Chapitre 2 : Algorithmes quantiques à base d'oracles

ENSIIE - Informatique quantique pour la recherche opérationnelle

Dimitri Watel (dimitri.watel@ensiie.fr)

2022

Algorithmes du chapitre

- **Algorithme de Deutsch-Jozsa** : savoir si une fonction f est constante ou équilibrée.
- **Algorithme de Bernstein-Vazirani** : trouver $s \in \{0,1\}^n$ quand on a accès à $f : x \rightarrow x \cdot s$
- **Algorithme de Grover** : trouver $x \in \{0,1\}^n$ tel que $f(x) = 1$ quand on a accès à f

- Algorithmes basés sur la notion d'oracle ou de boîte noire
- Plus rapide que les meilleurs algorithmes déterministes ou probabilistes

Plan

Problème résolu par l'algorithme de Deutsch-Jozsa

Soit une fonction $f : (\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$

Fonction équilibrée ou constante

- Une fonction **constante** si

$$\forall x, f(x) = 0 \text{ ou } \forall x, f(x) = 1$$

- Une fonction **équilibrée** si

$$\#\{x|f(x) = 0\} = \#\{x|f(x) = 1\} = 2^{n-1}$$

Problème à résoudre

Soit f constante ou équilibrée, f est-elle constante?

(! Beaucoup de fonctions ne sont ni constantes ni équilibrées)

Efficacité de l'algorithme

- Meilleure complexité classique : $O(2^{n-1})$ appels à f
- Complexité de l'algorithme de Deutsch-Jozsa :

$$O(1) \text{ appels à } f + O(n)$$

(plus exactement, l'algorithme effectue 2^n appels à f en simultané)

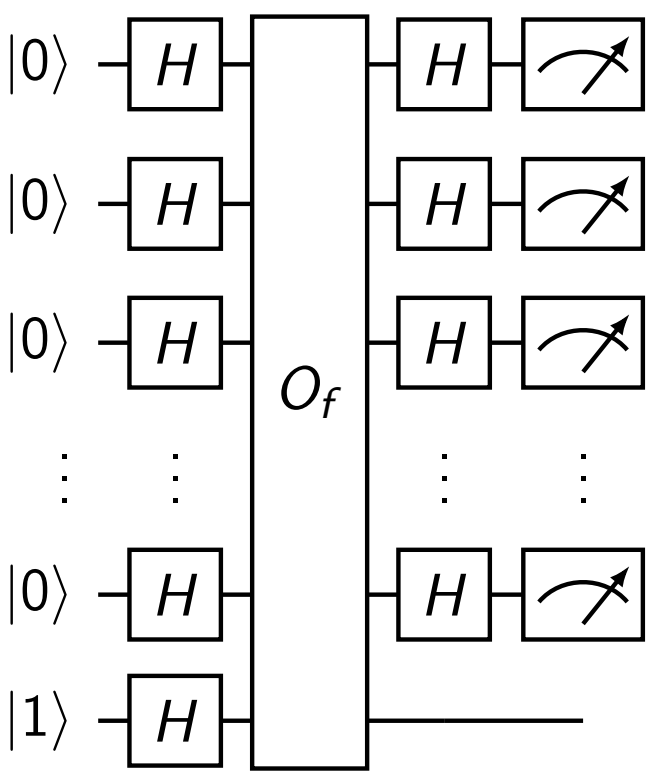
Théorème

Il existe des problèmes de décision qu'on peut résoudre plus rapidement avec l'informatique quantique.

