COLLÈGE DE FRANCE
1530

Algorithmes quantiques

Limites du calcul quantique

02-06-2021

Frédéric Magniez

Professeur invité sur la chaire Informatique et sciences numériques
En partenariat avec Inria
Année académique 2020-2021

frederic.magniez@college-de-france.fr

Partie 3 - Algorithmique avancée

- Apprentissage automatique
- Limites du calcul quantique
- Usage décentralisé de type Internet

26 mai 2021
Cours : Simulation hamiltonienne, résolution ultra-rapide de systèmes linéaires, et applications
Séminaire : Quantum Machine Learning, Iordanis KERENIDIS, *CNRS, Paris*

02 juin 2021
Cours : Limites du calcul quantique : liens entre complexité classique et quantique
Séminaire : Suprématie quantique : où en sommes-nous aujourd'hui ?
André CHAILLOUX, *Inria, Paris*

09 juin 2021
Cours : Conclusion et ouverture vers le calcul distribué quantique
Séminaire : Quantum Computing as a Service:
Secure and Verifiable Multi-Tenant Quantum Data Centre
Elham KASHEFI, *CNRS, Paris et University of Edinburgh*



Simulation du calcul quantique

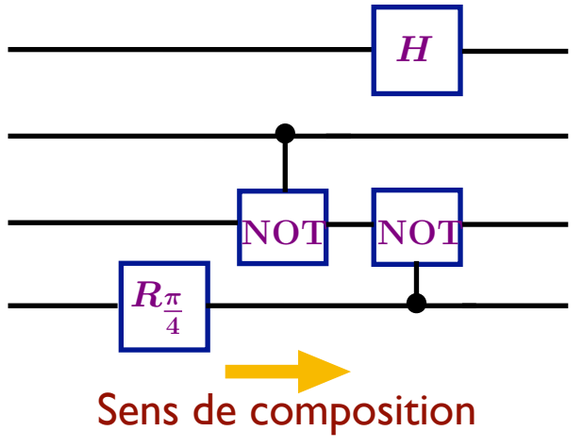
Circuits quantiques

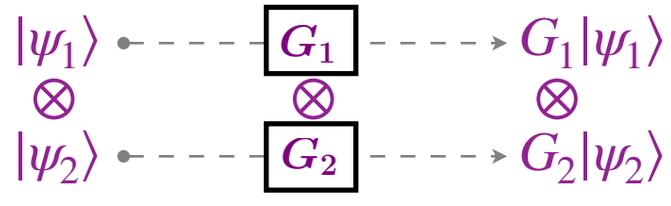
- Porte

  Transformation unitaire sur au plus 3 qubits

- Circuit

  Composition de portes (ordre et sur quels qubits)





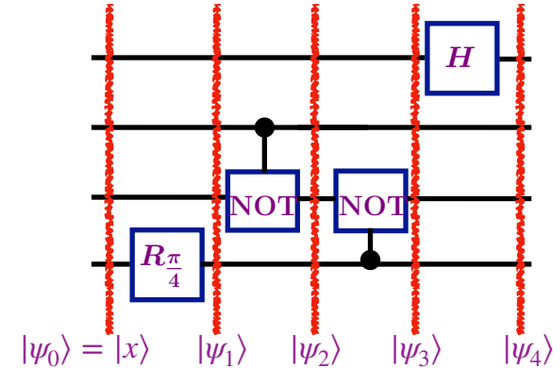
- Complexités : taille (nb de portes) et profondeur

Algorithmes quantiques

- Calcul classique sur mémoire classique
- Opérations quantiques (circuit) sur une mémoire quantique
- Interaction entre les deux
  - Description classique du circuit quantique
  - Réalisation "physique" du circuit quantique
  - Mesure (partielle ou totale) de la sortie du circuit quantique

Simulation

- Entrée : n bits (classiques) x et un circuit C sur n qubits de T portes
- Sortie : n bits y distribués selon l'observation des n qubits en sortie de C ayant pour entrée x



Approche Schrödinger

- Calculer la superposition après chaque porte
- Espace nécessaire : 2^n réels
- Simplification : circuit C composé de portes classiques/réversibles (NOT, c-NOT, Toffoli) et k portes H (Hadamard)

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

Les amplitudes finales sont de la forme $a/2^{k/2}$ avec a entier

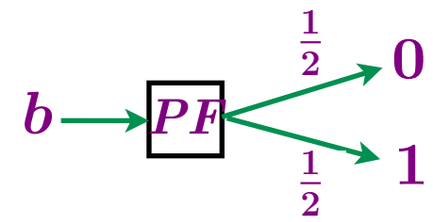
- Espace nécessaire : 2^n entiers d'au plus $(k/2)+1$ bits
- Chaque porte modifie tout état de la superposition : Temps 2^n
- Conclusion : Mémoire $O(k2^n)$ - Temps $O(T2^n)$

Remarque

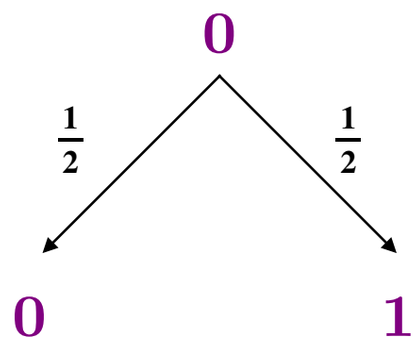
- Toute la superposition finale est calculée, soit bien plus que demandé

Chemins de calcul

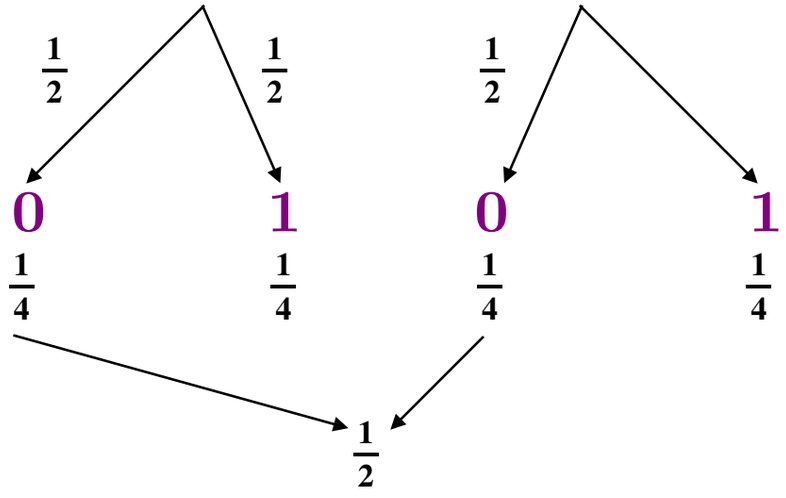
- Cas de 2 portes Pile ou Face (PF)



