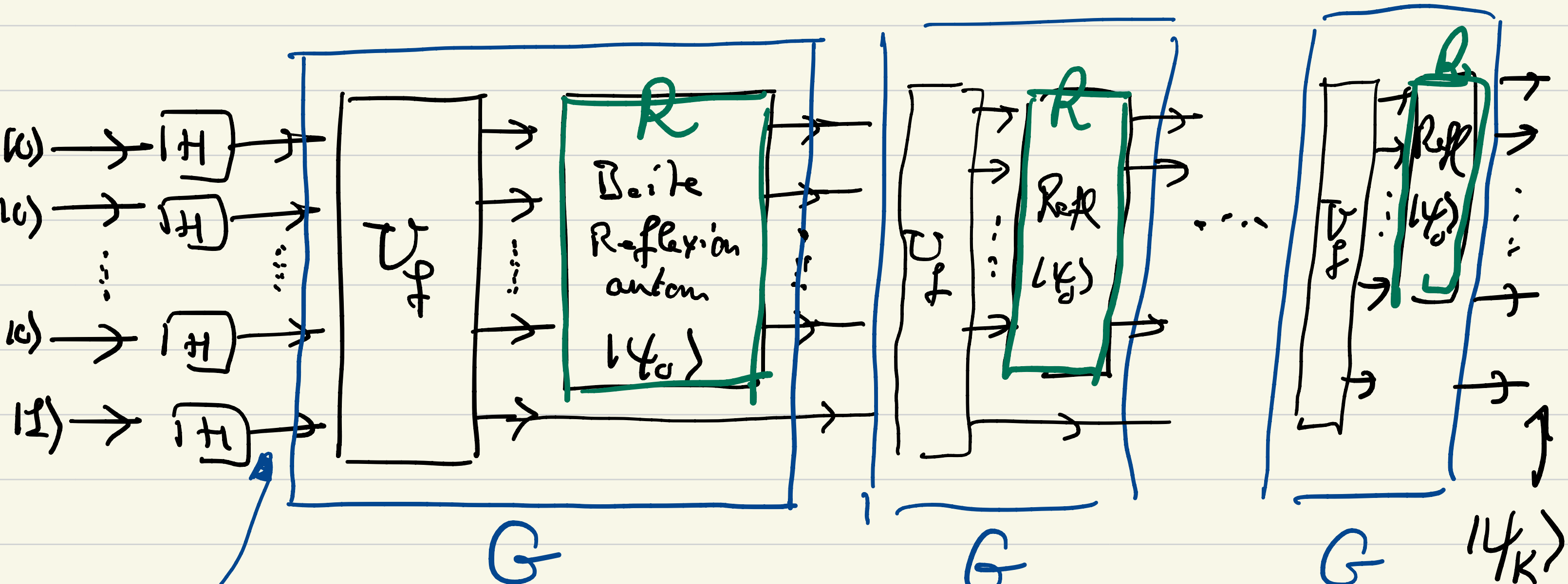
Alg de Grover. (Base de donnée non structurée)

Circuit quantique :



- itérations K fois de G.

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{\underline{x} \in \mathbb{F}_2^n} |\underline{x}\rangle .$$

indép de f . ! vecteur commun de $(\mathbb{C}^2)^{\otimes n}$

- état final :