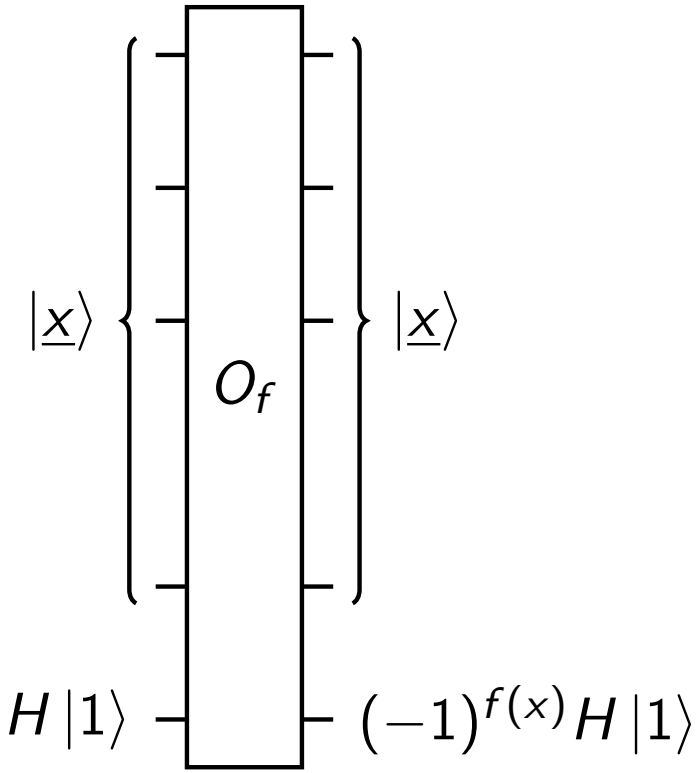
Description de l'algorithme

- Entrée de taille $n+1$: $|000\ldots01\rangle$
- Effectuer une transformation de Hadamard
- Appliquer un *oracle*
- Effectuer une transformation de Hadamard sur les n premiers qbits
- Mesurer ces qbits
- La fonction est constante si la mesure donne 0 partout

Description de l'algorithme

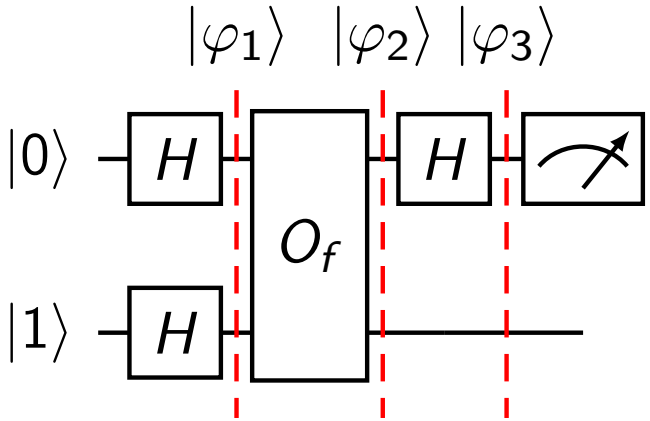


avec

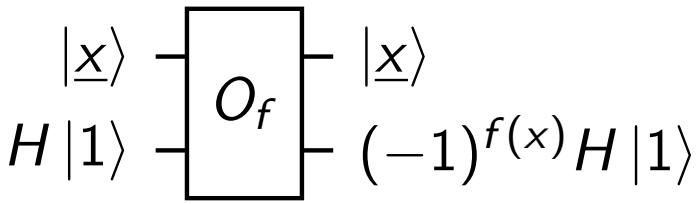


O_f est nommé l'oracle.

Preuve pour $n = 1$



avec



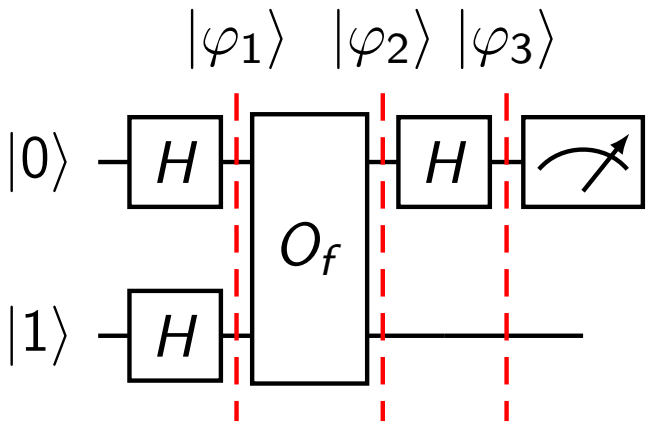
Que valent les qbits $|\varphi_1\rangle$, $|\varphi_2\rangle$, $|\varphi_3\rangle$?

Alerte confusion

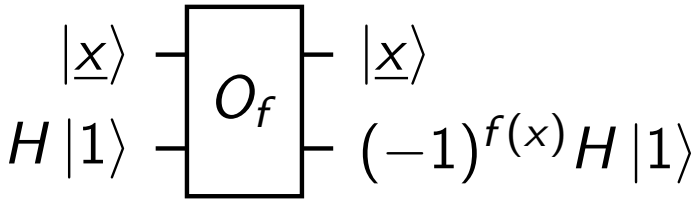
Le 1e qbit de $|\varphi_3\rangle$ ne vaut pas toujours 0, même s'il ne semble pas modifié par l'oracle!

