Informatique quantique IFT6155

Algorithme de Grover

et

applications

NP

Un langage L est dans **NP** s'il existe un algorithme en temps polynomial F tel que

$$\forall w \in L, \exists x, F(w, x) = 1$$

$$\forall w \notin L, \forall x, F(w, x) = 0$$

En général on est intéressé à savoir si un mot appartient au langage mais aussi à trouver w tel que $F(w, x) = 1$.

Exemples de problèmes dans NP

Premier: Dire si un nombre est premier.

Composé: Dire si un nombre est composé.

Horaire: Étant donné un ensemble de contraintes vérifiables efficacement, existe-t-il un horaire satisfaisant les contraintes?

Voyageur de commerce:
Étant donné un budget et une matrice de coût pour voyager entre n villes, existe-t-il un circuit parcourant une et une seule fois chaque ville et respectant le budget?

Partout, "existe-t-il" peut être remplacé par "trouver".

Exemples de problèmes dans NP

Sac à dos: Étant donné une liste d'objets L avec leurs poids et leurs valeurs ainsi qu'une capacité maximale c pour le sac à dos, est-il possible de mettre dans le sac un sous-ensemble des objects ayant pour valeur totale au moins v?

Cryptographie Étant donnés un algorithme d'encryption E, un message encrypté m' et une fonction F facile à calculer, existe-t-il m tel que $m' = E(M)$ et $F(m) = 1$?

Satisfiabilité: Étant donnée une expression booléene E, existe-t-il une affectation aux variables x_i telle que $E(x_1, \ldots, x_n) = 1$?

Partout, "existe-t-il" peut être remplacé par "trouver".

Problème de fouille

Chercher dans une base de données

Étant donné un tableau T et une entrée y,
trouver i tel que $T[i] = y$.

Recherche satisfaisant aux contraintes

Étant donnée une fonction booléene $F : X \rightarrow \{0, 1\}$
trouvez i tel que $F(i) = 1$.

Note: Le lien avec **NP** est clair.

Algorithme de Grover[Gr96]

Grover(F, m)

1. $|\Psi\rangle \leftarrow H\,|0\rangle$

2. Faire m fois
   $|\Psi\rangle \leftarrow G_F\,|\Psi\rangle$

3. Retourne: Mesure $|\Psi\rangle$.

Itération de Grover [Gr96]