Porte Pile ou Face n° I



Porte Pile ou Face n°2



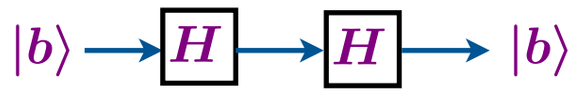
Remarques

- Un chemin de calcul ne nécessite que peu de mémoire
- En probabiliste : les probabilités s'accumulent constructivement

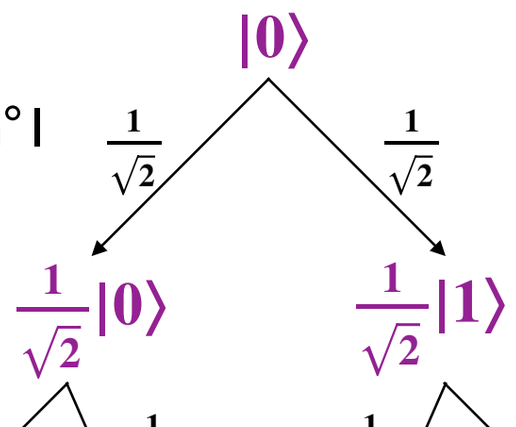
  Il suffit donc de suivre un chemin au hasard

Chemins de calcul

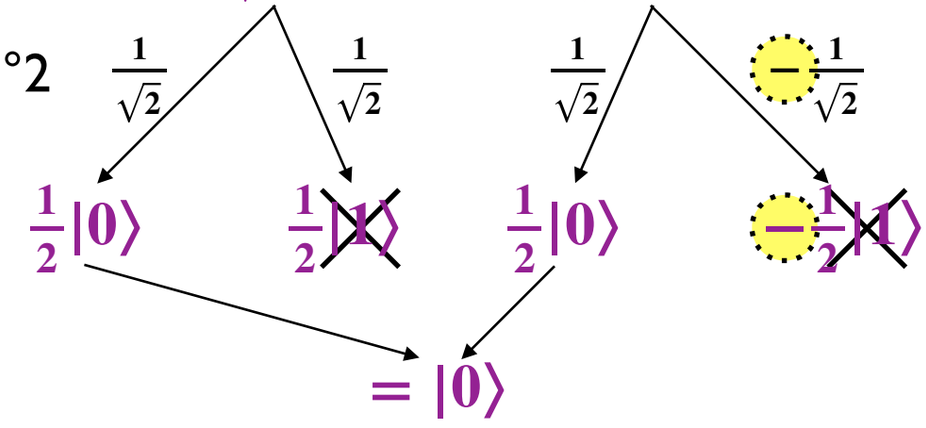
- Cas de 2 portes de Hadamard



Porte de Hadamard n°1



Porte de Hadamard n°2



Remarques

- Un chemin de calcul ne nécessite que peu de mémoire
- En quantique : les amplitudes peuvent être très grandes puis se compenser les unes les autres → interférences constructives ET destructives

  Il faut donc énumérer tous les chemins : temps exponentiel

Simulation simplifiée

- Entrée : n bits classiques x et un circuit C sur n qubits de T portes dont k portes H (Hadamard) et les autres "classiques" (NOT, c-NOT, Toffoli)
- Sortie : amplitude de $00\ldots0$ en sortie de C ayant pour entrée x

Approche Feynman

- Simulation selon chemin p = séquence de k bits

  Partir de $y=x$, $s=1$ et de la première porte G

  Si G est classique : appliquer directement G sur y

  Sinon $G=H$ est appliquée sur un qubit d'indice i

  Lire le prochain bit b de p

  Si $y_i=1$ et $b=1$, faire $s \leftarrow -s$

  Affecter $y_i \leftarrow b$

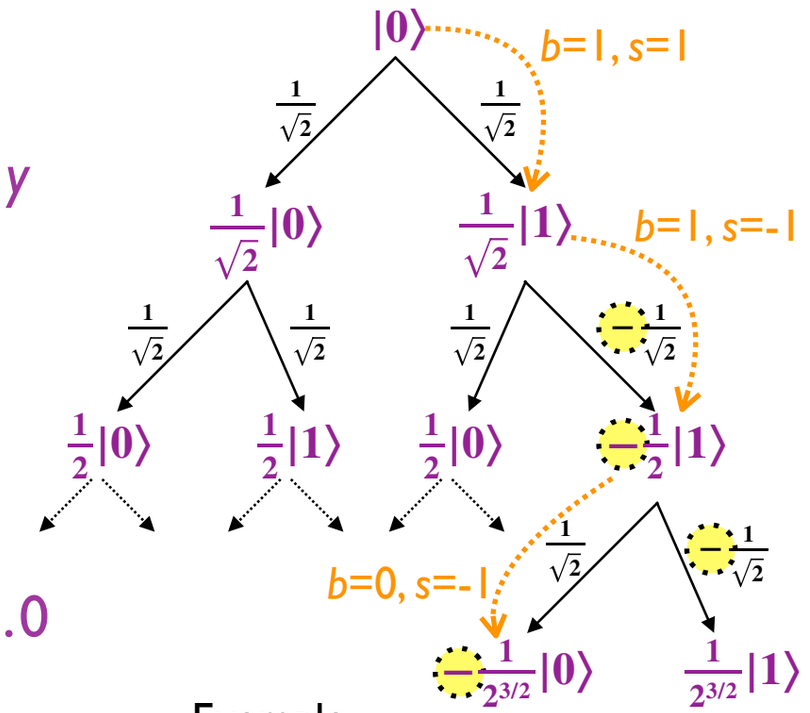
- Puis énumérer tous les chemins p menant à $y=00\ldots0$

  et cumuler les amplitudes $s/2^{k/2}$

- Conclusion : Mémoire $O(n+k)$ - Temps $O(T2^k)$
- Améliorations multiples selon la structure du circuit !

