Informatique quantique IFT6155

Comptage aproximatif

Comptage approximatif

Soit $F : X \to \{0, 1\}$ avec $|X| = N$ et $|\{x|F(x) = 1\} = t$. Nous savons comment trouver x tel que $F(x) = 1$ avec une accélération quadratique par rapport aux meilleurs algorithmes classiques dans le contexte où F est une boite noire.

Nous allons maintenant étudier un algorithme qui nous permettra d'estimer t.

Itération de Grover

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

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

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

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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

Grover, révision

Nous avons déjà vu que:

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

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

$$k_m = \frac{\sin((2m+1)\theta)}{\sqrt{t}}$$

$$\ell_m = \frac{\cos((2m+1)\theta)}{\sqrt{N-t}}$$

$$(G_F)^m (H|0\rangle) = k_m \sum_{F(x)=1} |x\rangle + \ell_m \sum_{F(x)=0} |x\rangle$$

L'opérateur G_F

$$G_F = -HS_0HS_F$$

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

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

HS_0H

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

Valeurs propres G_F

Regardons les vecteurs propres et les valeurs propres de l'opérateur G_F.

$$|V_1\rangle = \frac{1}{\sqrt{2}}(|\Psi_1\rangle + i\,|\Psi_0\rangle) \quad |V_2\rangle = \frac{1}{\sqrt{2}}(|\Psi_1\rangle - i\,|\Psi_0\rangle)$$

$$G_F\,|V_1\rangle = e^{i2\theta}\,|V_1\rangle \quad G_F\,|V_2\rangle = e^{-i2\theta}\,|V_2\rangle$$

$$G_F^k\,|V_1\rangle = e^{i2k\theta}\,|V_1\rangle \quad G_F^k\,|V_2\rangle = e^{-i2k\theta}\,|V_2\rangle$$

Vérifions la première équation. La deuxième se vérifie de la même façon.

Valeurs propres G_F

$$
\begin{aligned}
G_F\,|V_1\rangle &= -HS_0HS_F\ \frac{1}{\sqrt{2}}(|\Psi_1\rangle + i\,|\Psi_0\rangle) \\
&= HS_0H\ \frac{1}{\sqrt{2}}(|\Psi_1\rangle - i\,|\Psi_0\rangle) \\
&= \frac{1}{\sqrt{2}}\left(1-\frac{2t}{N}+i\frac{2\sqrt{(N-t)t}}{N}\right)|\Psi_1\rangle + \frac{1}{\sqrt{2}}\left(-i+i\frac{2(N-t)}{N}-\frac{2\sqrt{(N-t)t}}{N}\right)|\Psi_0\rangle \\
&= \frac{1}{\sqrt{2}}\left(1+\frac{2t}{N}-i\frac{2\sqrt{(N-t)t}}{N}\right)|\Psi_1\rangle + \frac{i}{\sqrt{2}}\left(-1+\frac{2(N-t)}{N}-i\frac{2\sqrt{(N-t)t}}{N}\right)|\Psi_0\rangle \\
&= \left(1-\frac{2t}{N}+i2\sqrt{\frac{N-t}{n}}\sqrt{\frac{t}{n}}\right)\ \frac{1}{\sqrt{2}}(|\Psi_1\rangle + i\,|\Psi_0\rangle) \\
&= \left(1-2\sin^2(\theta)+i2\cos(\theta)\sin(\theta)\right)\ |V_1\rangle \\
&= (\cos(2\theta)+i\sin(2\theta))\ |V_1\rangle \\
&= e^{i2\theta}\,|V_1\rangle
\end{aligned}
$$

Valeurs propres G_F

Les vecteurs propres de l'opérateur G_F.