$$\boxed{G_F = -HS_0HS_F}$$

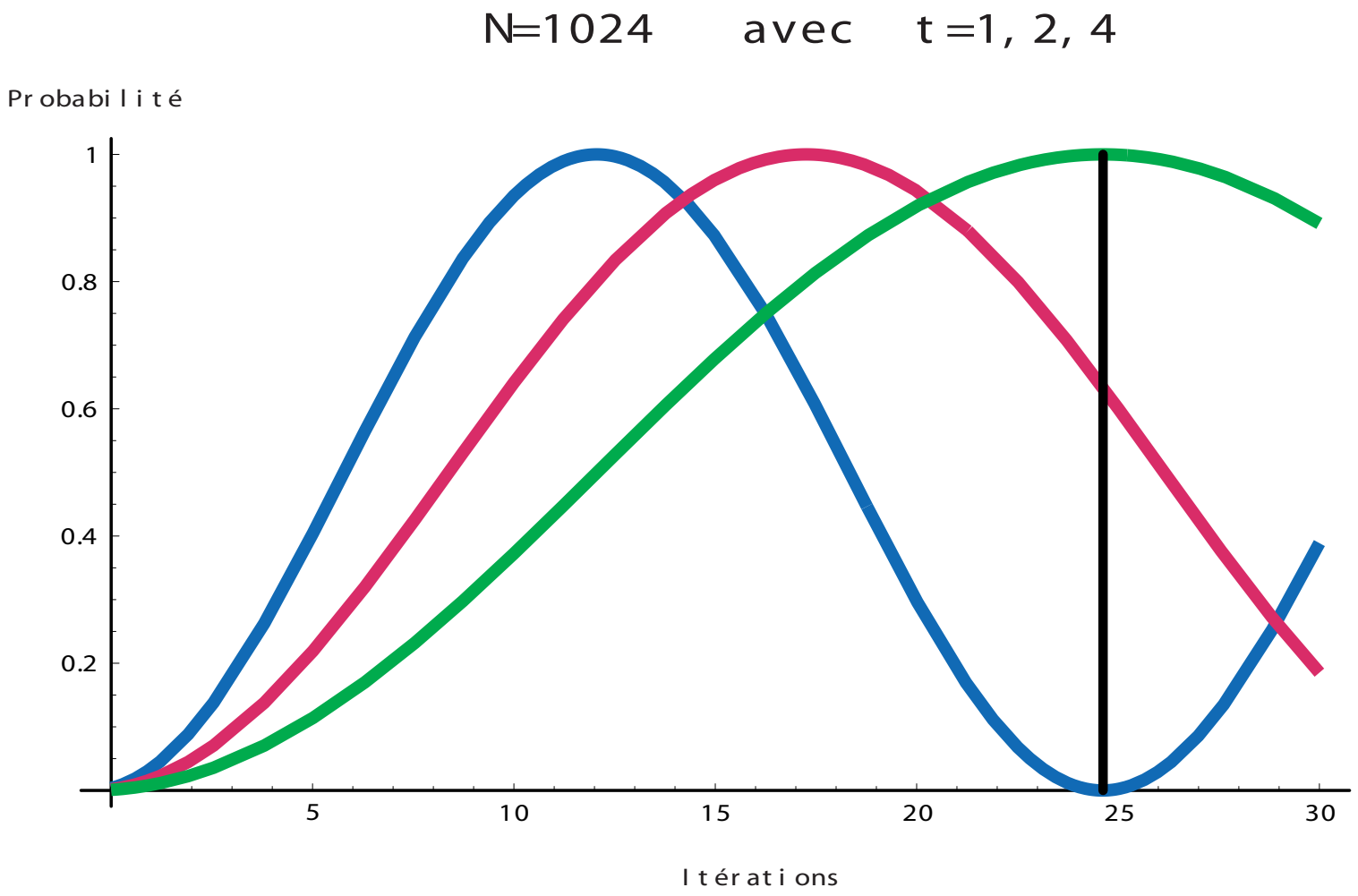
$$S_0 |i\rangle = \begin{cases} -|i\rangle & \text{if } i = 0 \\ |i\rangle & \text{otherwise.} \end{cases}$$