  Exemple si profondeur d [Aaronson, Chen 2017]

  Mémoire $O(n \log d)$ - Temps $O(n(2d)^{n+1})$

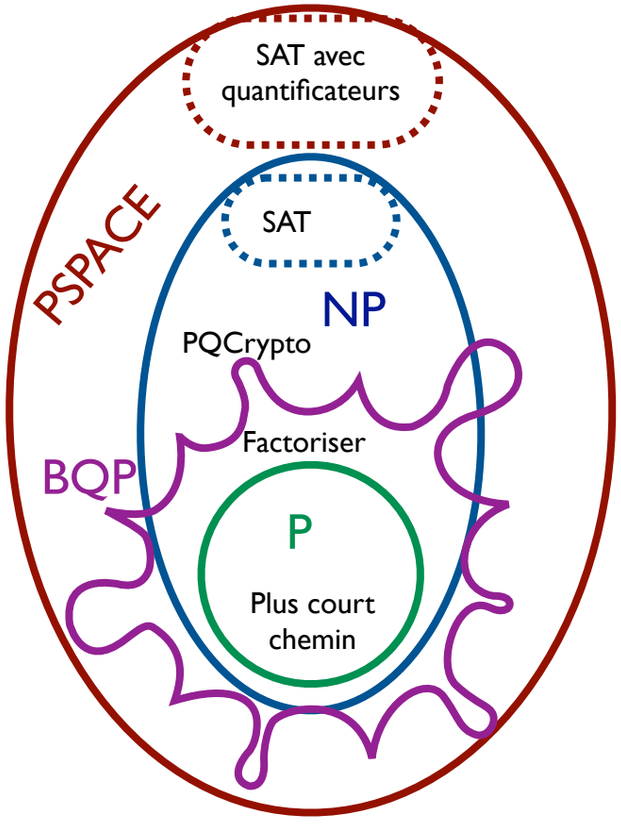


Exemple

C : H H H

x=0 p=110

Classes de complexité



Motivation / Objectifs

- Comprendre les limites calculatoires des ordinateurs

  En termes qualitatifs : calculabilité

  En termes quantitatifs : complexité

- Complexité : quantité de ressources nécessaires (mémoire, temps, nb de processeurs …) pour résoudre un problème algorithmique

Méhodologie

- Fixer un modèle de calcul : déterministe, probabiliste, quantique …
- Définir la complexité mesurée
- Cartographier les problèmes selon leur complexité asymptotique, identifier des problèmes représentatifs (complets) de leur classe

Quelques problèmes représentatifs

- Plus court chemin (plan de métro, réseau routier, graphe)
- Factorisation de nombres
- Problèmes à la base de la crypto post-quantique
- Satisfaction de contraintes : SAT, CSP
- Décision de l'arrêt d'une machine de Turing sur une entrée donnée

Classes de complexité

TRAITABLE - P : ce qui est *décidable* en temps polynomial (par rapport à la taille de l'entrée) et de façon déterministe

TRES DIFFICILE - EXP : idem en temps exponentiel

STRATEGIQUE - NP : ce qui peut être vérifié en temps polynomial de façon déterministe

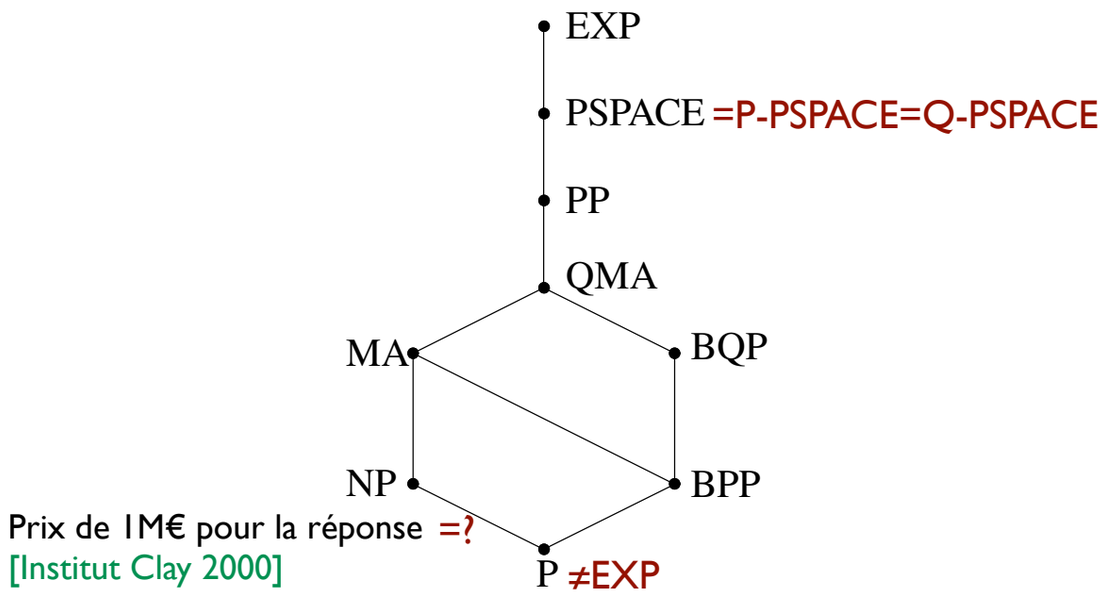
TRES DIFFICILE - PSPACE : ce qui est décidable en espace polynomial déterministe

TRAITABLE - BPP : idem P mais l'algorithme peut se tromper sur chaque entrée, avec avec une probabilité d'erreur ≤ 1/3 (sur l'aléa possible)

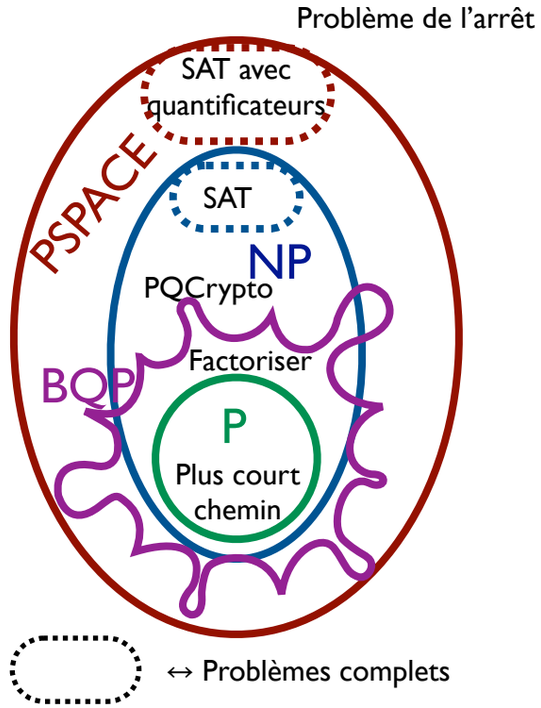
- MA : idem NP mais probabiliste

??? - BQP, QMA : idem pour les algorithmes quantiques

Que savons-nous ?



Prix de 1M€ pour la réponse =?
[Institut Clay 2000]



Complexité en requêtes

Cas du tri

- Entrée : N entiers $x_0, x_1, \ldots, x_{N-1}$
- Sortie : les mêmes entiers mais triés

  ou encore $\pi : [N] \to [N]$ une permutation telle que

  $$x_{\pi(0)} \leq x_{\pi(1)} \leq \cdots \leq x_{\pi(N-1)}$$

Meilleur algorithme connu ?