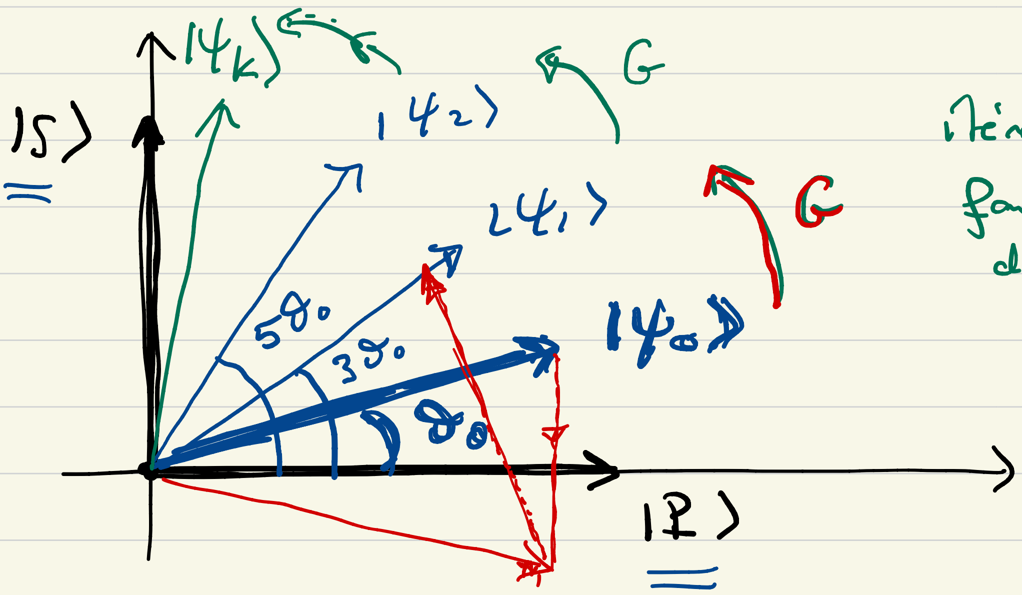
$$|\psi_K\rangle = (\cos(2K+1)\vartheta_0)\,|P\rangle + (\sin(2K+1)\vartheta_0)\,|S\rangle$$

$$|P\rangle = \frac{1}{\sqrt{N-M}} \sum_{\underline{x} \in P} |\underline{x}\rangle \quad \text{et} \quad |S\rangle = \frac{1}{\sqrt{M}} \sum_{\underline{x} \in S} |\underline{x}\rangle$$

$f(\underline{x})=0$ $\qquad$ $f(\underline{x})=1$.

- Deux questions :
  - a) Fabriquer la boite ou le circuit de Réflexion autour de $|\psi_0\rangle$.
  - b) Combien de fois itérer → choix de K.

Interprétation Géométrique du circuit :



itérateur de Grover font des rotations d'angle $2\vartheta_0$.

$$\begin{cases} \cos\vartheta_0 = \sqrt{1-\frac{M}{N}} \\ \sin\vartheta_0 = \sqrt{\frac{M}{N}} \end{cases}$$

Avec K bien choisi

$$|\psi_K\rangle \simeq |S\rangle.$$

$$(\cos(2K+1)\vartheta_0)|P\rangle + (\sin(2K+1)\vartheta_0)|S\rangle$$

Idée : $(2K+1)\vartheta_0 \simeq \frac{\pi}{2}$.

$$\Rightarrow 2K+1 \simeq \frac{\pi}{2\vartheta_0}$$

Limite sur le # d'itérations.

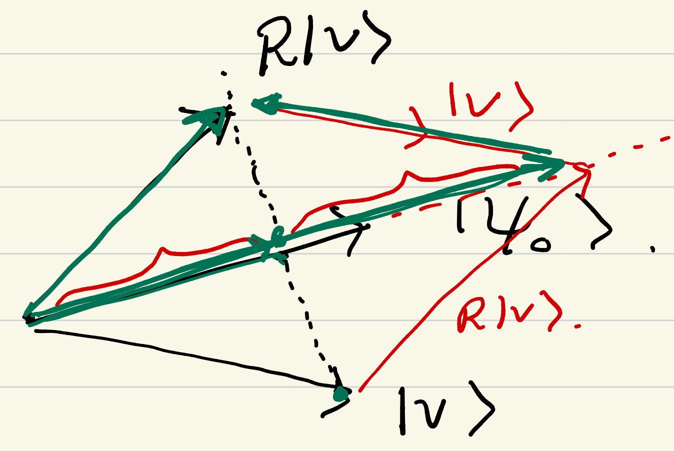
$$K = \left[\frac{\pi}{4\vartheta_0} - \frac{1}{2}\right].$$

Revoir cela plus loin.