$$S_0 = I - 2|0\rangle\langle 0|$$

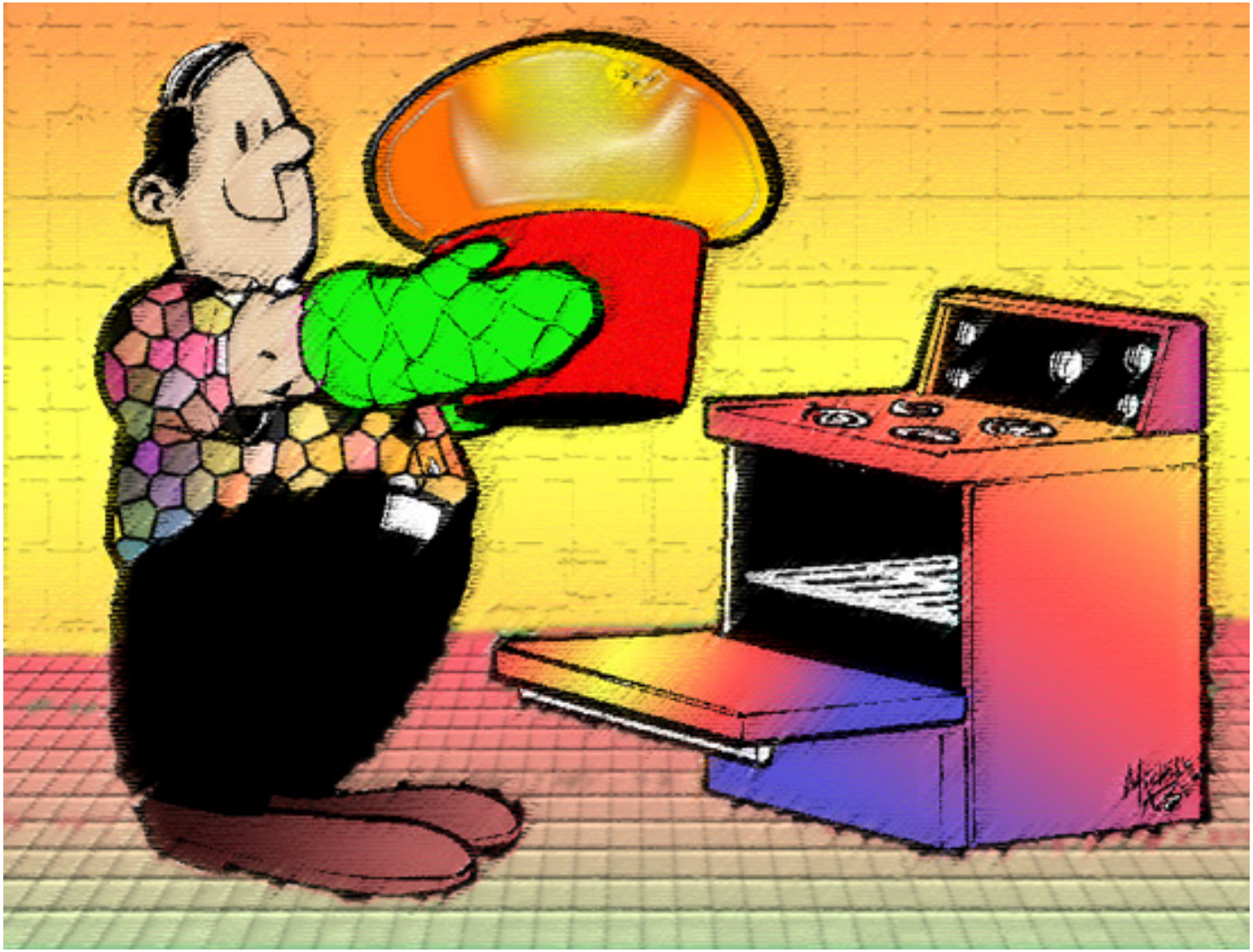
$$S_F |i\rangle = \begin{cases} -|i\rangle & \text{if } F(i) = 1 \\ |i\rangle & \text{otherwise.} \end{cases}$$

$$H^{\otimes n} |j\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{i \cdot j} |i\rangle$$

Probabilité de succès



Soufflé



Sous-espace bidimensionnel

$$N = |X| \qquad t = |\{x \in X | F(x) = 1\}|$$

$$|\Psi_0\rangle = \frac{1}{\sqrt{t}} \sum_{F(x)=0} |x\rangle \qquad |\Psi_1\rangle = \frac{1}{\sqrt{N-t}} \sum_{F(x)=1} |x\rangle$$

$$S_F(\alpha\,|\Psi_0\rangle + \beta\,|\Psi_1\rangle) = \alpha\,|\Psi_0\rangle - \beta\,|\Psi_1\rangle$$

$$H\,|0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in X} |x\rangle = \sqrt{\frac{t}{N}}\,|\Psi_1\rangle + \sqrt{\frac{N-t}{N}}\,|\Psi_0\rangle$$

