Complexité de requêtes du problème de collision et de problèmes liés

C. Dürr (LRI - Orsay)

travail avec Harry Buhrman, Mark Heiligman, Peter Høyer, Frédéric Magniez, Miklos Santha, Ronald de Wolf

Trouver de nouveaux algorithmes quantiques

Utiliser de nouveaux opérateurs unitaires

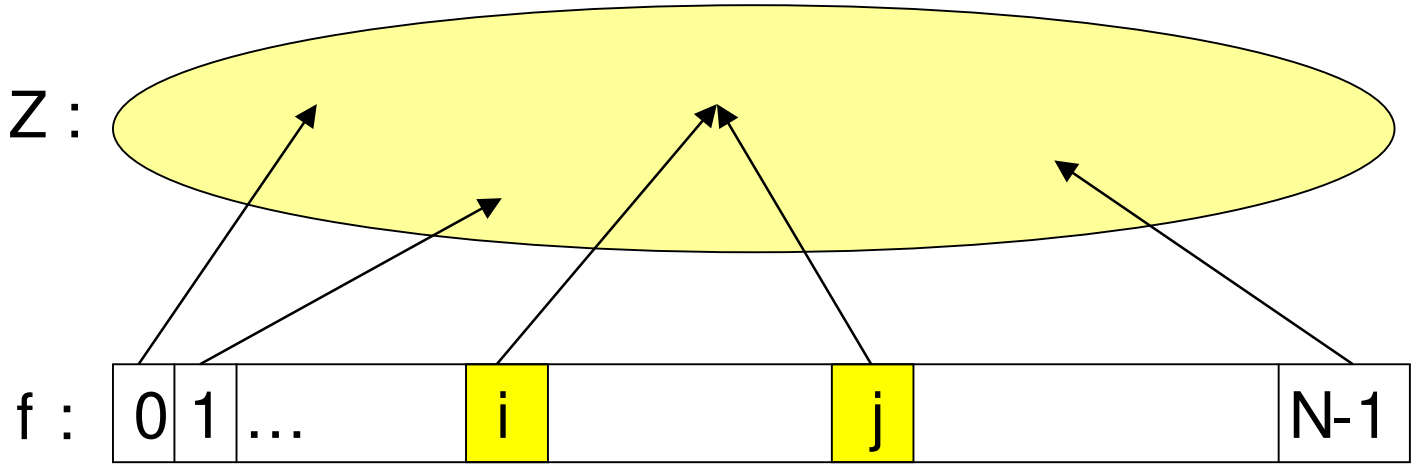
- Transformée de Hadamard
  - Deutsch-Jozsa, Bernstein-Vazirani
- Transformée de Fourier
  - Simon, Shor
- Matrice de Haar
  - Høyer-Neerbek-Shi
- Matrices de Hadamard
  - van Dam

Utiliser les algorithmes quantiques connus

- Shor :
  - Problème de sous-groupe caché
- Grover :
  - Recherche du minimum, Problème de collision, Recherche du median