- N ? $N \log N$?

  Tout dépend de l'accès à l'entrée !
- Si uniquement des comparaisons : $N \log N$
- Si accès par valeurs et entiers dans $[N]$: N

Formalisation

- Arbres de décision / Complexité en requêtes

  (decision tree / query complexity)

Accès à l'entrée par Oracle

- Exemple : $x \in \{0,1\}^N$ (au lieu de $f : [N] \to \{0,1\}$ au cours 3)

  Requête $i \in [N]$ $\mapsto$ Réponse x_i

  En quantique : $O_x : |i, b\rangle \mapsto |i, b \oplus x_i\rangle$ (au lieu de $U_f : |i, b\rangle \mapsto |i, b \oplus f(i)\rangle$)

- Utilisation théorique

  Contraindre la façon dont l'algorithme utilise l'entrée

- Modélisation "pratique"

  Donnée : Accès à une masse de données

  Exemple : Mémoire (Q)RAM (cours 5, séminaire 6)

  Algorithme : l'oracle est calculé par un autre algorithme

  Exemple : Utilisation de Grover pour CSP (cours 5)

Retour sur le tri

- Accès aux N entiers $x_0, x_1, \ldots, x_{N-1}$ par comparaison signifie

  Accéder à $M = N^2$ bits

  Requête $i, j \in [N]$ $\mapsto$ Réponse 1 si $x_i \leq x_j$ et 0 sinon

- Dans ce modèle, Trier requiert $\Omega(N \log N)$ comparaisons

Notations

- $F : \{0,1\}^N \to \{0,1\}$ décrit le problème : une fonction à calculer
- $D(F), R(F), Q(F)$ sont les complexités en requêtes pour calculer F dans les modèles respectifs déterministes, probabilistes et quantiques (avec probabilité d'erreur ≤ 1/3)

Résultats généraux

- $D(F) \geq R(F) \geq Q(F)$
- $D(F) \leq R(F)^3$ et $D(F) \leq Q(F)^4$
- $R(F) \leq Q(F)^4$

Gains exponentiels sur le nombre de requêtes ?

- Uniquement pour des fonctions partielles (ou encore à promesse)
- Cas des problèmes de Bernstein-Vazirani (cours 3), ou plus généralement du Hidden Subgroup Problem (cours 4)
- Attention : ces relations ne présument rien sur les complexités en temps ou espace

Méthode par adversaire

Optimalité de l'algorithme de Grover

Problème

- Entrée : $x = x_0 x_1 x_{N-1} \in \{0,1\}^N$

  Accès : $O_x : |i, b\rangle \mapsto |i, b \oplus x_i\rangle$

- Sortie : $\mathrm{OR}(x_0, \ldots, x_{N-1})$ (au lieu de i tel que x_i s'il existe)

Calcul

- C un circuit à T requêtes
- Etat initial : $|0 \ldots 0\rangle$
- Sortie : Mesure d'un qubit dédié fournit $\mathrm{OR}(x_0, \ldots, x_{N-1})$

  avec probabilité au moins $\geq 1 - \varepsilon$ (en général 2/3)

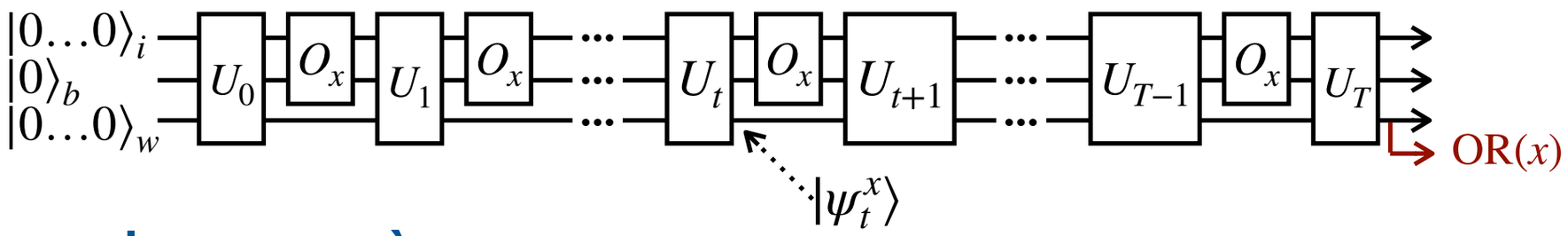
Solution à l'aide de l'algorithme de Grover

- Recherche : En $O(\sqrt{N})$ requêtes à x, l'algorithme de Grover produit une superposition de candidats $|i\rangle$ tels que $x_i = 1$ (s'ils existent)
- Vérification : En 1 requête supplémentaire à x sur ces indices, vérifier qu'ils correspondent à des bits à 1.

  Si c'est bien le cas, répondre 1, sinon 0.

Circuit à T requêtes

- $C = U_T O_x U_{T-1} O_x \ldots U_1 O_x U_0$, $|\psi_t^x\rangle$: Etat entre U_t et le prochain O_x



Mesure de progrès

- Notons $\overrightarrow{0} = 00\ldots0$ et $(j) = 0\ldots010\ldots0$ position j
- $W_t = \sum_{j=0}^{N-1} |\langle \psi_t^{\overrightarrow{0}} | \psi_t^{(j)} \rangle|$

Condition initiale

- Etat initial $|0\ldots0\rangle$, donc $W_0 = N$

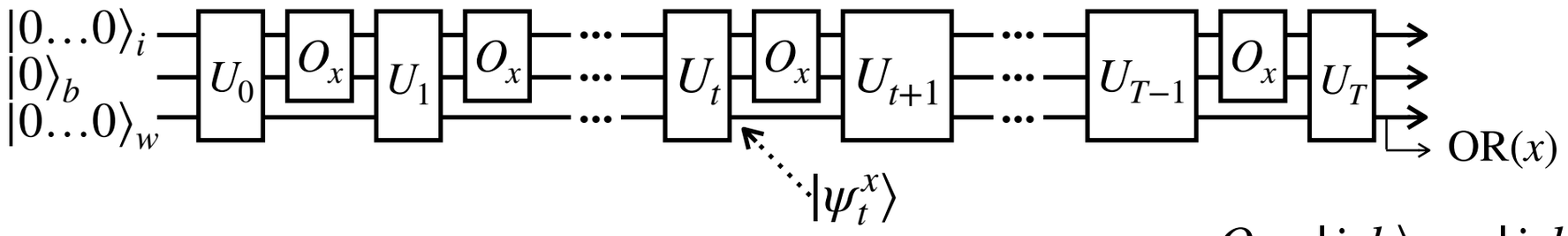
Condition finale

- Etat final : mesure du qubit dédié = $\mathrm{OR}(x_0, \ldots, x_{N-1})$ avec proba $\geq 1 - \varepsilon$
- Donc les états finaux $|\psi_T^{(j)}\rangle$ quasi-orthogonaux à $|\psi_T^{\overrightarrow{0}}\rangle$

$$|\langle \psi_T^{\overrightarrow{0}} | \psi_T^{(j)} \rangle| \leq 2\sqrt{\varepsilon(1-\epsilon)} \text{ et donc } W_T \leq 2N\sqrt{\varepsilon(1-\varepsilon)}$$