Sous-espace bidimensionnel

HS_0H

$$
\begin{aligned}
&= H(I - 2\left|0\right\rangle\left\langle 0\right|)H \\
&= I - 2\left(\sqrt{\frac{t}{N}}\left|\Psi_1\right\rangle + \sqrt{\frac{N-t}{N}}\left|\Psi_0\right\rangle\right)\left(\sqrt{\frac{t}{N}}\left\langle\Psi_1\right| + \sqrt{\frac{N-t}{N}}\left\langle\Psi_0\right|\right) \\
&= I - \frac{2(N-t)}{N}\left|\Psi_0\right\rangle\left\langle\Psi_0\right| - \frac{2t}{N}\left|\Psi_1\right\rangle\left\langle\Psi_1\right| \\
&\quad -\frac{2\sqrt{(N-t)t}}{N}(\left|\Psi_0\right\rangle\left\langle\Psi_1\right| + \left|\Psi_1\right\rangle\left\langle\Psi_0\right|)
\end{aligned}
$$

Solution générale

Théorème[BHMT98]:
Posons

$$|\Psi_0\rangle = \frac{1}{\sqrt{t}} \sum_{F(x)=0} |x\rangle \quad |\Psi_1\rangle = \frac{1}{\sqrt{N-t}} \sum_{F(x)=1} |x\rangle$$

$$\sin^2\theta = t/N$$

alors pour $m \geq 0$

$$(G_F)^m(H|0\rangle) = \sin((2m+1)\theta)\,|\Psi_1\rangle + \cos((2m+1)\theta)\,|\Psi_0\rangle$$

Preuve:
Par induction sur m.

Base: $m = 0$

$$
\begin{aligned}
&(G_F)^m(H\,|0\rangle) \\
&\qquad = \; (G_F)^0(H\,|0\rangle) \\
&\qquad = \; H\,|0\rangle \\
&\qquad = \; \sqrt{\frac{t}{N}}\,|\Psi_1\rangle + \sqrt{\frac{N-t}{N}}\,|\Psi_0\rangle \\
&\qquad = \; \sqrt{\frac{t}{N}}\,|\Psi_1\rangle + \sqrt{1-\frac{t}{N}}\,|\Psi_0\rangle \\
&\qquad = \; \sin(\theta)\,|\Psi_1\rangle + \sqrt{1-\sin^2(\theta))}\,|\Psi_0\rangle \\
&\qquad = \; \sin(\theta)\,|\Psi_1\rangle + \cos(\theta)\,|\Psi_0\rangle \\
&\qquad = \; \sin((2m+1)\theta)\,|\Psi_1\rangle + \cos((2m+1)\theta)\,|\Psi_0\rangle
\end{aligned}
$$

En général

$$
\begin{aligned}
& G_F\ (\alpha\,|\Psi_0\rangle + \beta\,|\Psi_1\rangle) \\
&\quad = \quad -HS_0HS_F\ (\alpha\,|\Psi_1\rangle + \beta\,|\Psi_0\rangle) \\
&\quad = \quad HS_0H\ (\alpha\,|\Psi_1\rangle - \beta\,|\Psi_0\rangle) \\
&\quad = \quad \Big(I - \frac{2(N-t)}{N}\,|\Psi_0\rangle\,\langle\Psi_0| - \frac{2t}{N}\,|\Psi_1\rangle\,\langle\Psi_1| \\
&\qquad -\frac{2\sqrt{(N-t)t}}{N}(|\Psi_0\rangle\,\langle\Psi_1| + |\Psi_1\rangle\,\langle\Psi_0|)\Big) \\
&\qquad (\alpha\,|\Psi_1\rangle - \beta\,|\Psi_0\rangle) \\
&\quad = \quad \left(\alpha - \alpha\frac{2t}{N} + \beta\frac{2\sqrt{(N-t)t}}{N}\right)|\Psi_1\rangle \\
&\qquad + \left(-\beta + \beta\frac{2(N-t)}{N} - \alpha\frac{2\sqrt{(N-t)t}}{N}\right)|\Psi_0\rangle \\
&\quad = \quad \left(\alpha\left(1 - \frac{2t}{N}\right) + \beta\frac{2\sqrt{(N-t)t}}{N}\right)|\Psi_1\rangle + \left(\beta\left(1 - \frac{2t}{N}\right) - \alpha\frac{2\sqrt{(N-t)t}}{N}\right)|\Psi_0\rangle
\end{aligned}
$$

