Informatique Quantique

Frédéric Magniez

Cours 5 :
Limitations du calcul classique et quantique

Montrer qu'un algorithme est optimal

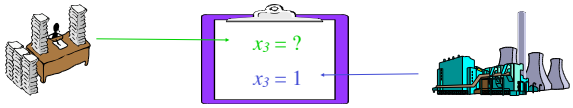
- Résultats connus
  - P-TIME ≠ EXP-TIME
  - LINEAR-TIME ≠ QUADRATIC-TIME
- Plus difficile, mais faisable
  - Trouver un problème dans EXP-TIME, mais pas dans P-TIME
- Pour le moment infaisable
  - Montrer que Factorisation, Isomorphisme de graphes ne sont pas dans P-TIME
  - Plus généralement, montrer que P ≠ NP
  - Montrer que la multiplication de matrices est au moins en $n^{2(1+\epsilon)}$

Difficulté illustrée sur l'algorithme de tri

- Entrée : Tableau X de n valeurs numériques (prises dans $1, 2, ..., m$)
- Sortie : Tableau Y ayant les mêmes valeurs que X, mais triées
- Accès aux valeurs : algorithme en temps $n + m$
- Accès uniquement aux comparaisons : algorithme en temps $n \log n$

Conclusion : Nécessité de modéliser l'accès à l'entrée

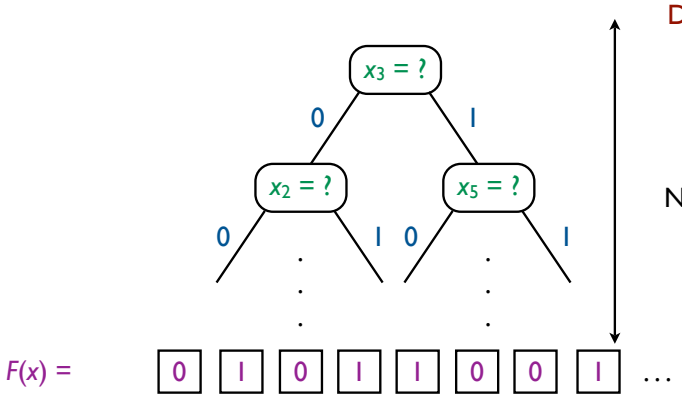
Modèle de requêtes



Définition

- Accès à l'entrée x par oracle
- Autres ressources (temps, espace, ...) infinies
- Complexité en requêtes d'un algo = nb d'accès à l'oracle ds le pire cas
- Complexité en requêtes de F = meilleur complexité en requêtes d'un algo calculant F

Cas déterministe : arbre de décision



Deterministic Query Complexity

Profondeur
=
Nombre de requêtes
dans le pire cas

Borne inférieure par adversaire

Fonction OR

- Entrée : $x \in \{0,1\}^n$
- Accès : $i \longrightarrow x_i$

Théorème

- DQC(OR) = n

Preuve par *adversaire*

- Fixons un arbre T qui calcule OR
- Soit σ le chemin de la racine vers une feuille tel que toutes les réponses sont 0
- Si σ est de longueur $< n$, il existe un bit x_i non interrogé le long de σ
- Le même chemin, et donc la même feuille est atteinte que $x_i=0$ ou $x_i=1$
- Contradiction : OR $(0^n)= 0$ et OR$(0^{i-1}10^{n-i})=1$

Borne inférieure pour le tri

Problème revu

- Entrée : Tableau X de n valeurs numériques
- Sortie : Tableau Y = Tableau X trié
- Requête : $x_i < x_j$?