$$|V_1\rangle = \frac{1}{\sqrt{2}}(|\Psi_1\rangle + i\,|\Psi_0\rangle)$$

$$|V_2\rangle = \frac{1}{\sqrt{2}}(|\Psi_1\rangle - i\,|\Psi_0\rangle)$$

Clairement,

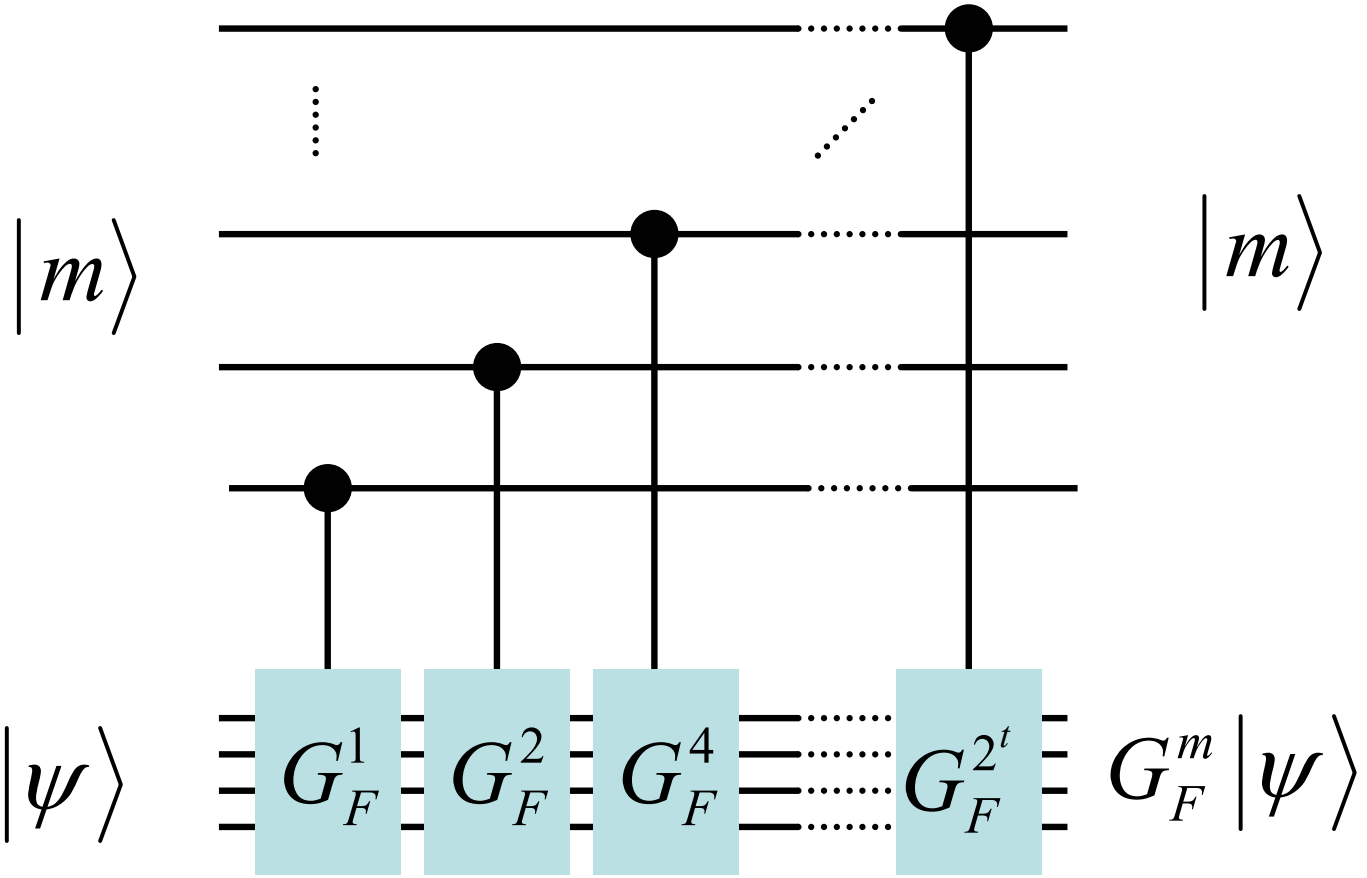
$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}(-i\,|V_0\rangle + i\,|V_1\rangle)$$

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|V_0\rangle + |V_1\rangle)$$

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

$$H\,|0\rangle = \left(\frac{1}{\sqrt{2t}} - \frac{i}{\sqrt{2(N-t)}}\right)|V_1\rangle + \left(\frac{1}{\sqrt{2t}} + \frac{i}{\sqrt{2(N-t)}}\right)|V_2\rangle$$

Outils de base



$$G'_F \;:\; |m\rangle \otimes |\Psi\rangle \rightarrow |m\rangle \otimes (G_F)^m |\Psi\rangle$$

Algorithme

Compte(F, m)