Problème de collision

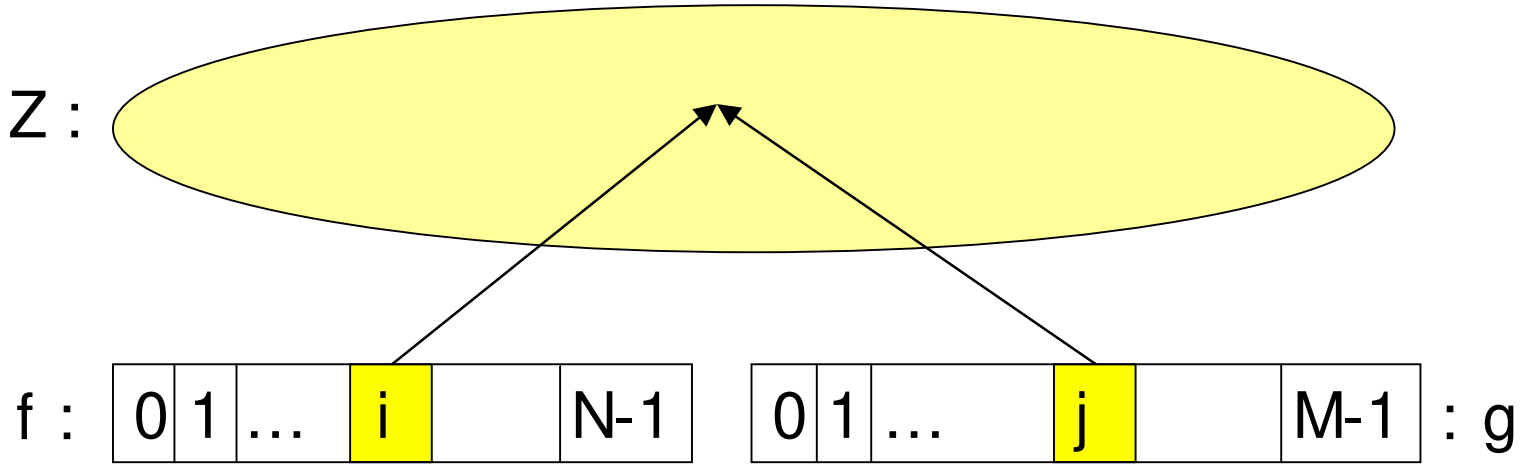
Entrée : $f:[N] \rightarrow Z$



Chercher : $i,j \in [N]$ tel que $f(i)=f(j)$, $i \neq j$

Problème d'intersection

Entrée : $f:[N]\rightarrow Z$ $g:[M]\rightarrow Z$



Chercher : $i\in[N]$, $j\in[M]$ tel que $f(i)=g(j)$

Modèles de complexité

Modèle de requêtes

On compte le nombre d'appels à f ou g

Modèle de comparaisons

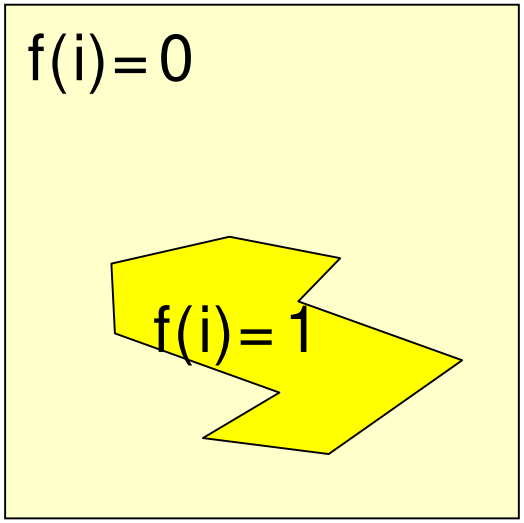
On ne peut pas lire directement f ou g

Seuls des comparaisons $f(i)<f(j)$, $g(i)<g(j)$, $f(i)<g(j)$ sont possibles et comptées

Aucune hypothèse n'est faite sur Z, sauf qu'il est muni d'un ordre

Outil recherche quantique

Entrée: $f:[N] \rightarrow \{0,1\}$



[Grover]

Trouver (avec proba ½): $i \in [N]$, tel que $f(i)=1$ en appelant f $O(N^{1/2})$ fois

Complexité classique/quantique

Rechercher $z \in Z$ dans $f:[N] \to Z$

cas général (f n'est pas forcément triée)

$\Theta(N)$, $\Theta(N^{1/2})$ [Grover]

cas f triée

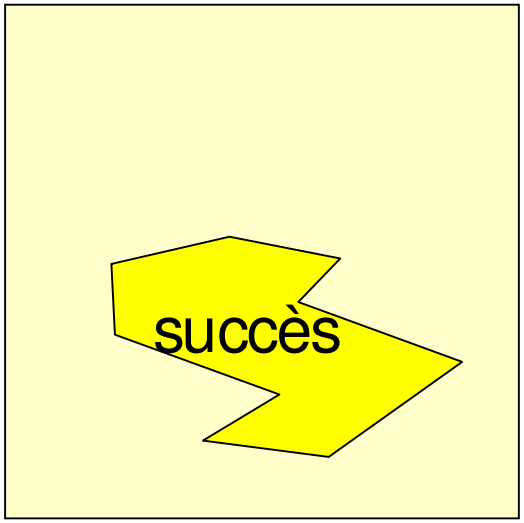
$\Theta(\log N)$, $\Theta(\log N)$

0.53 log N par [Fahri,Goldstein,Gutman,Sipser]