Remarque :

- on ne sait dans quel plan le vecteur $|\psi_0\rangle$ tourne. $\{|P\rangle, |S\rangle\}$
- connait on pas ϑ_0 ?

Circuit pour la Matrice de réflexion autour de $|\psi_0\rangle$:

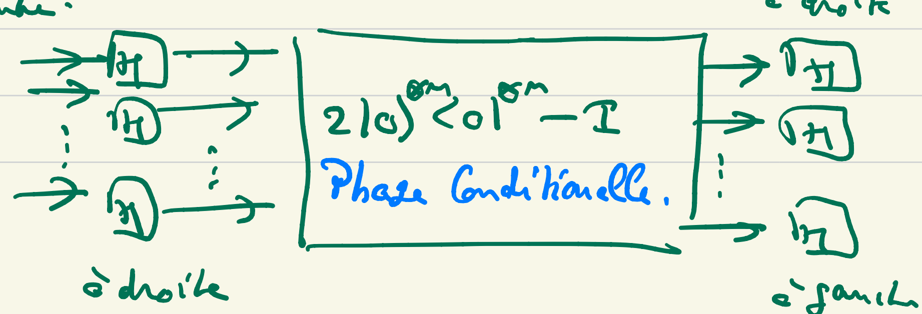


$$R|v\rangle = 2\,\underbrace{|\psi_0\rangle}_{\text{unité}}\,\langle\psi_0|v\rangle - |v\rangle$$

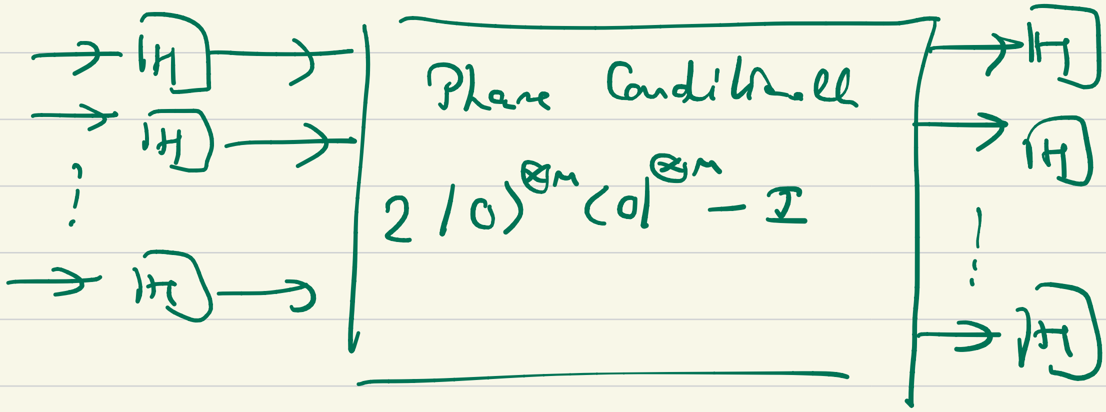
$$= \Big(2\,\underbrace{|\psi_0\rangle\langle\psi_0|}_{\text{projecteur sur } |\psi_0\rangle} - I\Big)\,|v\rangle.$$

$$R = 2\,|\psi_0\rangle\langle\psi_0| - I = \Big(2\,H^{\otimes m}|0\rangle^{\otimes m}\langle 0|^{\otimes m}H^{\otimes m} - \underbrace{I}_{H^{\otimes m}\cdot H^{\otimes m}}\Big).$$

$$\Rightarrow R = \underbrace{H^{\otimes m}}_{\text{à gauche.}}\big(2\,|0\rangle^{\otimes m}\langle 0|^{\otimes m} - I\big)\underbrace{H^{\otimes m}}_{\text{à droite}}.$$

