Information Quantique

Frédéric Magniez

Cours 2 :
Tirage à pile ou face
Algorithmes élémentaires

Problème

- Alice et Bob sont éloignés
- Ils veulent tirer à pile ou face de manière équitable

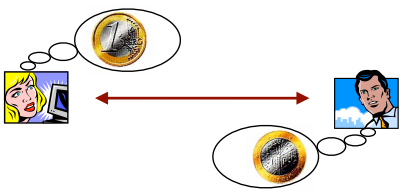
Classiquement

- Solutions basées sur des difficultés combinatoires
- Aucune solution inconditionnellement sure

Quantiquement

- Biais possible : 0,25 [Ambainis 2001]
- Biais impossible : 0,207 [Kitaev 2002]

Version faible : élection



- Alice voudrait pile
- Bob voudrait face
- Aucune impossibilité connue !
- Biais possible : arbitrairement petit ! [Mochon 2007]

Essai de protocole

$$|\psi_{b,x}\rangle = \begin{cases} |0\rangle, & \text{si } b=0, x=0 \\ |1\rangle, & \text{si } b=0, x=1 \\ \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle), & \text{si } b=1, x=0 \\ \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle), & \text{si } b=1, x=1 \end{cases}$$

- Alice choisit deux bits aléatoires b, x
- Alice envoie $|\psi_{b,x}\rangle$ à Bob
- Bob choisit un bit aléatoire b' qu'il envoie à Alice
- Alice envoie b, x à Bob qui vérifie l'état reçu
- Le résultat du protocole est $b \oplus b'$

Exercice

- Montrer que si Alice et Bob sont honnêtes, alors $\Pr_{x,b,b'}(b \oplus b' = 0) = \frac{1}{2}$
- Montrer que Bob ne peut pas tricher
- Montrer qu'Alice peut tricher avec certitude : biais = 0.5

  Indication : utiliser une paire EPR

Solutions

- Ne pas prendre $|\psi_{b,0}\rangle \perp |\psi_{b,1}\rangle \implies$ biais ≤ 0.42
- Augmenter la dimension $\implies$ biais ≤ 0.25

Protocole à 2 paires EPR

- Alice prépares 2 paires EPR $|\beta_{00}\rangle|\beta_{00}\rangle$

  et envoie le second qubit de chaque paire à Bob
- Bob choisit aléatoirement une des 2 paires EPR à vérifier
- Alice envoie le qubit manquant de la paire EPR choisie par Bob
- Bob fait une mesure dans la base de Bell :

  S'il observe $|\beta_{00}\rangle$, il continue sinon il annule le protocole
- Bob mesure le qubit de la paire EPR non utilisée

  et annonce son résultat à Alice
- Alice vérifie que la mesure du qubit restant donne le même résultat

Théorème

- Le biais maximal de triche pour Alice et Bob est 1/4

Exercice

- Prouver que Bob ne peut pas tricher avec un biais supérieur à 1/4, et donner la tricher correspondante.
- Est-ce que Bob peut se faire prendre en suivant votre triche ?

Exercice

- Alice va tricher en préparant l'état $\frac{1}{\sqrt{3}}(|00\rangle|\beta_{00}\rangle + |\beta_{00}\rangle|00\rangle)$
  puis en suivant le protocole décrit
- Calculer la probabilité que Bob n'annule pas le protocole
- En supposant que Bob continue le protocole, calculer la probabilité que le résultat du protocole soit 0

Definition

- Etats pures
$$F(|\phi\rangle, |\psi\rangle) = \langle\phi|\psi\rangle^2$$
- Etat pur et état mélangé
$$F(\rho, |\psi\rangle) = \langle\psi|\rho|\psi\rangle$$
- Etats mélangés
$$F(\rho, \sigma) = \left(\mathrm{tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)\right)^2$$

Propriétés

- $0 \leq F(.,.) \leq 1$ et $F(\rho, \sigma) = 1$ ssi $\rho = \sigma$
- $F(\rho, \sigma) \leq F(\mathrm{tr}_A(\rho), \mathrm{tr}_A(\sigma))$
- $F(\rho, \sigma_0) + F(\rho, \sigma_1) \leq 1 + \sqrt{F(\sigma_0, \sigma_1)}$

Théorème

- $F(\rho, \sigma) = \max_{|\phi\rangle\langle\phi|=\rho,\ |\psi\rangle\langle\psi|=\sigma} F(|\phi\rangle, |\psi\rangle)$

Remarque

- La fidélité mesure la difficulté de distinguer 2 états
  (Exercice : Pourquoi dans le cas d'états purs?)