$\log_3 N + O(1)$ par [Høyer,Neerbek,Shi]

Outil amplification quantique

Entrée : Algorithme A avec probabilité de succès p



[Brassard,Høyer,Mosca,Tapp]

Répéter $O(p^{-1/2})$ fois A

pour probabilité de succès ½

Borne inférieure par réduction

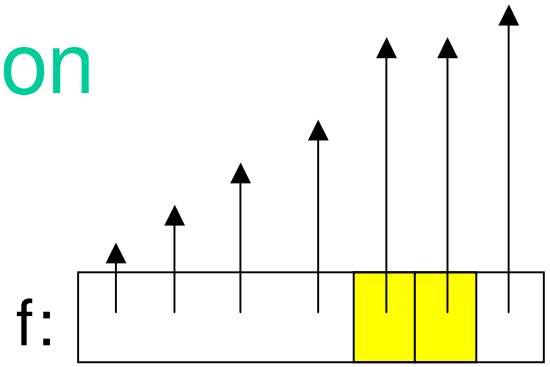
Problème de recherche

pour $h:[N]\rightarrow\{0,1\}$ trouver i tel que $h(i)=1$

$\Omega(N^{1/2})$ [Bennet,Bernstein,Brassard,Vazirani]

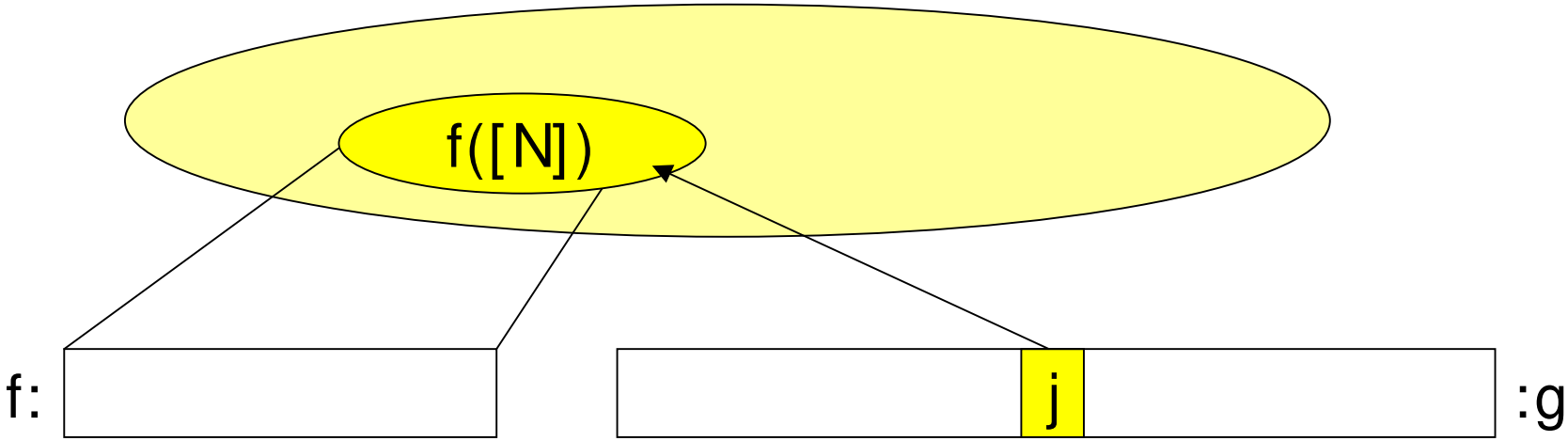
Problème de collision

$f: i \rightarrow i+h(i)$



Donc le problème de collision est $\Omega(N^{1/2})$

Intersection: cas f trié ...et N<M



Chercher $j \in [M]$ tel que $g(j) \in f([N])$

ce test coûte log(N)