Circuit à *T* requêtes

- $C = U_T O_x U_{T-1} O_x \dots U_1 O_x U_0$, $|\psi_t^x\rangle$: Etat entre U_t et le prochain O_x



$$O_x : |i, b\rangle \mapsto |i, b \oplus x_i\rangle$$

Progrès de chaque question

- $|\psi_{t+1}^x\rangle = U_{t+1} O_x |\psi_t^x\rangle$ avec $O_{\overrightarrow{0}} = \mathrm{Id}$ et U_{t+1} unitaire donc

$$\langle \psi_{t+1}^{\overrightarrow{0}} | \psi_{t+1}^{(j)} \rangle = \langle \psi_t^{\overrightarrow{0}} | U_t | U_t O_{(j)} | \psi_t^{(j)} \rangle = \langle \psi_t^{\overrightarrow{0}} | O_{(j)} | \psi_t^{(j)} \rangle$$

- Le progrès est donc

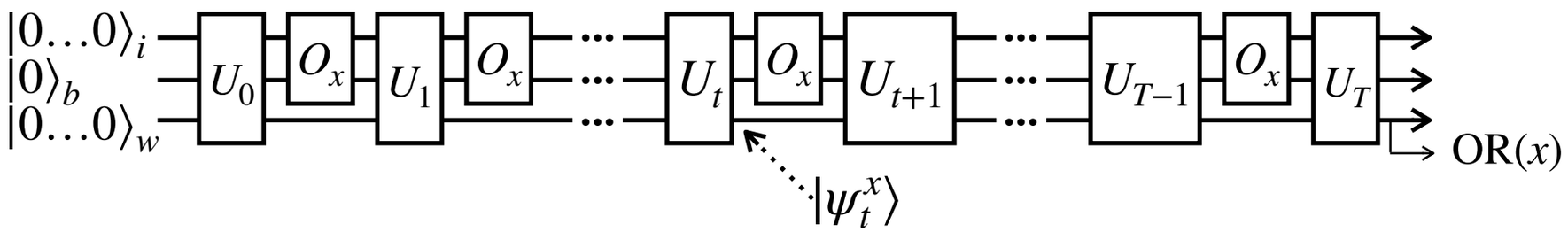
$$|\langle \psi_{t+1}^{\overrightarrow{0}} | \psi_{t+1}^{(j)} \rangle| - |\langle \psi_t^{\overrightarrow{0}} | \psi_t^{(j)} \rangle| \leq \left| \langle \psi_{t+1}^{\overrightarrow{0}} | \psi_{t+1}^{(j)} \rangle - \langle \psi_t^{\overrightarrow{0}} | \psi_t^{(j)} \rangle \right|$$

$$= \left| \langle \psi_t^{\overrightarrow{0}} | \mathrm{Id} - O_{(j)} | \psi_t^{(j)} \rangle \right| \leq 2 |\alpha_{t,j}^{\overrightarrow{0}}|$$

Amplitude de poser la question *j* sur $|\psi_t^{\overrightarrow{0}}\rangle$

Circuit à *T* requêtes

- $C = U_T O_x U_{T-1} O_x \dots U_1 O_x U_0$, $|\psi_t^x\rangle$: Etat entre U_t et le prochain O_x



Bilan

- $W_t = \sum_{j=0}^{N-1} |\langle \psi_t^{\vec{0}} | \psi_t^{(j)} \rangle|$

- $W_0 = N$, $W_T \leq 2N\sqrt{\varepsilon(1-\varepsilon)}$

- $W_t - W_{t+1} \leq \sum_{j=0}^{N-1} 2|\alpha_{t,j}^{\vec{0}}| \leq \sqrt{\sum_{j=0}^{N-1} 4} \sqrt{\sum_{j=0}^{N-1} |\alpha_{t,j}^{\vec{0}}|^2} \leq 2\sqrt{N}$

  Inégalité de Cauchy-Schwarz

- Donc $2T\sqrt{N} \geq N - 2N\sqrt{\varepsilon(1-\varepsilon)}$

  i.e. $T \geq \left(\frac{1}{2} - \sqrt{\varepsilon(1-\varepsilon)}\right)\sqrt{N}$

  Donc l'algorithme de Grover est optimal : $Q(OR) = \Theta(\sqrt{N})$

Autre exemple : PARITÉ

Problème

- Pour $x \in \{0,1\}^N$, $\mathrm{PAR}(x) = \sum_i x_i \mod 2$

Mesure de progrès

- $W_t = \sum_{x\in\{0,1\}^N, j\in[N]} |\langle \psi_t^x | \psi_t^{x^{(j)}} \rangle|$ avec $x^{(j)}$ = x dont le j-ème bit est modifié
- Etat initial $|0\ldots0\rangle$, donc $W_0 = N2^N$
- Chaque état final $|\psi_T^x\rangle$ est quasi-orthogonal à $|\psi_T^{x^{(j)}}\rangle$

$$|\langle \psi_T^x | \psi_T^{(j)} \rangle| \leq 2\sqrt{\varepsilon(1-\epsilon)} \text{ et donc } W_T \leq N2^{N+1}\sqrt{\varepsilon(1-\varepsilon)}$$

Progrès de chaque question

- $\langle \psi_{t+1}^x | \psi_{t+1}^{x^{(j)}} \rangle = \langle \psi_t^x | O_x O_{x^{(j)}} | \psi_t^{x^{(j)}} \rangle$ mais $O_x O_{x^{(j)}} = O_{(j)}$ …
- $|\langle \psi_{t+1}^x | \psi_{t+1}^{x^{(j)}} \rangle| - |\langle \psi_t^x | \psi_t^{x^{(j)}} \rangle| \leq \left| \langle \psi_t^x | \mathrm{Id} - O_{(j)} | \psi_t^{x^{(j)}} \rangle \right| \leq 2|\alpha_{t,j}^x \alpha_{t,j}^{x^{(j)}}|$
- $W_t - W_{t+1} \leq \sum_{x,j} 2|\alpha_{t,j}^x \alpha_{t,j}^{x^{(j)}}| \leq \sum_{x,j} \left(|\alpha_{t,j}^x|^2 + |\alpha_{t,j}^{x^{(j)}}|^2 \right) \leq 2^{N+1}$