Théorème

- DQC (Tri) $\geq n \log n$

Preuve (exercice)

- Fixer un arbre T calculant Y
- Soit π la permutation qui trie le tableau
- Montrer qu'un chemin code la permutation π
- En déduire le nombre de feuilles de T
- En déduire la profondeur de T et le résultat

Arbre de décision probabiliste

Randomized Query Complexity

Définition

- Un arbre de décision probabiliste calculant F est une distribution probabiliste d'arbres de décision qui calcule F avec une probabilité d'erreur $\leq \epsilon$ ($= 1/8$)

Interprétation

- Les tirages au sort sont effectués avant le calcul, puis le calcul est déterministe

Théorème (Min-Max)

- RQC(F) $\geq 1/2 \times$ Max (**D**QC des arbres calculant F avec erreur $\leq 2\epsilon$ selon π)

  π : distribution sur les entrées

Théorème : RQC(OR) $\geq n/2$ ($\epsilon = 1/8$)

Preuve par adversaire probabiliste

- Soit π telle que 0^n est obtenu avec proba $1/3$ sinon distribution uniforme.
- Soit T un arbre déterministe calculant OR avec erreur $\leq 1/4$ selon π
- Nécessairement T s'évalue à 0 sur 0^n
- Soit σ le chemin de la racine vers une feuille tel que toutes les réponses sont 0
- Si σ est de longueur $< n/2$, plus de $n/2$ bits ne sont pas interrogés le long de σ
- T s'évalue identiquement sur 0^n ainsi que sur les chaînes correspondant aux modifications des bits non interrogés. Donc erreur $\geq 2/3 \times 1/2 = 1/3$

Arbre de décision quantique

Quantum Query Complexity

Modèle de circuits

- L'accès à l'oracle x est modélisé par U_f où

  f est la fonction *requêtes* (exemple $f(i)=x_i$)
- Complexité en requêtes d'un circuit quantique

  = nb de portes U_f utilisées par le circuit quantique
- QQC(F) = meilleur complexité en requêtes d'un circuit quantique calculant F avec erreur $\leq \epsilon$

Remarques

- Pas de notion d'arbres
- Pas de théorème Min-Max *naturel*

Optimalité de l'algorithme de Grover

Modélisation

- Soit U un circuit qui résout le problème de Grover avec erreur ε

$$U = U_T f_\oplus \dots U_2 f_\oplus U_1 f_\oplus U_0$$

- Soit $|\psi_t^i\rangle$ l'état du circuit après la t-ème question à f_i, où

$$f_i : \{1, \dots, N\} \to \{0,1\},\ x \mapsto \begin{cases} 1, & x = i \\ 0, & x \neq i \end{cases} \qquad i = 1, \dots, N$$

$$f_0 \equiv 0$$

- La réponse est soit la solution i soit "pas de solution", cas f_0. Il faut donc adapter l'algorithme de Grover en vérifiant à la fin que la solution donnée est correcte

Mesure du progrès

$$W_t = \sum_{i=1}^{N} \langle \psi_t^0 | \psi_t^i \rangle$$

Condition initiale

$$W_0 = N$$

Condition finale

- Les états finaux $|\psi_T^0\rangle$ et $|\psi_T^i\rangle$ sont quasi-orthogonaux :

$$|\langle\psi_T^0|\psi_T^i\rangle| \leq 2\sqrt{\varepsilon(1-\varepsilon)} \implies |W_T| \leq 2N\sqrt{\varepsilon(1-\varepsilon)}$$

Exercice :Vérifier cette majoration

Majoration des sauts

- Les applications unitaires ne comptent pas :

$$\langle\psi_t^0|\psi_t^i\rangle = \langle\psi_t^0 U|U\psi_t^i\rangle$$

- Influence des questions.

$$\begin{aligned} |\langle\psi_t^0|\psi_t^i\rangle - \langle\psi_{t+1}^0|\psi_{t+1}^i\rangle| &= |\langle\psi_t^0|\psi_t^i\rangle - \langle\psi_t^0|U_{f_i}|\psi_t^i\rangle| \\ &\leq |\langle\psi_t^0|P_i|\psi_t^i\rangle\rangle| + |\langle\psi_t^0|P_i U_{f_i}|\psi_t^i\rangle\rangle| \\ &\leq 2\|P_i|\psi_t^0\rangle\| \end{aligned}$$

Exercice :Vérifier cette majoration

- Au total :