En général

$$\sin^2(\theta) = \frac{t}{N}$$

$$
\begin{aligned}
& G_F\ (\alpha\,|\Psi_0\rangle + \beta\,|\Psi_1\rangle) \\
&= \left(\alpha\left(1-\frac{2t}{N}\right)+\beta\frac{2\sqrt{(N-t)t}}{N}\right)|\Psi_1\rangle \\
&\quad + \left(\beta\left(1-\frac{2t}{N}\right)-\alpha\frac{2\sqrt{(N-t)t}}{N}\right)|\Psi_0\rangle \\
&= \left(\alpha\left(1-2\frac{t}{N}\right)+\beta 2\sqrt{\frac{t}{N}-\frac{t^2}{N^2}}\right)|\Psi_1\rangle \\
&\quad + \left(\beta\left(1-2\frac{t}{N}\right)-\alpha 2\sqrt{\frac{t}{N}-\frac{t^2}{N^2}}\right)|\Psi_0\rangle \\
&= \left(\alpha\cos(2\theta)+\beta 2\sqrt{\sin^2(\theta)-\sin^4(\theta)}\right)|\Psi_1\rangle \\
&\quad + \left(\beta\cos(2\theta)-\alpha 2\sqrt{\sin^2(\theta)-\sin^4(\theta)}\right)|\Psi_0\rangle \\
&= (\alpha\cos(2\theta)+\beta\sin(2\theta))\,|\Psi_1\rangle + (\beta\cos(2\theta)-\alpha\sin(2\theta))\,|\Psi_0\rangle
\end{aligned}
$$

Pas d'induction

$$
\begin{aligned}
& G_F^{m+1}\ (H\,|0\rangle) \\
&\quad = \ G_F G_F^m\ (H\,|0\rangle) \\
&\quad = \ G_F(\sin((2m+1)\theta)\,|\Psi_1\rangle + \cos((2m+1)\theta)\,|\Psi_0\rangle) \\
&\quad = \ (\sin((2m+1)\theta)\cos(2\theta) + \cos((2m+1)\theta)\sin(2\theta))\,|\Psi_1\rangle \\
&\qquad + (\cos((2m+1)\theta)\cos(2\theta) - \sin((2m+1)\theta)\sin(2\theta))\,|\Psi_0\rangle \\
&\quad = \ \sin((2m+1)\theta + 2\theta)\,|\Psi_1\rangle + \cos((2m+1)\theta + 2\theta)\,|\Psi_0\rangle \\
&\quad = \ \sin((2(m+1)+1)\theta)\,|\Psi_1\rangle + \cos((2(m+1)+1)\theta)\,|\Psi_0\rangle
\end{aligned}
$$

Quand t est connu

Théorème: Si

$$m \;=\; \lfloor \frac{\pi}{4 \arcsin\left(\sqrt{t/N}\right)} \rfloor \leq \frac{\pi}{4}\sqrt{\frac{N}{t}}$$

Grover(F, m) retourne x tel que $F(x) = 1$ avec probabilité au moins $\frac{N-t}{N}$.

Preuve: Par le théorème précédent la probabilité de succès est maximale quand $\tilde{m} = (\pi - 2\theta)/4\theta$ ($\cos((2\tilde{m}+1)\theta) = 0$). Prenons $m = \lfloor \frac{\pi}{4\theta} \rfloor$ alors $|m - \tilde{m}| \leq 1/2$ et $|(2m+1)\theta - (2\tilde{m}+1)\theta| \leq \theta$ et donc $|\cos((2m+1)\theta)| \leq |\sin(\theta)|$.
Finalement $\cos((2m+1)\theta)^2 \leq \sin(\theta)^2 = t/N$.

Exercice: Qu'arrive-t-il quand $t = N/4$?

Quand t est inconnu

Théorème: Si $0 < t < 3N/4$ alors l'algorithme **Search** trouve x tel que $F(x) = 1$ en temps espéré $O(\sqrt{N/t})$.

