

PLAN C.i. 5 - Calcul quantique, algr. Deutsch

- Rappel : téléportation quantique et états intriqués
- Calcul quantique : registres quantiques, entrées et sorties, parallélisme quantique
- Algr. de Deutsch

Supplément :

- théorème du non-clonage quantique (notes C.i. 4)

appel: états intriqués (enchevêtrés)

Dans un espace produit (exemple: espace des états à 2 qubits) il existe des états qui ne se factorise pas - états intriqués

Ex.: base: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

$$|ij\rangle = |i\rangle \otimes |j\rangle \quad (\text{états factorisés})$$

$$|\psi\rangle = \sum_{i,j=0}^1 \alpha_{ij} |ij\rangle$$

$$|\beta\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \quad \text{état intriqué}$$

$$\exists \alpha, \beta, \gamma, \delta \in \mathbb{C} \quad \text{c. s.}$$

$$|\beta\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle).$$

Application: téléportation quantique

Chp. 3 - CALCUL QUANTIQUE

1.) Ordinateurs classique vs. ordinateurs quantiques

On peut schématiser un ordinateur classique (machine de Turing) à l'aide de 3 composants:

- 1.) des registres (qui contiennent les données à traiter)
- 2.) une unité de calcul (qui transforme les données suivant un algorithme défini en actionnant des portes logiques)
- 3.) une unité d'entrées/sorties (qui initialise les registres au début du traitement et lit les résultats à la fin.)

1.1.) Les registres

Registre classique: un ensemble de n bits, permettant de stocker $N = 2^n$ entiers entre 0 et $2^n - 1$.

Registre quantique: est défini en associant à chaque bit un qubit
 $\Rightarrow$ un registre quantique est un système quantique de n qubits dont les états seront éléments de l'espace des états de dimension $N = 2^n$.

On définit dans cet espace la base

$$\boxed{|j_1 j_2 \dots j_n\rangle := |j_1\rangle |j_2\rangle \dots |j_n\rangle, \quad j_1, \dots, j_n \in \{0, 1\}}$$

notations pour les vecteurs de la base de l'espace:
 1) liste des états de chaque qubit, éléments de $\mathbb{Z}_2 = \{0, 1\}$

$$|j_1 j_2 \dots j_n\rangle$$

2.) nombre entier $j \in [0, 2^n - 1]$ dont l'ensemble $(j_1, j_2, \dots, j_n)$ constitue la décomposition binaire

$$j = j_1 2^{n-1} + \dots + j_n$$

$\mathbb{Z}_N$ - l'ensemble des entiers modulo N
 $j \in \mathbb{Z}_N \Leftrightarrow (j_1, j_2, \dots, j_n) \in \mathbb{Z}_2^n$, $N = 2^n$

$$j = j_1 2^{n-1} + j_2 2^{n-2} + \dots + j_n 2^0$$

$$k = k_1 2^{n-1} + k_2 2^{n-2} + \dots + k_n 2^0$$

notation:

$$\Rightarrow j \cdot k = (j_1 k_1 + j_2 k_2 + \dots + j_n k_n) \bmod 2$$

$$= j_1 k_1 \oplus j_2 k_2 \oplus \dots \oplus j_n k_n$$

$\oplus$ - addition binaire sans retenue

$$(ou XOR: 0 \oplus 0 = 1 \oplus 1 = 0, 0 \oplus 1 = 1 \oplus 0 = 1)$$

$|x\rangle$ - les N états de la base, $x \in \mathbb{Z}_N$,

$$x \in \{0, \dots, 2^n - 1\}$$

$$\underbrace{100\dots00}_n \text{ qubits} \stackrel{\text{not}}{=} |0\rangle$$

$$100\dots01 \stackrel{\text{not}}{=} |1\rangle$$

$$\dots$$

$$|x_1 x_2 \dots x_n\rangle \stackrel{\text{not}}{=} |x\rangle, \text{ où } x = x_1 2^{n-1} + \dots + x_n 2^0$$

spécificité registres quantiques:

ils peuvent se trouver non seulement dans un des états de la base (comme le registre classique), mais aussi dans un état de superposition

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle$$

85. Quantiques: représentés par l'évolution
 d'un ou plusieurs registres sous l'effet de l'application
 d'opérateurs unitaires.
 L'état de l'ordi peut comprendre plusieurs registres
 (le plus souvent 2).

exemple:

un registre à n qubits (états: $|x\rangle$, $x \in \mathbb{Z}_{2^n}$)
 — , — m — (— : $|y\rangle$, $y \in \mathbb{Z}_{2^m}$)

état quantique total: $|x\rangle|y\rangle \stackrel{\text{not.}}{=} |xy\rangle$
 (élément d'un espace des états
 de 2^{n+m} dim.)

Les entrées / sorties

L'entrée correspond à mettre le système quantique
à constituer les registres dans un état initial;

on dit qu'on prépare le système.

Remarque: le plus souvent les différents registres
sont initialement dans l'état $|0\rangle$, et la préparation
consiste à faire agir différents opérateurs, comme la
transformation de Hadamard.