1. $|\Psi_0\rangle \leftarrow H^{\otimes m+n} |\mathbf{0}\rangle |\mathbf{0}\rangle$
2. $|\Psi_1\rangle \leftarrow GI_F |\Psi_1\rangle$
3. $|\Psi_2\rangle \leftarrow F_m^{-1} \otimes I^{\otimes n} |\Psi_2\rangle$
4. $\tilde{f} \leftarrow$ mesure premier registre de $|\Psi_3\rangle$
5. Retourne: $\tilde{t} = N \sin^2 \frac{\tilde{f}\pi}{2^m}$ (et $\tilde{f}$ si nécessaire)

Intuition et analyse originales

$$
\begin{aligned}
|\Psi_0\rangle &= |\mathbf{0}\rangle\,|\mathbf{0}\rangle \\
|\Psi_1\rangle &= \left(\frac{1}{\sqrt{2^m}}\sum_{y=0}^{2^m-1}|y\rangle\right)\otimes\left(\frac{1}{\sqrt{N}}\sum_{x=X}|x\rangle\right) \\
&= \sum_{y=0}^{2^m-1}\frac{1}{\sqrt{2^m}}\,|y\rangle\left(\frac{1}{\sqrt{t}}\sum_{F(x)=1}|x\rangle+\frac{1}{\sqrt{N-t}}\sum_{F(x)=0}|x\rangle\right) \\
|\Psi_2\rangle &= \sum_{y=0}^{2^m-1}\frac{1}{\sqrt{2^m}}\,|y\rangle\left(k_m\sum_{F(x)=1}|x\rangle+\ell_m\sum_{F(x)=0}|x\rangle\right) \\
&\quad \text{On observe } x \text{ tel que } F(x)=1 \\
|\Psi_3\rangle &= \alpha\sum_{y=0}^{2^m-1}\sin((2y+1)\theta)\,|y\rangle \\
|\Psi_4\rangle &= a\,|f\rangle+b\,|2^m-f\rangle+c\,|R\rangle
\end{aligned}
$$

$$
\sin^2(\theta)=\frac{t}{N}\qquad f\simeq 2^m\theta/\pi\qquad t\simeq N\sin^2(\frac{f\pi}{2^m})
$$

Intuition et analyse originales

$$
\begin{aligned}
|\Psi_0\rangle &= |\mathbf{0}\rangle\,|\mathbf{0}\rangle \\
|\Psi_1\rangle &= \left(\frac{1}{\sqrt{2^m}}\sum_{y=0}^{2^m-1}|y\rangle\right)\otimes\left(\frac{1}{\sqrt{N}}\sum_{x=X}|x\rangle\right) \\
&= \sum_{y=0}^{2^m-1}\frac{1}{\sqrt{2^m}}\,|y\rangle\left(\frac{1}{\sqrt{t}}\sum_{F(x)=1}|x\rangle+\frac{1}{\sqrt{N-t}}\sum_{F(x)=0}|x\rangle\right) \\
|\Psi_2\rangle &= \sum_{y=0}^{2^m-1}\frac{1}{\sqrt{2^m}}\,|y\rangle\left(k_m\sum_{F(x)=1}|x\rangle+\ell_m\sum_{F(x)=0}|x\rangle\right) \\
&\quad \text{On observe } x \text{ tel que } F(x)=0 \\
|\Psi_3\rangle &= \alpha\sum_{y=0}^{2^m-1}\cos((2y+1)\theta)\,|y\rangle \\
|\Psi_4\rangle &= a\,|f\rangle+b\,|2^m-f\rangle+c\,|R\rangle
\end{aligned}
$$

$$
\sin^2(\theta)=\frac{t}{N}\qquad f\simeq 2^m\theta/\pi\qquad t\simeq N\sin^2(\frac{f\pi}{2^m})
$$

Théorème principal

Théorème:

Si $\tilde{t} = \textbf{Compte}(F, m)$ alors

$$|t - \tilde{t}| < \frac{4\pi}{2^m}\sqrt{t(N-t)} + N\left(\frac{2\pi^2}{2^{2m}}\right)$$

avec probabilité au moins 3/4.