Scénario

- Alice prépare un état différent $|\psi\rangle$ sur plusieurs (au moins 4) qubits

  Parmi ces qubits, distinguons 4 positions : 1, 1', 2 et 2'

  Les autres positions sont désignées par l'ensemble S
- Alice envoie 2 de ces qubits, numérotés 1' et 2'
- Quand Bob lui demande le qubit qui complète la présupposée paire EPR, Alice peut effectuer une transformation unitaire sur ces qubits, puis il envoie soit le qubit numéroté 1, soit le qubit numéroté 2

Exercice

- Montrer qu'on peut supposer qu'Alice effectue une transformation unitaire uniquement lorsque Bob demande le qubit 2.

  On appellera par la suite cette transformation U
- Montrer que la probabilité que le résultat du protocole soit 0 est

$$\frac{1}{2}(F(\mathrm{tr}_{2S}(|\psi\rangle\langle\psi|), |\beta\rangle_{11'}|0\rangle_{2'}) + F(\mathrm{tr}_{1S}(U|\psi\rangle\langle\psi|U^*), |0\rangle_{1'}|\beta\rangle_{22'})$$

  où $|\beta\rangle = |\beta_{00}\rangle$
- Borner cette probabilité par la quantité suivante puis conclure :

$$\frac{1}{2}\left(1 + \sqrt{F(|0\rangle\langle 0|_{1'} \otimes \frac{\mathrm{Id}_{2'}}{2}, \frac{\mathrm{Id}_{1'}}{2} \otimes |0\rangle\langle 0|_{2'})}\right)$$

Calculabilité

- Que veut dire calculer ?
- Qu'est-ce qu'une machine, un programme ?
- Comment modéliser (universellement) un ordinateur ?

Difficulté (intrinsèque) d'un problème

- Calculable / Non calculable
- Facile / Intraitable

Rappels historiques

- Machine de Turing, calculabilité, universalité : [Turing 1936]
- Proposition : EDVAC (Electronic Discrete VAriable Computer) [von Neumann 1945]
- Premier ordinateur : Mark I [Robinson-Tootill-Williams 1949]

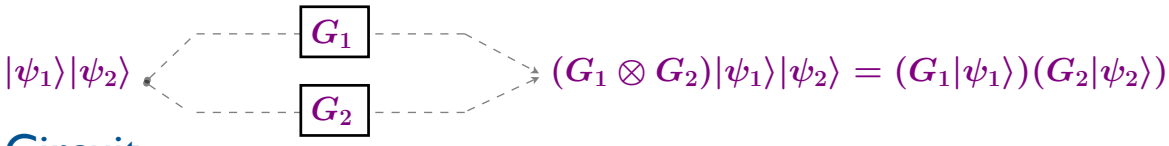
Calcul quantique

- Idée : simulation de systèmes quantiques [Feynman 1982]
- Machine de Turing quantique : [Deutsch 1985,1989], [Bernstein-Vazirani 1993]
  Circuits quantiques : [Yao 1993]
- Technologie: 2 qubits [ENS (Haroche) 1995], 5 qubits [IBM (Chuang) 2000], 12 qubits [IQC, PI, MIT 2006],

Portes $U \in \mathcal{U}(2^k), \quad k = 1, 2, 3$

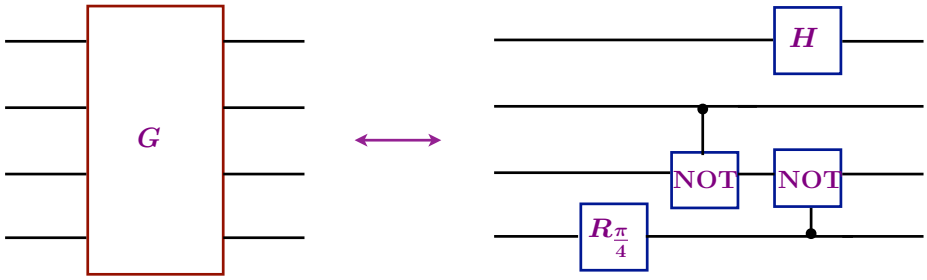
- Une porte quantique est une transformation unitaire qui agit sur au plus **3** qubits

Produit tensoriel de portes



Circuit

- Un circuit quantique est la composition de portes (étendues par $\otimes$ Id)



Théorème. Familles universelles (au sens approché)

