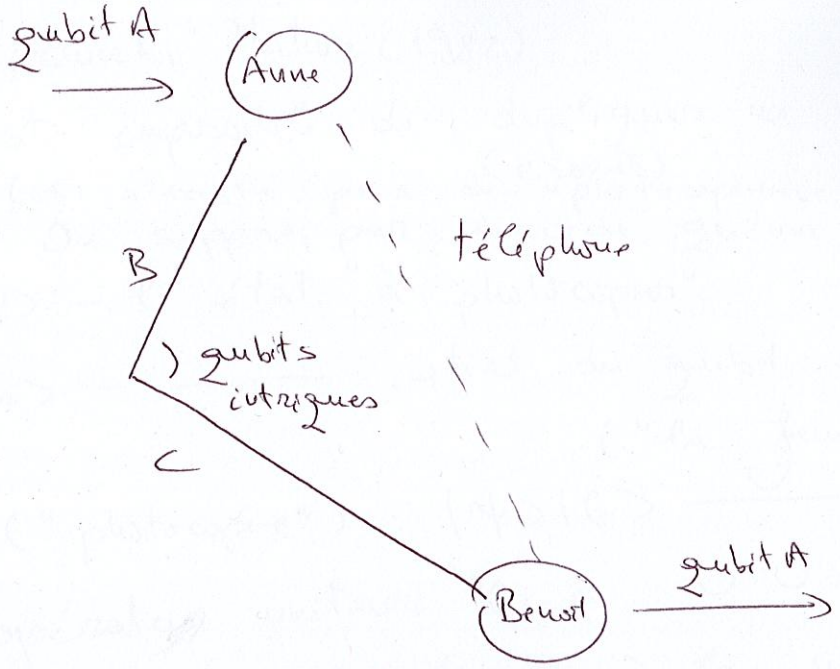
Téléportation: l'état du qubit C est complètement déterminé par celui de la paire (A,B), determiné par Anne — effet de la corrélation quantique due à l'intrication de la paire (BC)

3.) mesure de Bell
Anne fait (mesure) la paire (A,B) et transmet le résultat à Benoit par téléphone (info classique)
— la téléportation ne viole pas la relativité restreinte d'Einstein (aucune info ne peut être transmise plus vite que la lumière)!

4.) Benoît reçoit ~~$b_1 b_2$~~ le résultat d'Anne; Benoît réalise sur son qubit C l'opération

$$Z^{b_1} X^{b_2}$$

On peut vérifier que l'état résultant du qubit C est l'état $|\Psi\rangle$! (Exo.)



réalisation expérimentale :

1997 : équipe d'Anton Zeilinger (Autriche) (téléportation quantique états photons)

Théorème de non-clonage quantique

(Wooters, Zurek, Nature (1982)

Il est impossible de dupliquer un état quantique.
(cloner)

Preuve: (i.e. n'existe pas de "photocopieuse" quantique)

On suppose, par absurde, qu'une telle "machine" existe

Soit $|\psi\rangle$ – l'état "à photocopier"

$|b\rangle$ – — , — initial du qubit de copie
("la feuille blanche")

clonage ("photocopie"): $|\psi\rangle|G\rangle \xrightarrow{U} |\psi\rangle|\psi\rangle$

U – opérateur unitaire (i.e. $U^+U = UU^+ = Id$) (système à 2 qubits)

Rq.: U est "caractéristique à la machine"
(i.e.: il ne dépend pas de l'état à cloner)

$|\psi\rangle|\psi\rangle = U|\psi\rangle|G\rangle$

$|\phi\rangle$ – autre état à cloner, $|\phi\rangle \neq |\psi\rangle$

$\Rightarrow |\phi\rangle|\phi\rangle = U|\phi\rangle|G\rangle \Rightarrow \langle\phi|\langle\phi| = \langle G|\langle\phi|U^+$

$\Rightarrow \langle\phi|\langle\phi|\psi\rangle|\psi\rangle = \langle G|\langle\phi|U^+U|\psi\rangle|G\rangle$

$(\langle\phi|\psi\rangle)^2 = \langle G|G\rangle\langle\phi|\psi\rangle$ (car $U^+U = Id$) $\Rightarrow$

mais $\langle G|G\rangle = 1$ (notation de Dirac)

$\Rightarrow (\langle\phi|\psi\rangle)^2 = \langle\phi|\psi\rangle$, $\forall |\phi\rangle, |\psi\rangle$