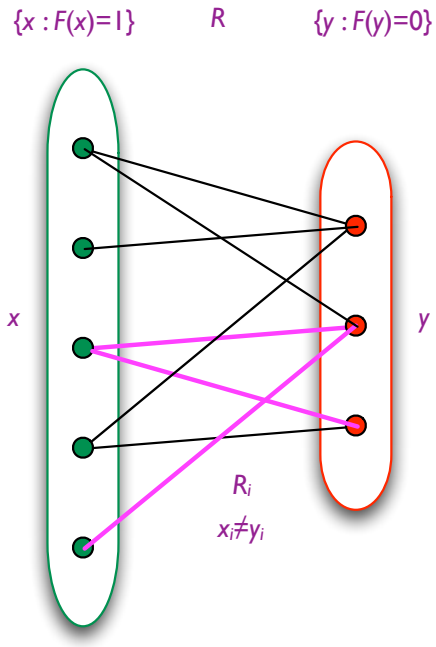
$$|W_t - W_{t+1}| \leq \sum_{i=1}^{N} 2\|P_i|\psi_t^0\rangle\| \leq 2\sqrt{N}\sqrt{\sum_{i=1}^{N}\|P_i|\psi_t^0\rangle\|^2} = 2\sqrt{N}$$

Conclusion

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

Hypothèses

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



Conséquencs

- $|R| \geq m|X|, m'|Y|$
- $|R_i| \leq l|X|, l'|Y|$

Résultats

$$\mathrm{QQC}(F) = \Omega\left(\sqrt{\frac{mm'}{ll'}}\right)$$

$$\mathrm{RQC}(F) = \Omega\left(\max\left(\frac{m}{l}, \frac{m'}{l'}\right)\right)$$

Schéma de la preuve (à compléter en exercice)

Etat du système

- étape t, entrée x : $|\psi_t^x\rangle$

Contraintes du modèle de calcul

- FIXONS (x,y) dans R
- Au début : $\langle\psi_0^x|\psi_0^y\rangle = 1$
- A chaque étape : $|\langle\psi_t^x|\psi_t^y\rangle - \langle\psi_{t+1}^x|\psi_{t+1}^y\rangle| \leq 2 \sum_{i:x_i\neq y_i} \sqrt{p_t^x(i)p_t^y(i)}$

  Progress$_{t,x,y}$(i)
- A la fin : $|\langle\psi_T^x|\psi_T^y\rangle| \leq 2\sqrt{\varepsilon(1-\varepsilon)}$

$$T \cdot \sum_i 2\sqrt{p_t^x(i)p_t^y(i)} \quad \geq \quad 1-2\sqrt{\varepsilon(1-\varepsilon)}$$

Contraintes combinatoires de la fonction

- Prise en compte de TOUTES les paires (x,y) de R

$$\sum_i Progress_t(i) \leq 2\sqrt{l|X| \cdot l'|Y|}$$

somme de tous les *Progress$_{t,x,y}$(i)* pour *(x,y)* de *R*

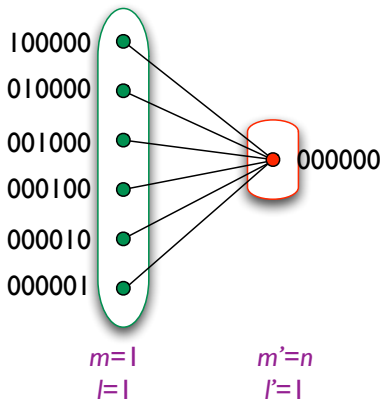
- *|R| ≥ m|X|, m'|Y|* donc ≥ $\sqrt{mm'|X||Y|}$

Conclusion : $T = \Omega\left(\sqrt{\frac{mm'}{ll'}}\right)$

Exemples

Fonction OR

- Complexité quantique $\geq \sqrt{\frac{mm'}{ll'}} = \sqrt{n}$
- Complexité classique ≥ n



Exercice

- Complexité de la fonction XOR ?
- Complexité de la fonction Majorité ?