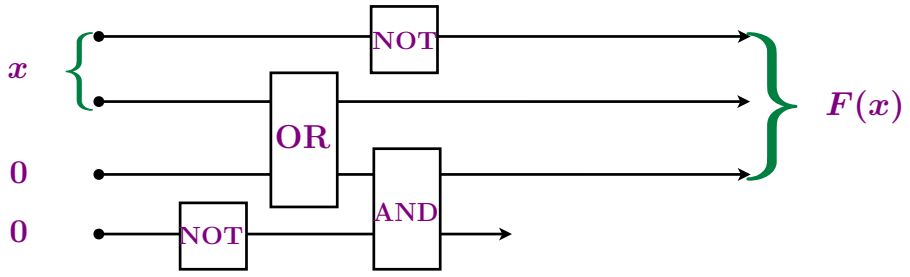
- NOT, H et Toffoli (c-c-NOT) (transformations uniquement réelles)
- NOT, $\sqrt{\text{H}}$ et c-NOT
- La porte c-NOT et toutes les portes sur 1-qubit (simulation exacte)

Définition

- Un circuit $C = C_L \dots C_2 C_1$ calcule une fonction F si pour toute entrée x :

$$C(x, 0^k) = (F(x), z)$$

- La taille d'un circuit est le nombre de portes utilisées pour le réaliser.
- La complexité d'une fonction est la taille minimale du circuit qui la calcule



Remarque

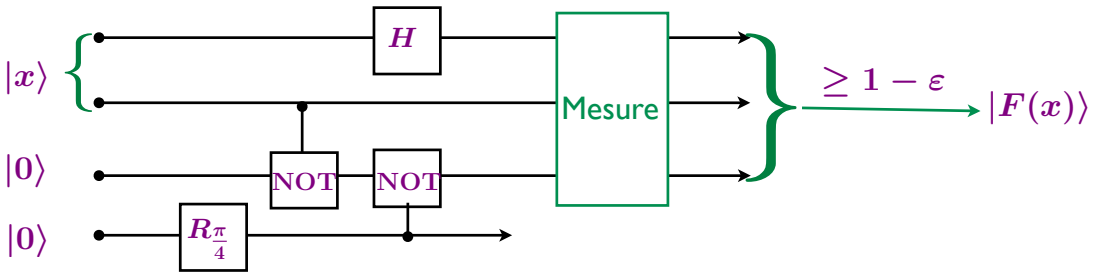
- La complexité d'une fonction ne dépend pas du choix de base universelle de portes (à une constante multiplicative près qui ne dépend que des bases)

Définition

- Un circuit $U = U_L \dots U_2 U_1$ calcule une fonction F avec erreur ε si pour toute entrée x :

$$\sum_z |\langle F(x), z|U|x, 0^k\rangle|^2 \geq 1 - \varepsilon$$

- La taille d'un circuit est le nombre de portes utilisées pour le réaliser.
- La complexité approchée (resp. exacte) d'une fonction est la taille minimale du circuit qui la calcule avec erreur 1/3 (resp. 0)



Remarques

- La complexité d'une fonction ne dépend pas du choix de base universelle
- L'erreur peut arbitrairement être réduite à ε par $\log(1/\varepsilon)$ itérations

Définition

- Un algorithme quantique pour le calcul d'une fonction $F : \{0,1\}^* \to \{0,1\}^*$ est un algorithme classique qui calcule une famille de circuits $(C_n)_{n\in\mathbb{N}}$ telle que C_n calcule avec erreur $\varepsilon < 1/3$ la fonction F restreinte aux entrées de $\{0,1\}^n$
- La complexité en temps $T(n)$ d'un algorithme quantique est la taille du circuit C_n **PLUS** le temps qu'il faut pour décrire le circuit C_n avec précision $O(1/|C_n|)$

Remarques

- En règle générale la description du circuit est négligeable
- Les amplitudes des portes sont donc calculables !
- La complexité *ne dépend pas* du choix des portes

Classes de complexité

- Fonctions (problèmes) calculable (résoluble) en temps polynomial en la taille de l'entrée

  déterministe : P

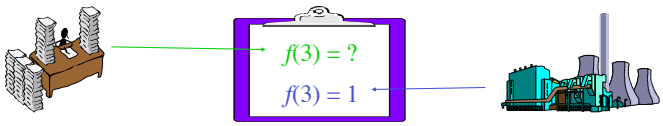
  probabiliste avec erreur $\varepsilon < 1/3$: BPP

  quantique avec erreur $\varepsilon < 1/3$: BQP

$$\mathrm{P} \subseteq \mathrm{BPP} \subseteq \mathrm{BQP}$$

Problème

- Entrée : $f : \{0,1\}^n \to \{0,1\}$ soit constante, soit balancée
- Sortie : 0 ssi f est constante
- Contrainte : f est une boîte noire



Complexité en requêtes

- Déterministe : $1 + 2^{n-1}$
- Quantique : 1

Cas $n = 1$

- Problème équivalent à décider si $f(0) = f(1)$ pour f quelconque

STOP $x \mapsto f(x)$ n'est pas nécessairement réversible !