Cette recherche coûte $\sqrt{M}$ tests

Coût total $O(\sqrt{M} \log(N))$

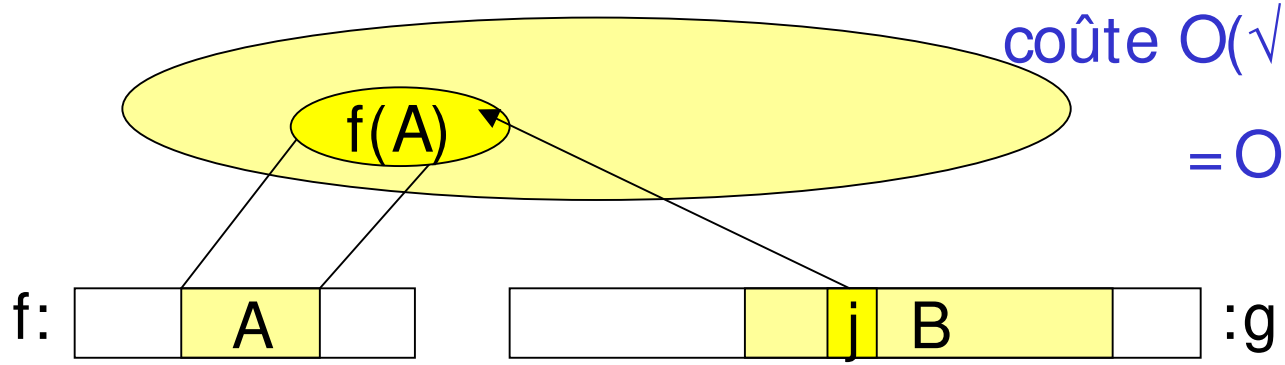
Intersection: cas général

Trouver une intersection entre f et g

– Chercher $A \subset [N]$, $|A| = k$
et $B \subset [M]$, $|B| = k^2$ tel que $f(A) \cap g(B) \neq \{\}$

coûte $O(\sqrt{(MN/k^3)}\ k \log k)$

$= O(\sqrt{(MN/k)} \log k)$



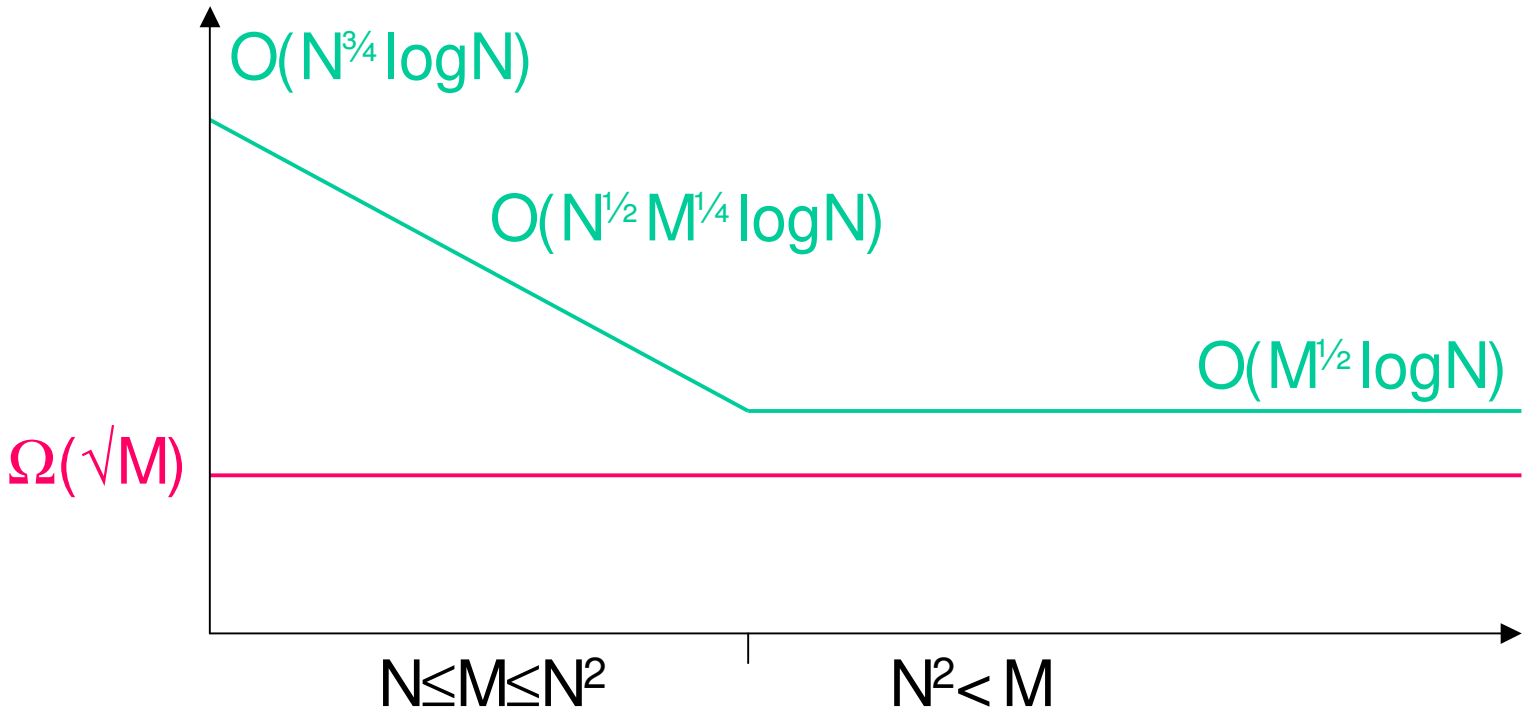
Trouver une intersection entre f(A) et g(B)