Recherche dichotomique

Dichotomie

- Entrée : $x \in \{0,1\}^n$ tel que $x = 00...011...1$
- Sortie : $D(x) = \min (i : x_i = 1)$ et $n+1$ si non défini
- Accès : $i \rightarrow x_i$

Théorème

- QQC(Dichotomie) = $\Omega (\log n)$

Remarque

- La méthode précédente ne donne pas mieux qu'une constante !

Généralisation

- QQC(Tri) = $\Omega (n \log n)$

Idée

- Il faut considérer toutes les paires mais...
- ... certaines paires sont plus difficiles à distinguer

  Les quelles ?
- Il faut donc mettre plus de poids sur ces paires

Adversaires avec poids

Notation

- Poids sur la paire (x,y) : $w_{x,y} = 1/|D(x)-D(y)|$, si $D(x)<D(y)$, et 0 sinon
- Mesure du progrès : $W_t = \sum_{x,y} w_{x,y} \langle \psi_t^x | \psi_t^y \rangle$

Ce qui est inchangé

- Initialement : $W_0 = \Sigma_{x,y}\ 1/|D(x)-D(y)| \approx N \log N$
- A la fin : $|W_T| \leq 2\ (\epsilon(1-\epsilon))^{1/2}\ W_0$

Progrès à chaque étape

- $$W_j - W_{j+1} = \sum_{x,y\in\{0,1\}^N} \omega(x,y)\ \langle \psi_x^j | \psi_y^j \rangle - \sum_{x,y\in\{0,1\}^N} \omega(x,y)\ \langle \psi_x^{j+1} | \psi_y^{j+1} \rangle$$

  $$= 2 \sum_{x,y\in\{0,1\}^N} \sum_{i:x_i\neq y_i} \omega(x,y)\ \langle \psi_x^j | \mathsf{P}_i | \psi_y^j \rangle .$$

- $$\left| W_j - W_{j+1} \right| \leq 2 \sum_{0\leq a<b<N} \sum_{a\leq i<b} \frac{1}{b-a} \beta_{a,i} \beta_{b,i}$$

  $$\beta_{a,i} = \| \mathsf{P}_i | \psi_x^j \rangle \|$$

Analyse du progrès...

- $$\left|W_j - W_{j+1}\right| \leq 2 \sum_{d=1}^{N-1} \sum_{i=0}^{d-1} \frac{1}{d} \left(\sum_{a=0}^{N-d-1} \beta_{a,a+i} \beta_{a+d,a+i} \right)$$

$$|W_j - W_{j+1}| \leq 2 \sum_{d=1}^{N-1} \sum_{i=0}^{d-1} \frac{1}{d} \gamma_i \delta_{d-i-1}$$

$$\gamma_i = \left(\sum_{a=0}^{N-1} \beta_{a,a+i}^2 \right)^{1/2}$$

$$\delta_i = \left(\sum_{a=0}^{N-1} \beta_{a,a-i-1}^2 \right)^{1/2}$$

$$|W_j - W_{j+1}| \leq 2\gamma K \delta \leq 2 \|\gamma\|_2 \cdot \|K\|_2 \cdot \|\delta\|_2$$

Conclusion

- Considérations techniques

$$\|\gamma\|_2^2 + \|\delta\|_2^2 \leq \sum_{a=0}^{N-1} \sum_{i \geq 0} \beta_{a,i}^2 \leq N$$

$$\|\gamma\|_2 \|\delta\|_2 \leq \frac{1}{2} N$$

$$\|K\|_2 \leq \|L\|_2 = \pi$$

$$(K)_{(k,l)} = \begin{cases} \frac{1}{k+l+1} & \text{if } k+l < N-1 \\ 0 & \text{otherwise} \end{cases}$$

$$\gamma = [\gamma_0, \ldots, \gamma_{N-2}] \quad \delta = [\delta_0, \ldots, \delta_{N-2}]^t$$

$$L = \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \cdots \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & & \\ \frac{1}{3} & \frac{1}{4} & & & \\ \frac{1}{4} & & & & \\ \vdots & & & & \end{bmatrix}.$$

- Au final : $T = \Omega (\log N)$