$\Rightarrow$ i) $\langle\phi|\psi\rangle = 1$, $\forall |\phi\rangle, |\psi\rangle$ $\Rightarrow$ contradiction

ii) $\langle\phi|\psi\rangle = 0$, $\forall |\phi\rangle, |\psi\rangle$ (états orthogonaux)

$\Rightarrow$ contradiction $\Rightarrow$

$\Rightarrow \nexists$ de "photocopieuse quantique"
(c'est impossible de cloner un état quantique)

Remarque : On peut fabriquer une machine qui copie seulement les états de base $|ij\rangle$ $(i,j = 0,1)$, qui sont orthogonaux — l'analogue de la poste copie. Cette machine ne pourra pas copier / cloner les états de superposition.

Manipulations d'états à 2 qubits - Calcul quantique

Les opérateurs sur 1 (ou plusieurs) qubits correspondent à l'action d'opérateurs unitaires - évolutions réversibles

(différence fondamentale avec les ordi classiques - évolutions irréversibles)

Théorème de logique classique: toute porte logique peut être construite à partir de NAND et COPY

NAND est irreversible.

NAND et COPY ne peuvent pas être transposé ds. le Q. (à cause de l'irreversibilité et resp.

——, —— thm. de non-clonage quantique

Cependant, il est possible de transformer les algo. classiques irreversibles en

—n— réversibles.

coût: - augmentation du volume d'information traitée
- introduction d'une nouvelle porte à 3 bits, TOF (porte de Toffoli)

$(x, y, z) \rightarrow (x, y, z \oplus xy)$

SWAP : $(x, y) \rightarrow (y, x)$

$f : \mathbb{B}^n \to \mathbb{B}^n$ est calculable "avec variables auxiliaires" sur l'ensemble de portes (réversibles) $\mathcal{G}$ ssi $\exists$ un circuit C à $(n+m)$ entrées t.q.

$$C(\vec{x}, 0^m) = (f(\vec{x}), 0^m)$$

i.e. le circuit C se sert des m dernières places pour calculer, mais ne prend aucune donnée, ni ne retourne aucun résultat, dans ces m places ("places auxiliaires").

$$f_{\oplus}(\vec{x}, y) := (\vec{x}, y \oplus f(\vec{x})).$$

On peut montrer que tout circuit irréversible calculant une fonction f peut être transformé en circuit réversible, avec variable auxiliaires, calculant $f_{\oplus}$.

À travers cette équivalence, on pourra associer un algo quantique (réversible) à tout — classique (irréversible).

Théorème de Bennet – Landauer – Toffoli :

Soit $n \geq 2$. Toute application booléenne inversible

$$f : \mathbb{B}^n \longrightarrow \mathbb{B}^n$$

est calculable par un circuit (avec var. auxiliaires) sur l'ensemble de portes $\{NOT, SWAP, TOFF\}$.

La porte NOT peut être remplacée par

— ⊕ — cNOT (NON contrôlé – controlled NOT) :

entrée	sortie
0 0	0 0
0 1	0 1
1 0	1 1
1 1	1 0

1er bit – bit de contrôle : valeur inchangée

2ème bit – bit cible : sa valeur est inchangée si le bit de contrôle vaut 0, et il est inversé si

—●— , —⊕— 1 :

$$(x, y) \longrightarrow (x, x \oplus y)$$

CNOT quantique : est représentée par une matrice ds. la base $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ ou par un circuit quantique

$$\Lambda(U)|x_1,\dots,x_n\rangle := \begin{cases} |x_1\rangle \otimes |x_2,\dots,x_{n+1}\rangle & \text{si } |x_1\rangle = |0\rangle \\ |x_1\rangle \otimes U|x_2,\dots,x_{n+1}\rangle, & \text{si } |x_1\rangle = |1\rangle \end{cases}$$

Théorème de Kitaev - Shen-Vialyi :

Soit $n \geq 2$, $N = 2^n$. Toute matrice unitaire $U_N \in M_{N \times N}(\mathbb{C})$, vue comme une porte à n qubits, est calculée par un circuit sur l'ensemble de portes

$$\{\hat{NOT}, \hat{SWAP}, \hat{TOF}\} \cup \{\Lambda(U) \mid U \text{ de taille } 2\}$$

. Les portes réversibles de bases (traduits en transformations unitaires) ainsi que toutes les portes à 1 qubit, contrôlés par un autre —●—,

suffisent pour calculer n'importe quelle transformation unitaire sur N qubits