– Trier f(A) coûte $O(k \log k)$

– Chercher $j \in B$ tel que $g(j) \in f(A)$ coûte $O(\sqrt{k^2} \log k)$

Complexité

Meilleur choix de k avec $k \leq \min(N, \sqrt{M})$



Intersection: cas f et g triées

… et N=M

Application possible

Question à google.com “Calcul quantique”

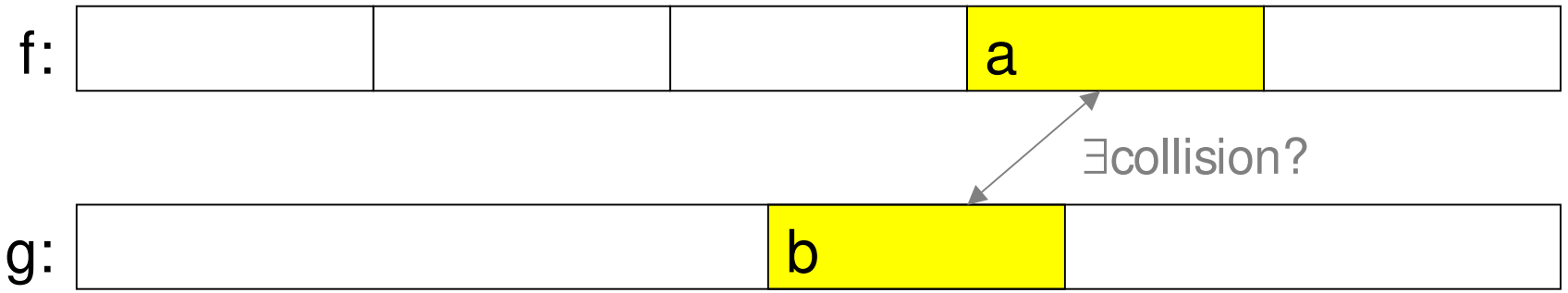
Réponse: éléments en commun de tableaux précalculées et triées (une par mot clé)

```
f:  4  7  8   12 15    21   22        27 29   32 34
g:   5   8 11    26        22      26         32
```

Sous-problème

f est découpé en blocs de taille r $0 \leq i \leq \lceil N/r \rceil$

f_i : restriction de f au i-ième bloc



g'_i : restriction de g au bloc de taille r,
commençant au premier b, tq $g(b) \geq f(a)$