Analyse utilisant les valeurs propres

$$
\begin{aligned}
|\Psi_0\rangle &= |\mathbf{0}\rangle\,|\mathbf{0}\rangle \\
|\Psi_1\rangle &= \left(\frac{1}{\sqrt{2^m}}\sum_{y=0}^{2^m-1}|y\rangle\right)\otimes\left(\frac{1}{\sqrt{N}}\sum_{x=X}|x\rangle\right) \\
&= \sum_{y=0}^{2^m-1}\frac{1}{\sqrt{2^m}}\,|y\rangle\,(a\,|V_1\rangle + b\,|V_2\rangle) \\
|\Psi_2\rangle &= \sum_{y=0}^{2^m-1}\frac{1}{\sqrt{2^m}}\,|y\rangle\,(ae^{2\theta yi}\,|V_1\rangle + be^{-2\theta yi}\,|V_2\rangle) \\
&\quad \text{On observe } V_1 \\
&= \frac{1}{\sqrt{2^m}}\sum_{y=0}^{2^m-1}e^{2\theta yi}\,|y\rangle \\
|\Psi_3\rangle &\simeq |f\rangle
\end{aligned}
$$

$$
\sin^2(\theta) = \frac{t}{N} \qquad f \simeq 2^m\theta/\pi \qquad t \simeq N\sin^2(\frac{f\pi}{2^m})
$$

Analyse utilisant les valeurs propres

$$
\begin{aligned}
|\Psi_0\rangle &= |\mathbf{0}\rangle\,|\mathbf{0}\rangle \\
|\Psi_1\rangle &= \left(\frac{1}{\sqrt{2^m}}\sum_{y=0}^{2^m-1}|y\rangle\right)\otimes\left(\frac{1}{\sqrt{N}}\sum_{x=X}|x\rangle\right) \\
&= \sum_{y=0}^{2^m-1}\frac{1}{\sqrt{2^m}}\,|y\rangle\,(a\,|V_1\rangle + b\,|V_2\rangle) \\
|\Psi_2\rangle &= \sum_{y=0}^{2^m-1}\frac{1}{\sqrt{2^m}}\,|y\rangle\,(ae^{2\theta yi}\,|V_1\rangle + be^{-2\theta yi}\,|V_2\rangle) \\
&\quad \text{On observe } V_2 \\
&= \frac{1}{\sqrt{2^m}}\sum_{y=0}^{2^m-1}e^{-2\theta yi}\,|y\rangle \;=\; \frac{1}{\sqrt{2^m}}\sum_{y=0}^{2^m-1}e^{2\theta(2^m-y)i}\,|y\rangle \\
|\Psi_3\rangle &\simeq |2^m - f\rangle
\end{aligned}
$$

$$
\sin^2(\theta) = \frac{t}{N} \qquad f \simeq 2^m\theta/\pi \qquad t \simeq N\sin^2(\frac{f\pi}{2^m})
$$

Lemme utile

Lemme:
Si $a = \sin^2(\theta)$ et $a' = \sin^2(\theta')$ avec $0 \leq \theta, \theta' \leq 2\pi$ alors

$$|\theta - \theta'| \leq \epsilon \quad \Rightarrow \quad |a - a'| \leq 2\epsilon\sqrt{a(1-a)} + \epsilon^2$$

Preuve: L'utilisation judicieuse d'identités trigonométriques nous donne

$$\sin^2(\theta + \epsilon) - \sin^2(\theta) = \sqrt{a(1-a)}\sin(2\epsilon) + (1-2a)\sin^2(\epsilon)$$

$$\sin^2(\theta) - \sin^2(\theta - \epsilon) = \sqrt{a(1-a)}\sin(2\epsilon) + (2a-1)\sin^2(\epsilon)$$

on utilise le fait que $\sin(x) \leq 1/x$ et on obtient le lemme.

Preuve

Nous savons que la qualité de l'approximation de la phase est telle que si $\tilde{f}$ est observé la phase exacte de f est telle que

$$|f - \tilde{f}| \leq 2$$

et donc

$$\left|\frac{f\pi}{2^m} - \frac{\tilde{f}\pi}{2^m}\right| \leq \frac{2\pi}{2^m}$$

en appliquant le lemme avec $\theta = \frac{f\pi}{2^m}$ et $\theta' = \frac{\tilde{f}\pi}{2^m}$ on obtient

$$\left|\sin^2\left(\frac{f\pi}{2^m}\right) - \sin^2\left(\frac{\tilde{f}\pi}{2^m}\right)\right| \leq \frac{4\pi}{2^m}\sqrt{\sin^2\left(\frac{f\pi}{2^m}\right)\left(1 - \sin^2\left(\frac{f\pi}{2^m}\right)\right)} + \left(\frac{2\pi}{2^m}\right)^2$$