Implémentation de f

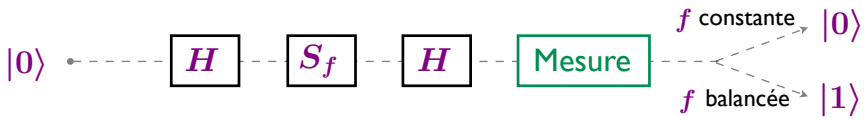
$$|b\rangle \dashrightarrow \boxed{S_f} \dashrightarrow (-1)^{f(b)}|b\rangle$$

Porte de Hadamard : lame demi-onde à 22,5°

$$|b\rangle \dashrightarrow \boxed{H} \dashrightarrow \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$$

Circuit quantique

$$|0\rangle \dashrightarrow \boxed{H} \dashrightarrow \boxed{S_f} \dashrightarrow \boxed{H} \dashrightarrow \boxed{\text{Mesure}} \dashrightarrow ?$$



Initialisation : $|0\rangle$

Parallélisation : $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

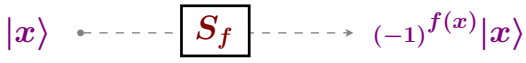
Appel de la fonction : $\frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)$

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

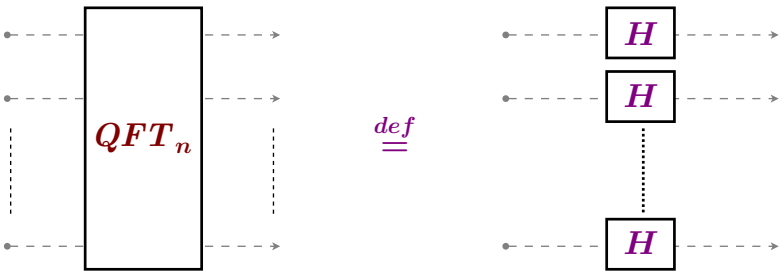
Au final : $\frac{1}{2}(((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + ((-1)^{f(0)} - (-1)^{f(1)})|1\rangle)$

Dans ce cas la supériorité du quantique ne vient pas de l'enchevêtrement, mais des interférences constructives et destructives.

Implémentation de f



Transformée de Fourier quantique



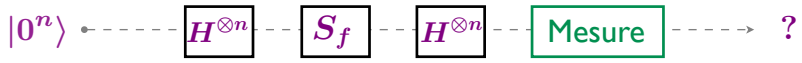
Exercice

- Vérifier que

$$QFT_n|x\rangle = \frac{1}{2^{n/2}} \sum_y (-1)^{x \cdot y} |y\rangle \quad \text{avec} \quad x \cdot y = \sum_i x_i y_i \mod 2$$

Exercice 1

- Montrer que le circuit suivant résout le problème



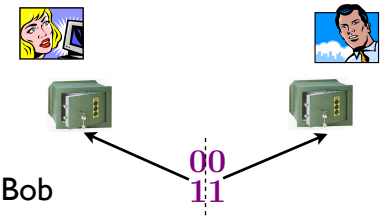
Exercice 2

- Montrer que le même circuit permet de trouver f avec la promesse que

$$f(x) = a \cdot x$$

- Remarque : on montre que pour ce problème, la complexité probabiliste en requêtes est en $\Omega(n)$

De l'enchevêtrement ?



- L'"enchevêtrement probabiliste" existe
  - Tirer à pile ou face 00 ou 11
  - Partager chacun des bits entre Alice et Bob
  - Alice/Bob regarde son bit quand il le désire, son résultat est alors corrélé avec celui de Bob/Alice
- Mais l'enchevêtrement quantique est "plus fort"
  - Paradoxe EPR (violation des inégalites de Bell)

Des amplitudes complexes ?

- Non, on peut les simuler par des amplitudes réelles

$$\alpha|0\rangle + \beta|1\rangle \simeq \alpha_r|00\rangle + \alpha_i|01\rangle + \beta_r|10\rangle + \beta_i|11\rangle \quad \mathcal{U}(2^n) \simeq \mathcal{O}(2^{n+1})$$

Des amplitudes négatives ?

- Oui car possibilité d'interférences destructives

De la complexité des amplitudes ?

- Non, les amplitudes doivent être facilement calculables pour être physiquement réalisables