La sortie: correspond à la lecture d'un registre -
mesure de l'état quantique final du registre.

d'après (le postulat de la mesure de la) méca. quantique,
cela modifie, et de façon irréversible, l'état du
registre (qui est projeté sur 1 des états de la base).

En général, les algo quantiques utilisent de
mesures partielles de l'état final

(mesure de seulement un de registres,
voire même 2 ou 3 bits d'un registre)

parallelisme quantique

Souvent on a besoin d'évaluer de fonctions

$$f: \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$$

on ne peut pas toujours représenter par un opérateur unitaire.

Pour associer un opérateur unitaire à l'évaluation d'une fonction, on introduit de qubits auxiliaires)

on définit:

- un registre de données $|x\rangle$ à n qubits, $x \in \mathbb{Z}_2^m$

contiendra la valeur de la variable)

- un registre de résultats $|y\rangle$ à $m - n$, $y \in \mathbb{Z}_2^m$

contiendra le résultat)

un opérateur unitaire

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$$

④ - l'addition binaire (sans retenue)

Exo.: Montrer que U_f est unitaire)

exemple: l'opérateur AND

	0	1
0	0	0
1	0	1

$(x, y) \mapsto f(x, y) = x \wedge y = xy$ n'est pas inversible

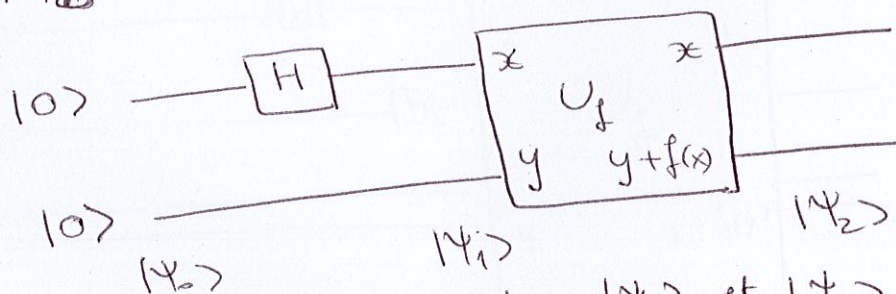
On peut le mettre en œuvre de façon réversible.)

$$(x, y, z) \rightarrow (x, y, z \oplus xy) \quad (\text{porte de Toffoli})$$

Le parallélisme est un trait de l'alg. quantique
 la fonction $f(x)$ peut être évaluée simultanément
 sur plusieurs valeurs de x (conséquence de la
superposition des états de qubits)

Exemple: registre donné } à 1 qubit
 — résultats

val. initiale de chaque registre: $|0\rangle$
 $|\Psi_0\rangle = |00\rangle$ (l'état initial du système des 2 registres)



Exo: Calculer les états $|\Psi_1\rangle$ et $|\Psi_2\rangle$.

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |10\rangle)$$

Etat de sortie:

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}} (|0, f(0)\rangle + |1, f(1)\rangle)$$

contient à la fois $f(0)$ et $f(1)$ obtenues par
 la seule application de la porte U_f

Ex: application de porte de Hadamard sur 2 qubits
 (registre donnée à 2 qubits)

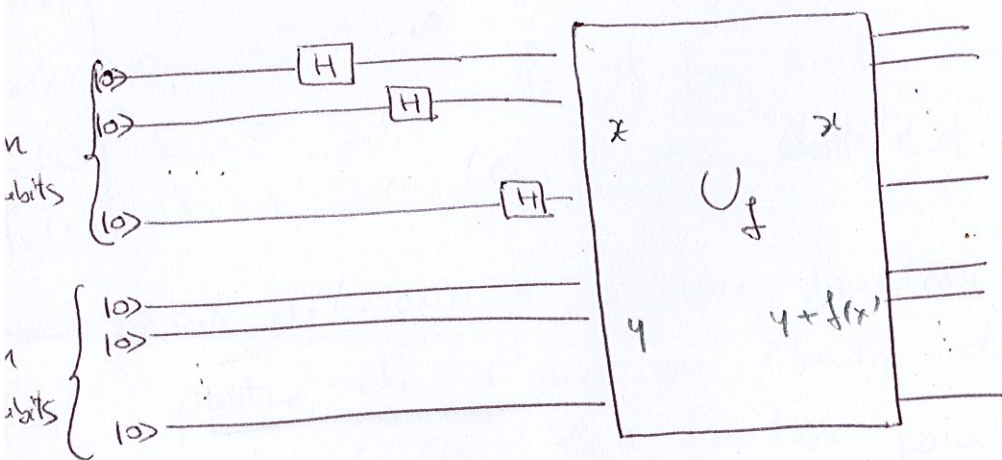
$$H_2\left(\frac{1}{\sqrt{2}}|00\rangle + |10\rangle\right) = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Généralisation:

Soit un registre à n qubits (registre de données)

La transformation / porte de Hadamard sur chaque qubit donne pour le registre de données

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle, \quad x \in \mathbb{Z}_{2^n}$$
$$= \frac{1}{\sqrt{2^n}} (|00\dots 0\rangle + |00\dots 01\rangle + \dots + |11\dots 11\rangle)$$



état de sortie:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |0 + f(x)\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

Remarque: cela fait apparaître de nouveau
toutes les valeurs de f en une seule opération —
parallélisme quantique.