$$\left|N\sin^2\left(\frac{f\pi}{2^m}\right) - N\sin^2\left(\frac{\tilde{f}\pi}{2^m}\right)\right| \leq N\frac{4\pi}{2^m}\sqrt{\sin^2\left(\frac{f\pi}{2^m}\right)\left(1 - \sin^2\left(\frac{f\pi}{2^m}\right)\right)} + N\left(\frac{2\pi}{2^m}\right)^2$$

$$|t - \tilde{t}| \leq \frac{4\pi}{2^m}\sqrt{t(N-t)} + N\left(\frac{2\pi}{2^m}\right)^2$$

Un bon estimé de t

Corollaire:
Étant donné F avec N et t tel que définis de façon habituelle, **Count**$(F, \log(c\sqrt{N}))$ retourne $\tilde{t}$ tel que

$$|t - \tilde{t}| < \frac{4\pi}{c}\sqrt{t} + \frac{2\pi^2}{c^2}$$

avec probabilité au moins $\frac{3}{4}$ avec exactement

$$c\sqrt{N}$$

évaluations de F.

Preuve:
Choisir m tel que with $2^m \simeq c\sqrt{N}$ dans le théorème principal.

Facteur constant

Corollaire:
Il existe un algorithme **CompteRel**(F, ϵ) qui retourne $\tilde{t}$ tel que

$$|t - \tilde{t}| \ < \ \epsilon t$$

avec probabilité 3/4 en utilisant un nombre espéré d'évaluation de F dans

$$O\left(\frac{1}{\epsilon}\sqrt{N/t}\right).$$

CompteRel(F, c)

1. $l = 0$
2. $l \leftarrow l + 1$
3. $\tilde{t} \leftarrow$**Count**(F, l)
4. Si $\tilde{t} = 0$ et $2^l < 2\sqrt{N}$ alors aller a 2
5. Retourne **Count**$(F, \log(\frac{200}{\epsilon}) + l)$

Comptage probablement exact

Corollaire:
Il existe un algorithme **CompteExact** qui retourne $\tilde{t}$ tel que

$$\tilde{t} = t$$

avec probabilité au moins 3/4 et utilise un nombre espéré d'évaluation de F dans

$$O(\sqrt{t(N-t)})$$

et qui utilise un espace dans $O(\log N)$.

CompteExact(F)

1. $\tilde{t_1} \leftarrow$**Compte**$(F, \log(50\sqrt{N}))$ et $\tilde{t_2} \leftarrow$**Compte**$(F, \log(50\sqrt{N}))$
2. $P \leftarrow \text{Min}(30\sqrt{\tilde{t_1}(N-\tilde{t_1})}, 30\sqrt{\tilde{t_1}(N-\tilde{t_1})})$
3. Retourne **Compte**$(F, \log(P))$

Tableau récapitulatif

Problème de comptage: Étant donné $F : X \to \{0, 1\}$ une boite noîre avec $|X| = N$, trouver un bon estimateur $\tilde{t}$ de $t = \{x|F(x) = 1\}$.

$\lvert t - \tilde{t}\rvert$	Quantum	Classical
$O(\sqrt{t})$	$O(\sqrt{N})$	$\Omega(N)$
ϵt	$O\left(\frac{1}{\epsilon}\sqrt{\frac{N}{t}}\right)$	$\Omega\left(\frac{N}{\epsilon^2 t}\right)$
< 1	$O(\sqrt{t(N-t)})$	$\Omega(N)$

Références

Lov K. Grover, A fast quantum mechanical algorithm for database search, Proceedings of 28th Annual ACM Symposium on Theory of Computing, Mai 1996, pp. 212 − 219.
(quant-ph/9605043)

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

Gilles Brassard, Peter Høyer et Alain Tapp, Cryptology Column —Quantum Algorithm for the Collision Problem, ACM SIGACT News, Vol. 28, Juin 1997, pp. 14-19.
(quant-ph/9705002)

References

Gilles Brassard, Peter Høyer et Alain Tapp, Quantum Counting, 25th International Colloquium, ICALP'98, LNCS vol. 1443, Springer, pp.820-831,1998.
(quant-ph/9805082)

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