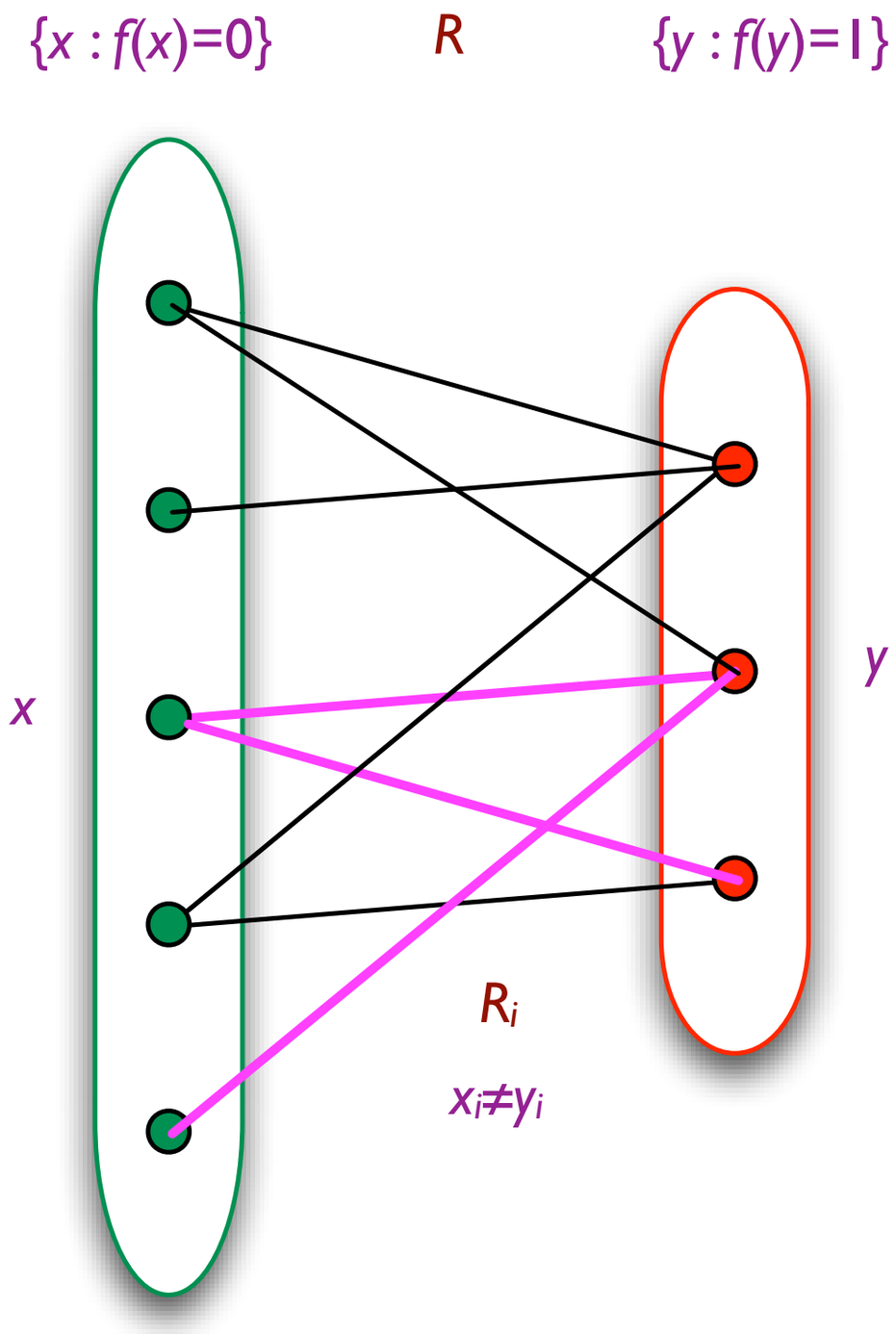
Conclusion

- $T \geq \left(\frac{1}{2} - \sqrt{\varepsilon(1-\varepsilon)}\right)N$

donc l'algorithme classique qui lit tout est optimal : $Q(\mathrm{PAR}) = \Theta(N)$

Adversaire quantique

- $R \subseteq \{(x,y) : F(x) = 0, F(y) = 1\}$
- $R_i \subseteq \{(x,y) \in R : x_i \neq y_i\}$



Hypothèses

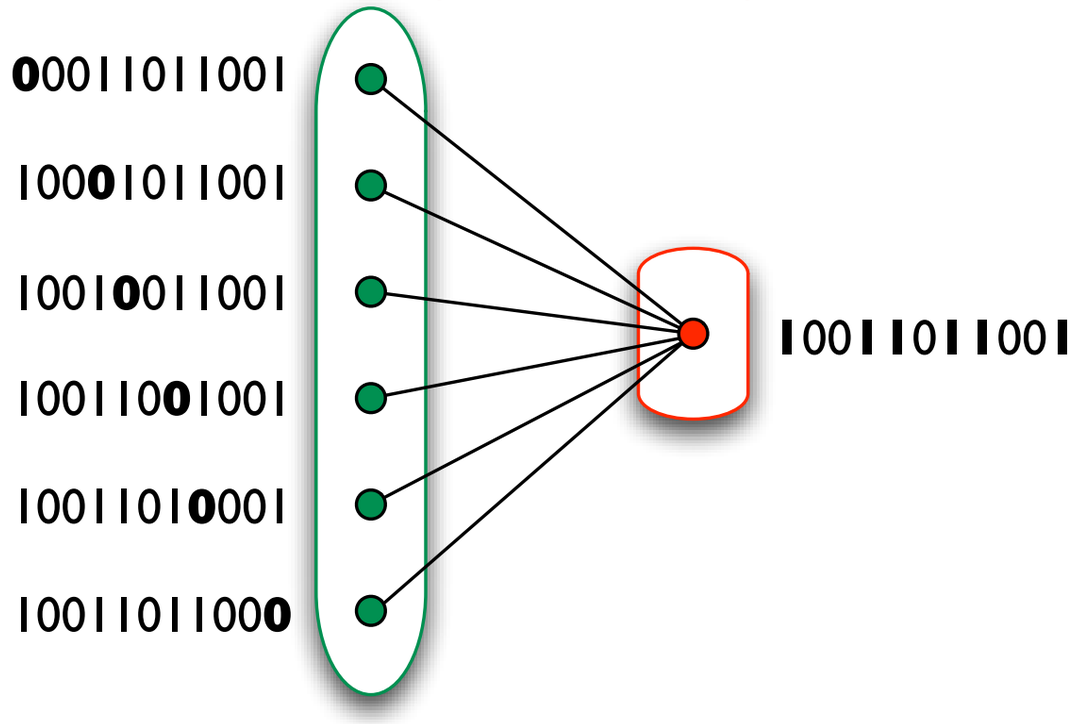
- Degré gauche de $R \geq m$
- Degré droite de $R \geq m'$
- Degré gauche de tout $R_i \leq \ell$
- Degré droite de tout $R_i \leq \ell'$