CALCUL QUANTIQUE

Algorithme de Deutsch

(1985)

problème: Soit $f: \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$. il en existe 4 fonctions
une telle fonction est soit constante, soit équilibrée
i.e. d. elle vaut 0 dans la moitié de cas et
1 ——— l'autre moitié)

x	0	1
$f_0(x)$	0	0
$f_1(x)$	0	1
$f_2(x)$	1	0
$f_3(x)$	1	1

f_0 et f_3 sont les fonctions constantes

f_1 et f_2 sont ——— équilibrées

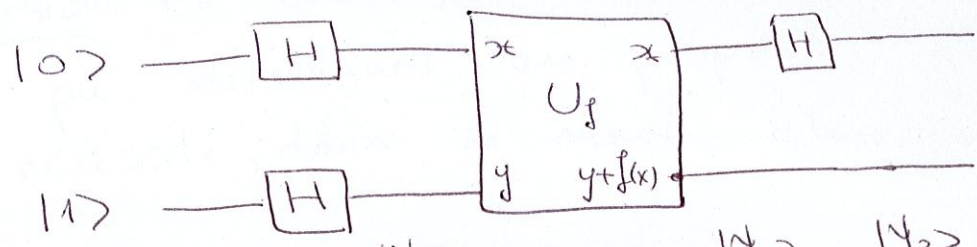
(la fonction identité et resp. la fonction NOT)

$\Rightarrow$ pour déterminer si une fonction prise au hasard
est partie de l'une ou l'autre de ces catégories,
il faut évaluer la fonction pour (au moins) 2 val.
différentes de la variable.

Deutsch a montré qu'en exploitant le parallélisme quantique
on peut répondre au problème en une seule évaluation.

ystème (de 2 registres):

2 registres, chaque u à 2 qubit



Ex.: Calculer les états $|\Psi_i\rangle$ du système (de 2 registres) au fil du circuit
 $|\Psi_0\rangle = |01\rangle$

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) =$$

$$= \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) =$$

$$= \frac{1}{2} \left(\sum_{x=0}^1 |x\rangle \right) (|0\rangle + |1\rangle) = \frac{1}{2} \sum_{x=0}^1 (|x, 0\rangle + |x, 1\rangle)$$

$$|\Psi_2\rangle = \frac{1}{2} \sum_{x=0}^1 (|x, 0 \oplus f(x)\rangle - |x, 1 \oplus f(x)\rangle)$$

Rq.: $y \oplus f(x) = \begin{cases} y, & \text{si } f(x)=0 \\ \bar{y}, & \text{sinon} \end{cases} \Rightarrow$

~~$|\Psi_2\rangle \Rightarrow$~~ $|x, 0 \oplus f(x)\rangle - |x, 1 \oplus f(x)\rangle = \begin{cases} |x, 0\rangle - |x, 1\rangle, & \text{si } f(x)=0 \\ |x, 1\rangle - |x, 0\rangle, & \text{si } f(x)=1 \end{cases}$

$$\Rightarrow |x, 0 \oplus f(x)\rangle - |x, 1 \oplus f(x)\rangle = (-1)^{f(x)} (|x, 0\rangle - |x, 1\rangle) \Rightarrow$$

$$\Rightarrow |\Psi_2\rangle = \frac{1}{2} \sum_{x=0,1} (-1)^{f(x)} (|x, 0\rangle - |x, 1\rangle) =$$

état résultant du 1er qubit est: $= \frac{1}{2} \left(\sum_{x=0}^1 (-1)^{f(x)} |x\rangle \right) (|0\rangle - |1\rangle)$

$$|\Psi_3\rangle = \frac{1}{2\sqrt{2}} (-1)^{f(0)} (|0\rangle + |1\rangle) + \frac{1}{2\sqrt{2}} (-1)^{f(1)} (|0\rangle - |1\rangle) =$$

$$= \frac{1}{2\sqrt{2}} ((-1)^{f(0)} + (-1)^{f(1)}) |0\rangle + \frac{1}{2\sqrt{2}} ((-1)^{f(0)} - (-1)^{f(1)}) |1\rangle$$

si f est cte. (i.e. $f(0)=f(1)$) $\Rightarrow$ le qubit vaut $|0\rangle$
 si f est équilibré (c.a.d. $f(0) \neq f(1)$) $\Rightarrow$ le qubit vaut $|1\rangle$

Conséquence: Une seule mesure du qubit donne le coup sûr: $\begin{cases} |0\rangle & \text{si la fonction } f \text{ est constante} \\ |1\rangle & \text{si } f \text{ est équilibré.} \end{cases}$

Conclusion: En une seule action de la porte U_f ,
on a pu déterminer une propriété globale de f ,
qui nécessite, dans le monde classique, 2 évaluations
de f .

C'est plus important si on généralise le problème
à un registre de données à n qubits.

Il suffit d'une seule action de U_f pour déterminer
si la fonction f est équilibrée ou constante;
classiquement, il faut $2^{n-1} + 1$ évaluations de f .