$R =$ 

$R =$



$$(\text{Phase Cond})\,|\underline{x}\rangle = 2|0\rangle^{\otimes n}\underbrace{\langle 0\cdots 0|x_1\cdots x_n\rangle}\, - \,\underline{|\underline{x}\rangle}$$

$$= \begin{cases} |0\cdots 0\rangle = |0\rangle^{\otimes n} & \text{si } (x_1\cdots x_n) = (0\cdots 0) \\ -|\underline{x}\rangle = -|x_1\rangle\otimes|x_2\rangle\cdots|x_n\rangle. & \text{si } (x_1\cdots x_n) \neq (0\cdots 0) \end{cases}$$

La phase Conditionnelle affecte l'état $|\underline{x}\rangle$ d'un "moins" si $\underline{x} \neq \underline{0}$ et laisse $|\underline{0}\rangle$ avec le signe "plus".

Circuit facilement réalisable. (IBM practice 4)

Discussion du nombre d'itérations et de la prob de succès de l'algorithme.

1er cas : M connu $\longrightarrow$ θ_0 est connu

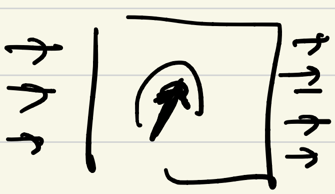
$$\begin{cases} \sin\theta_0 = \sqrt{\dfrac{M}{N}} \\ \cos\theta_0 = \sqrt{1 - \dfrac{M}{N}} \end{cases}.$$

Cas le "plus dur" $M = 1$. et $N \gg 1$.

$$\sin\theta_0 = \frac{1}{\sqrt{N}} \quad \text{et donc} \quad \theta_0 \simeq \frac{1}{\sqrt{N}}.$$

Sortie du circuit

$$|\psi_K\rangle = (\cos(2K+1)\theta_0)\,|P\rangle + (\sin(2K+1)\theta_0)\,|S\rangle.$$



$|\underline{x}\rangle \in P$ ou $\in S$.

base computationnelle

$$\boxed{\begin{aligned} \mathrm{Prob}(\underline{x} \in S) &= \left(\sin(2K+1)\theta_0\right)^2 \\ &= |\langle S|\psi_K\rangle|^2. \end{aligned}}$$

Choisir K t.q $\mathrm{Prob}(\underline{x} \in S) \simeq 1$.

soit $(2K+1)\theta_0 \simeq \pi/2 \Longrightarrow 2K+1 \simeq \frac{\pi\sqrt{N}}{2} \Longrightarrow \boxed{K \simeq \frac{\pi\sqrt{N}}{4} - \frac{1}{2}}$

Avec un peu d'analyse on peut montrer que pour $K = \left[\frac{\pi\sqrt{N}}{4}\right]$ la prob de succès $\Pr(\underline{x} \in S) = 1 - O\left(\frac{1}{N}\right)$.

L'opérateur de Grover doit être itéré $O(\sqrt{N})$.
La profondeur du circuit dans le cas le plus dur est $O(\sqrt{N})$. // $\underbrace{\text{complexité de l'alg}}_{\text{temporelle}}$ // . $\sqrt{N} = 2^{n/2}$.

accélération quadratique.
ou racine carrée.

<u>Cas simple et spécial</u> $M = \frac{N}{4}$. $\Rightarrow \begin{cases} \sin\vartheta_0 = \frac{1}{2} \\ \cos\vartheta_0 = \frac{\sqrt{3}}{2} \end{cases}$.

$\rightsquigarrow \vartheta_0 = \frac{\pi}{6}$.

$$\text{prob}(\underline{x} \in S) = |\sin(2k+1)\vartheta_0|^2 = \left|\sin(2k+1)\frac{\pi}{6}\right|^2 = 1$$

$$(2k+1)\frac{\pi}{6} = \frac{\pi}{2} \Rightarrow 2k+1 = 3 \Rightarrow \boxed{K = 1}$$

en une itération de G vous trouvez un élément marqué !!! avec prob de succès $= 1$.