Résultat

- $Q(F) = \Omega\left(\sqrt{\frac{mm'}{\ell\ell'}}\right)$

Fonction et relation

- N : impair, $\mathrm{MAJ} : \{0,1\}^N \to \{0,1\}, x \mapsto 0$ si majorité de 0 dans x, 1 sinon
- $R \subseteq \{(x,y) : \mathrm{MAJ}(x) = 0,\ \mathrm{MAJ}(y) = 1,\ x$ et y diffèrent d'un seul bit$\}$



Analyse

- $m = m' = (N+1)/2$
- $\ell = \ell' = 1$
- donc $Q(\mathrm{MAJ}) = \Theta(N)$

Extension

- Pour k-SEUIL (k-THRESHOLD), $Q(k\text{-SEUIL}) = \Theta\left(\sqrt{k(N-k)}\right)$

  (correspond à l'algorithme de comptage quantique exact)

Dualité algorithmes et bornes inférieures

Relation avec poids

- Possibilité de mettre des poids sur les *arêtes* de la relation R

Variante spectrale [Barnum, Saks, Szgedy 2003]

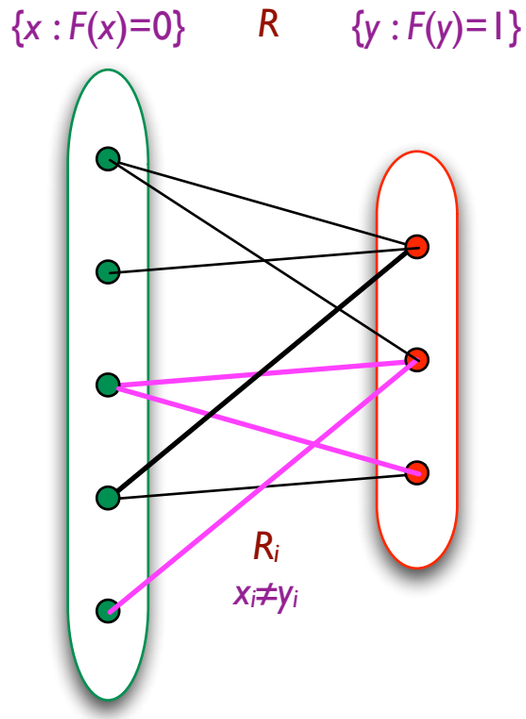
- R : matrice de taille $2^N \times 2^N$ telle que

  $R[x,y] \geq 0$ et $R[x,y] = R[y,x]$

  $R[x,y] = 0$ quand $F(x) = F(y)$

  $R_i[x,y] = 0$ quand $x_i = y_i$ (et sinon $R_i[x,y] = R[x,y]$)

  Alors $Q(F) \geq \dfrac{\|R\|}{\max_i \|R_i\|}$



Autres méthodes

- De multiples méthodes toutes équivalentes [Laplante, Lee, Szegedy 2005]
- Jusqu'à 2007 !

  où des poids négatifs sont introduits ! [Høyer, Lee, Spalek 2007]

Relation avec poids

- Possibilité de mettre des poids sur les *arêtes* de la relation *R*

Variante spectrale avec poids négatifs [Høyer, Lee, Spalek 2007]

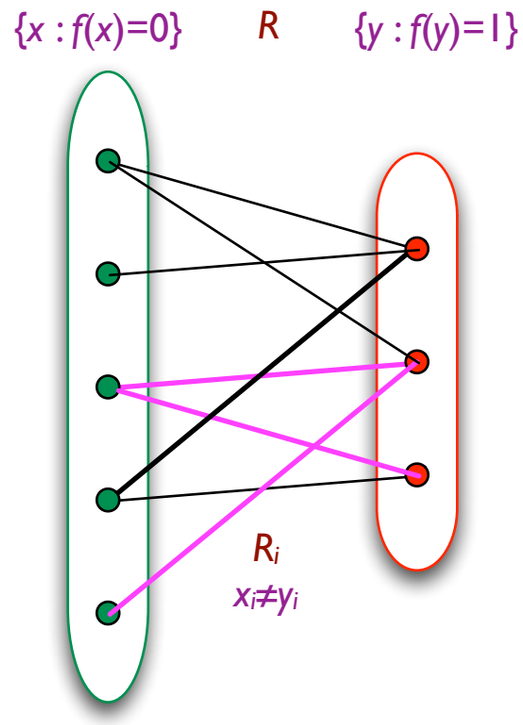
- R : matrice de taille $2^N \times 2^N$ telle que

  ~~$R[x,y] \geq 0$ et $R[x,y] = R[y,x]$~~

  $R[x,y] = 0$ quand $F(x) = F(y)$

  $R_i[x,y] = 0$ quand $x_i = y_i$ (et sinon $R_i[x,y] = R[x,y]$)

  Alors $Q(F) \geq \dfrac{\|R\|}{\max_i \|R_i\|}$



Autres méthodes

- De multiples méthodes toutes équivalentes [Laplante, Lee, Szegedy 2005]
- Jusqu'à 2007 !

  où des poids négatifs sont introduits ! [Høyer, Lee, Spalek 2007]

Poids négatifs [Høyer, Lee, Spalek 2007]

- R : matrice de taille $2^N \times 2^N$ telle que

  $R[x,y] = 0$ quand $F(x) = F(y)$

  $R_i[x,y] = 0$ quand $x_i = y_i$ (et sinon $R_i[x,y] = R[x,y]$)

  Alors $Q(F) \geq \dfrac{\|R\|}{\max_i \|R_i\|}$

Dual ?

- Nouvelle méthode algorithmique !