Search(F)

1. $m = 1, \lambda = 8/7$
2. $j \in_R \{0, \ldots, m-1\}$
3. $x =$**Grover**(F, j)
4. Si $F(x) = 1$ retourner x et arrêt
5. $m = min(\lambda m, \sqrt{N})$
6. aller à 2.

Note: Le cas $t \geq 3N/4$ peut être résolu par échantillonnage et le cas $t = 0$ en ajoutant un temps maximal de $O(\sqrt{N})$.

Preuve: t est inconnu

Posons $0 < \theta < \pi/2$ tel que $\sin^2\theta = t/N$.

Lemma:
Soit m un entier, $j \in_R \{0, \ldots, m-1\}$ et $x =$*Grover*(F, j) alors la probabilité que $F(x) = 1$ est

$$P_m \;=\; \frac{1}{2} - \frac{\sin(4m\theta)}{4m\sin(2\theta)}\,.$$

En particulier $P_m \geq 1/4$ when $m \geq 1/\sin(2\theta)$.

Preuve: t est inconnu

Preuve:

$$\begin{aligned} P_m &= \sum_{j=0}^{m-1} \frac{1}{m} \sin^2((2j+1)\theta) \\ &= \frac{1}{2m} \sum_{j=0}^{m-1} 1 - \cos((2j+1)2\theta) \\ &= \frac{1}{2} - \frac{\sin(4m\theta)}{4m\sin(2\theta)}. \end{aligned}$$

Si $m \geq 1/\sin(2\theta)$ alors

$$\frac{\sin(4m\theta)}{4m\sin(2\theta)} \leq \frac{1}{4m\sin(2\theta)} \leq \frac{1}{4}.$$

Preuve: t est inconnu

$$m_0 = 1/\sin(2\theta) = \frac{N}{2\sqrt{(N-t)t}} < \sqrt{\frac{N}{t}}$$

$$s_0 = \lceil \log_\lambda m_0 \rceil$$

On a donc que $m \leq m_0$ les s_0 premières itérations et $m > m_0$ après. Le nombre d'appels à F avant que $m > m_0$ est donné par

$$\frac{1}{2}\sum_{s=1}^{s_0} \lambda^{s-1} < \frac{1}{2}\frac{\lambda}{\lambda - 1} m_0 = 4m_0\,.$$

Preuve: t est inconnu

Une fois que $m > m_0$ chaque tentative réussit avec probabilité au moins 1/4 donc le nombre d'appels espéré est borné par

$$\frac{1}{2}\sum_{u=0}^{\infty}\frac{3^u}{4^{u+1}}\lambda^{u+s_0} < \frac{\lambda}{8-6\lambda}m_0 = \frac{3}{2}m_0\,.$$

donc

$$4m_0 + 4m_0 = 8m_0 = 8\frac{N}{2\sqrt{(N-t)t}} < \frac{1}{4}\sqrt{\frac{N}{t}}$$

Minimum

Théorème: L'algorithme **Minimum** trouve x_0 tel que $\forall x,\ T(x) \geq T(x_0)$, avec probabilité au moins 1/2, en faisant un nombre espéré de $O(\sqrt{N})$ évaluations de T.

Minimum(T)

1. $x_0 \in_R \{0, \ldots, N-1\}$
2. Définir F tel que $F(x) = 1 \Leftrightarrow T(x) < T(x_0)$
3. $x_1 =$**Search**(F)
4. Si $T(x_1) < T(x_0)$ alors $x_0 \leftarrow x_1$
5. Si le nombre total d'évaluations de T est inférieur à $25\sqrt{N}$ aller a l'étape 2
6. Retourner x_0.

Collision

Théorème:Étant donné $G : X \to Y$ une fonction deux-dans-un avec $|X| = N$, l'algorithme **Collision** trouve (x_0, x_1) tel que $G(x_0) = G(x_1)$ en temps et espace $O(\sqrt[3]{N})$.