Sous-problèmes (f'_i, g_i) définis pareillement

Algorithme

Le problème initial a une solution si et seulement si un parmi les 2N/r sous-problèmes a une solution (“est positif”)

- Recherche quantiquement un sous-problème positif
- Appliquer récursivement cet algorithme aux sous-problèmes

Complexité T(N)

pour des constantes c',c''

$$T(N) \leq c'(N/r)^{1/2}(\log(N+1)+T(r))$$

Appel récursif

Recherche binaire du début de bloc

Recherche quantique d'un sous-problème

Choisir $r=\log^2(N)$

$$T(N) \leq c'' (N/r)^{1/2}\ T(r)$$

Complexité

pour une constante c

$$T(N) = O(N^{1/2} c^{\log^*(N)})$$

Logarithme itéré

$\log^{(i)}(x) = \log \log \ldots \log (x)$

$\log^*(x) = \min\{ i \geq 0 : \log^{(i)}(x) \leq 1 \}$

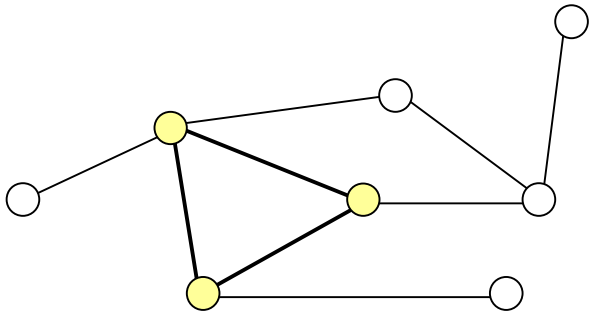
Fonction presque constante

$c^{\log^*(N)} = o(\log^{(i)}(N))$ pour tout i

Recherche de triangles

Entrée : graphe $G(V,E)$, $n=|V|$, $m=|E|$

Trouver : $a,b,c \in V$ tel que
$(a,b), (b,c), (c,a) \in E$



Recherche naïve

Recherche quantique sur $(a,b,c) \in V^3$

Complexité de requêtes $O(n^{3/2})$

Pour graphes épars

… $m = o(n^2)$

- Recherche quantique d'une arête $(a,b) \in E$

  $O(m^{1/2})$ requêtes

- Recherche quantique d'un 3-ième sommet c tel que (b,c), $(c,a) \in E$

  $O(n^{1/2})$ requêtes

- Amplifier quantiquement la probabilité de succès

  $O(m^{1/2})$ répétitions

Au total $O(n+(nm)^{1/2})$

Récapitulatif classique/quantique

Collision dans f 2-to-1 $(\forall i\ \exists! j\ f(i)=f(j))$

$\Theta(N^{1/2})$, $O(N^{1/3})$ [Brassard,Høyer,Tapp]

Collision dans f

$\Theta(N)$, $O(N^{3/4}\log N)$, $\Omega(N^{1/2}\log N)$ [Høyer,Neerbek,Shi]

Intersection entre f et g triées

$\Theta(N)$, $O(N^{1/2}c^{\log^*(N)})$

Triangles

$\Theta(n^2)$, $O(n+(nm)^{1/2})$

Problèmes difficiles

… même quantiquement $\Omega(N)$

Pour $f : [N] \to Z$

Parité des collisions

trouver la parité du nombre de i,j ($i<j$) tel que $f(i)=f(j)$

Sans collision

trouver i qui n'est pas en collision avec un j

Hors image

trouver $z \in Z$ tel que z n'est pas dans l'image de f

Directions futures

Trouver une borne inférieure pour le problème de collision dans f 2-to-1

Fermer le fossé entre les deux bornes pour le problème de collision

Dans le modèle de requêtes, utiliser le fait que pour $f : [N] \rightarrow [N]$

$$\sum_j \lambda^{f(j)} \text{ avec } \lambda = e^{2\pi i/N}$$

est 0 pour f sans collision et
diff. de 0 pour f avec une unique collision