  Les Span Programs [Karchmer, Wigderson 1993]

  sont solutions du dual de la méthode précédente [Reichardt 2009,11]

  Preuve : A l'aide de marches quantiques (cours 5)

- De nouveaux algorithmes

  Exemple : Toute formule logique read-once à N variables s'évalue quantiquement en $\sqrt{N}$ requêtes (optimal) [Reichardt, Spalek 2008]

- De nouveaux formalismes *intuitifs*

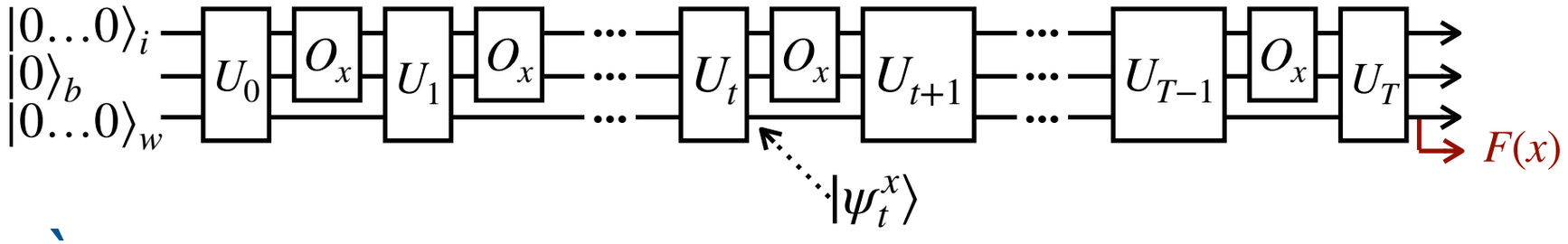
  Learning graphs [Belovs 2012]

  Extended learning graphs [Carette, Laurière, M 2017]

Méthode polynomiale

Circuit

- $C = U_T O_x U_{T-1} O_x \ldots U_1 O_x U_0$, $|\psi_t^x\rangle$: Etat entre U_t et le prochain O_x



Théorème

- Au bout de T requêtes, la probabilité d'observer 1 sur le qubit dédié au résultat est un polynôme p de degré au plus $2T$ en $x_0, x_1, \ldots, x_{N-1}$
- Si l'algorithme calcule F avec erreur ε alors pour tout x : $|p(x) - F(x)| \leq \varepsilon$

Définition

- $\deg_\varepsilon(F)$: plus petit degré des polynôme p t.q. pour tout x : $|p(x) - F(x)| \leq \varepsilon$

Remarques

- Caractérisation déjà étudiée et utilisée pour les algorithmes classiques

  $\deg_0(F) \leq D(F)$ et $\deg_{1/3}(F)/2 \leq Q(F) \leq R(F)$

- $\deg_0(OR_N) = \Theta(\sqrt{N}) = \deg_{1/3}(OR_N)$

Effet d'une requête

- Supposons que l'état est

$$\sum_{i,b,w} \alpha_{i,b,w} |i, b, w\rangle$$

- Après l'appel à O_x l'état devient

$$\sum_{i,b,w} \alpha_{i,b,w} |i, b \oplus x_i, w\rangle = \sum_{i,b,w} \beta_{i,b,w} |i, b, w\rangle$$

avec donc $\beta_{i,b,w} = (1 - x_i)\alpha_{i,b,w} + x_i \alpha_{i,1-b,w}$

Effet d'une transformation unitaire

- Les nouvelles amplitudes $\beta_{i,b,w}$ sont des combinaisons linéaires des anciennes $\alpha_{i,b,w}$. Ces combinaisons sont indépendantes de l'entrée x.

Conclusion

- Au bout de T requêtes, chaque amplitude est un polynôme de degré au plus T en $x_0, x_1, \ldots, x_{N-1}$
- Au bout de T requêtes, la probabilité d'observer 1 sur le qubit dédié au résultat est un polynôme p de degré au plus $2T$
- Si l'algorithme calcule F avec erreur ε alors pour tout x : $|p(x) - F(x)| \leq \varepsilon$

Toutes les constantes multiplicatives sont omises

Relations pour toute fonction totale *F*

- **$D(F) \leq R(F)^3$** [Nisan1989]

  Preuve : $D(F) \leq bs(F)^3$ $bs(F) \leq R(F)$

- $R(F) \leq deg_{1/3}(F)^6$ [Nisan, Szegedy 1992][Beals, Burhman, Cleve, Mosca, Wolf 98]

  Preuve : $D(F) \leq bs(F)^3$ $bs(F) \leq deg_{1/3}(F)^2$

- Conséquence : $Q(F) \leq R(F) \leq D(F) \leq Q^6(F)$

Cas déterministe et degré exact

- $D(F) \leq bs(F)\ deg_0(F)$ [Midrijanis 2004]
- Question : Quel lien entre $deg_0(F)$ et $deg_{1/3}(F)$?

Récents développements - Sensitivity conjecture

- $deg_0(F) \leq s(F)^2$ [Huang 2019]
- Généralisation "spectrale" [Aaronson, Ben-David, Kothari, Rao, Tal 2020]

  $deg_0(F) \leq \lambda(F)^2$ puis $\lambda(F) \leq s(F), Q(F), deg_{1/3}(F)$

- Conséquence :

  $deg_0(F) \leq deg_{1/3}(F)^2$

  $D(F) \leq Q^4(F)$

Cas général (transparent précédent)

- Pour <u>toute</u> fonction F (totale) : $D(F) \leq R(F)^3$ et $D(F) \leq Q^4(F)$

  Question : Ces relations sont-elles optimales ?

Avant 2015

- Meilleure séparation quantique connue

  $D(OR)=R(OR)=Q(OR)^2$ [1995]

- Meilleure séparation probabiliste connue pour un pb de type MIN-MAX

  $D(NAND)=R(NAND)^{1,3267}$ [Saks Wigderson 1986]

Après 2015

- Articles fondateurs [Göös, Pitassi, Watson 2015] [Ambainis, Balodis, Belovs, Lee, Santha, and Smotrovs 2016]

  Relient la complexité des fonctions partielles (séparation exponentielle) aux fonctions totales (séparation polynomiale)

- Constructions <u>explicites</u> de fonctions F totales telles que

  $D(F) \leq R(F)^2$

  $D(F) \leq Q(F)^4$

  $R(F) \leq Q(F)^3$ [Tal 2020][Sherstov, Storozhenko, Wu 2020]

Articles

- Complexity-Theoretic Foundations of Quantum Supremacy Experiments [Aaronson, Chen 2017]
- What Limits the Simulation of Quantum Computers? [Zhou, Stoudenmire, Waintal 2020]
- The quantum adversary method and classical formula size lower bounds [Laplante, Lee, Szegedy 2005]
- Negative weights make adversaries stronger [Høyer, Lee, Spalek 2007]
- Reflections for quantum query algorithms [Reichardt 2011]
- Separations in query complexity based on pointer functions [Ambainis, Balodis, Belovs, Lee, Santha, and Smotrovs 2016]
- Degree vs. Approximate Degree and Quantum Implications of Huang's Sensitivity Theorem [Aaronson, Ben-David, Kothari, Rao, Tal 2020]

Séminaire du cours !

- Suprématie quantique : où en sommes-nous aujourd'hui ?

  avec André Chailloux, Inria, Paris