Collision(G)

1. Pour i de 1 à $\sqrt[3]{N}$, T[i]=(i,G(i)).
2. Trier T et regarder s'il y a collision dans T
3. Définir $F(x) = 1 \Leftrightarrow (x \geq \sqrt[3]{N}$ et $G(x) \in T)$
4. x_0 =**Search**(F), x_1 tel que $G(x_1) = G(x_0)$
5. Retourner (x_0, x_1).

Exemples d'heuristiques

Hill-climbing: recherche locale pour une solution qui accroit la fonction objectif. Parfois très efficace!

Exemple: 3-SAT, trouver une assignation de $\{x_1, x_2, x_3, x_4\}$ qui satisfait chaque clause de

$(\bar{x_1} \vee \bar{x_4} \vee \bar{x_2})(\bar{x_1} \vee x_2 \vee \bar{x_3})(\bar{x_2} \vee \bar{x_4} \vee x_3)$
$(x_1 \vee \bar{x_1} \vee x_4)(x_4 \vee x_3 \vee x_3)(\bar{x_3} \vee \bar{x_4} \vee \bar{x_2})$

On débute avec une assignation aléatoire:
$x_1 = 1,\ x_2 = 1,\ x_3 = 1$ and $x_4 = 1$
qui satisfait 4 clauses
variation locale $x_1 = 0$
satisfait 5 clauses
variation locale $x_2 = 0$
satisfait les 6 clauses!

Heuristiques

Soit $\mathcal{F}$ une famille de fonctions de la forme
$F : X \to \{0, 1\}$ et $\mathcal{D}$ une distribution de probabilité sur cette famille.

Une **heuristique** est une fonction
$G : \mathcal{F} \times R \to X$.

Soit $t_F = |\{x | F(x) = 1\}|$
et $h_F = |\{r | F(G(F, r)) = 1\}|$

Une *bonne* heuristique est telle que

$$E_{\mathcal{F}}\left(\frac{h_F}{|R|}\right) > E_{\mathcal{F}}\left(\frac{t_F}{|N|}\right)$$

Heuristiques

Soit $G'_F(r) = F(G(r, F))$

Algorithme:
Output $G(F,$ **Search**$(G'_F))$

Analyse:
Attention! En général

$$\left(\sum x_i\right)^{1/2} \leq \sum \sqrt{x_i}$$

mais

$$\sum_{F\in\mathcal{F}} \sqrt{\frac{R}{t_F}} P_F = \sum_{F\in\mathcal{F}} \sqrt{\frac{R}{t_F} P_F} \sqrt{P_F} \leq$$

$$\left(\sum_{F\in\mathcal{F}} \frac{R}{t_F} P_F\right)^{1/2} \left(\sum_{F\in\mathcal{F}} P_F\right)^{1/2} = \left(\sum_{F\in\mathcal{F}} \frac{R}{t_F} P_F\right)^{1/2}$$

Références

[Gr96] Lov K. Grover, A fast quantum mechanical algorithm for database search. STOC'96, pages 212-219, 1996.
(quant-ph/9605043)

[BHMT98] Michel Boyer, Gilles Brassard, Peter Høyer and Alain Tapp, Tight Bounds on Quantum Searching, Fortschritte der Physik, vol. 46(4-5), pp. 493-505, 1998.
(quant-ph/9605034)

[BHMT] Gilles Brassard, Peter Høyer, Michele Mosca and Alain Tapp, Quantum Amplitude Amplification and Estimation, in Quantum Computation & Quantum Information Science, AMS Contemporary Math Series,
(quant-ph/0005055)

Références (2)

[DH96] Christoph Dürr and Peter Høyer, A Quantum Algorithm for Finding the Minimum.
(quant-ph/9607014)

[BHT98] Gilles Brassard, Peter Høyer and Alain Tapp, Quantum Algorithm for the Collision Problem, 3rd Latin American Theoretical Informatics Symposium (LATIN'98), Springer-Verlag, LNCS, vol. 1380, pp.163-169, 1998.
(quant-ph/9705002)