$\boxed{\text{Lire les notes}}$

Généraliser quand M est connu : $\to M = 1$; $\to M = \frac{N}{4}$.

$M > \frac{3}{4} N \Rightarrow$ en tirant élément au hasard prob succès $= 3/4 \geq 1/4$.

et $M < \frac{3}{4} N \Rightarrow$ avec $K = O(\sqrt{N})$ prob(succès) $\geq \frac{1}{4}$.

#.

$\boxed{2^{\text{ème}} \text{ Cas}}$ si M est inconnu ? Ici θ_0 est inconnu

donc comment utiliser $|\sin (2K+1)\theta_0|^2 \approx 1$

M inconnu? Alg :

essayez de voir si $f(\underline{x})=1$?

1) Prend $\underline{x}$ aléatoirement. Si $M > \frac{3N}{4}$. vous aurez un succès avec prob(succès) $> \frac{3}{4}$ $\left(> \frac{1}{4} \right)$.

2) Si vous avez échec ; ce que vous faites c'est utilisez Grover avec un nombre d'itération $R \in \{1, 2, \ldots, [\sqrt{N}]\}$. unif aléatoirement choisi.

$\boxed{G^R \leftarrow \text{ds le circuit}}$

Lemme.

$$\boxed{\text{Prob(succès du point 2)} \geq \frac{1}{4} \text{ si } M < \frac{3N}{4}}$$

$\Rightarrow$ Prob(succès en 1) ou 2) $\forall M$) $\geq \frac{1}{4}$.

et ensuite cette prob peut être amplifié à $1-\epsilon$ en faisant $T = O(\ln \epsilon / \cdot 4)$ rounds de 1) et 2).

Complexité Totale : $O(\sqrt{N} \ln \epsilon)$.

Preuve du Lemme. $R \in \{1 \dots [\sqrt{N}]\}$.

$$\text{Prob(succès du pt 2)} = \sum_{R=1}^{[\sqrt{N}]} \underbrace{\text{Prob(succès} / R)}_{\downarrow\ (\sin(2R+1)\vartheta_0)^2} \ \underbrace{\text{Prob}(R)}_{\frac{1}{[\sqrt{N}]}}.$$

$$\text{Prob(succès 2)} \approx \frac{1}{[\sqrt{N}]} \sum_{R=1}^{[\sqrt{N}]} (\sin(2R+1)\vartheta_0)^2.$$

$$= \frac{1}{2} - \frac{\sin(4[\sqrt{N}]\vartheta_0)}{4[\sqrt{N}](\sin 2\vartheta_0)}. \quad \checkmark$$

$\boxed{M < \frac{3}{4}N}$ $\quad \sqrt{\frac{M}{N}} = \sin\vartheta_0 \quad$ $\sin 2\vartheta_0 = 2\sin\vartheta_0 \cos\vartheta_0$

$$= 2\sqrt{\frac{M}{N}}\underbrace{\sqrt{1-\frac{M}{N}}}_{\geqslant \sqrt{\frac{N}{4N}}} \geqslant \frac{1}{\sqrt{N}}.$$

$$\begin{cases} \frac{1}{\sin 2\vartheta_0} < \frac{1}{\sqrt{N}} \Rightarrow -\frac{1}{\sin 2\vartheta_0} > -\frac{1}{\sqrt{N}}. \\ \sin(4\sqrt{N}\vartheta_0) < 1. \end{cases}$$

$$\Rightarrow \text{Prob(succès 2)} \geqslant \frac{1}{2} - \frac{1}{4\sqrt{N}\frac{1}{\sqrt{N}}} = \frac{1}{2} - \frac{1}{4} = \frac{1}{4}.$$