Raison : Dans le dessin de droite, $|\underline{x}\rangle$ est un état de base, $|0\rangle$ ou $|1\rangle$. Ce n'est plus vrai si $|\underline{x}\rangle$ est superposé. (La notation $f(x)$ n'aurai pas de sens.)

$|\varphi_1\rangle$



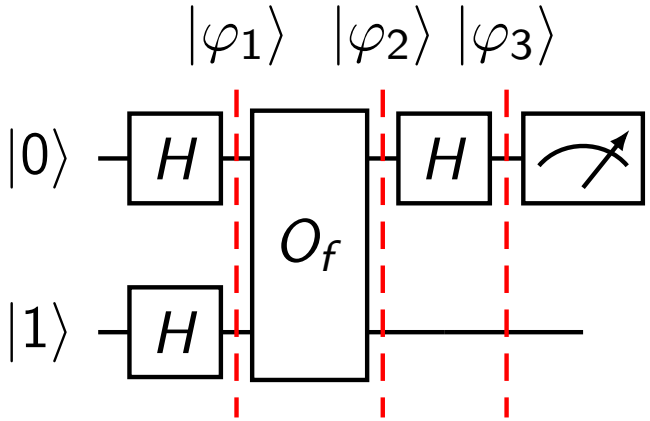
avec



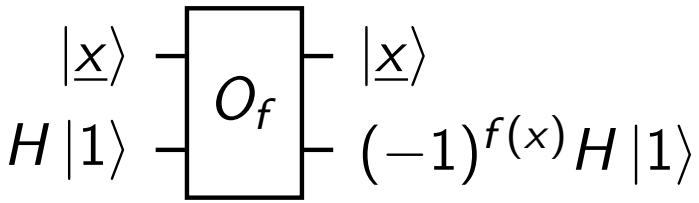
$$|\varphi_1\rangle = H|0\rangle \otimes H|1\rangle$$

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

$|\varphi_2\rangle$

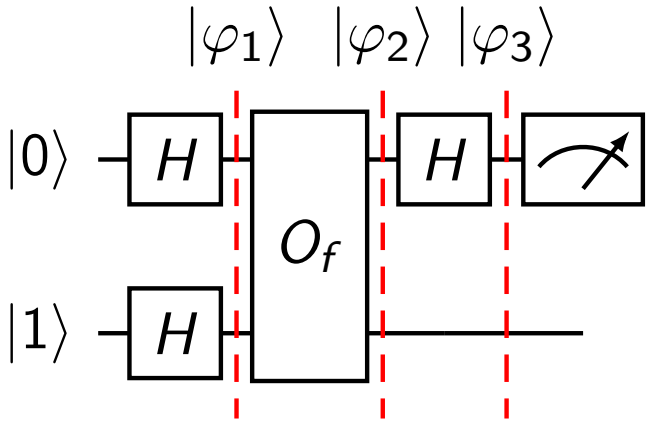


avec

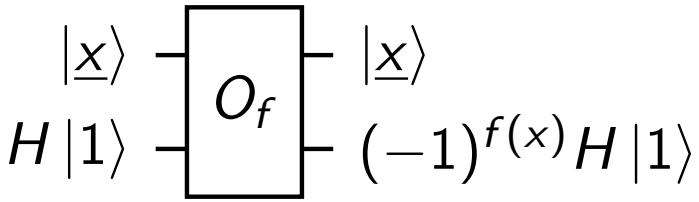


$$
\begin{aligned}
|\varphi_2\rangle &= O_f\,|\varphi_1\rangle \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle \otimes \left((-1)^{f(0)}\right) H|1\rangle \quad + |1\rangle \otimes \left((-1)^{f(1)}\right) H|1\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left((-1)^{f(0)}\,|0\rangle \otimes H|1\rangle \quad + (-1)^{f(1)}\,|1\rangle \otimes H|1\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left((-1)^{f(0)}\,|0\rangle \quad + (-1)^{f(1)}\,|1\rangle\right) \otimes H|1\rangle
\end{aligned}
$$

$|\varphi_3\rangle$

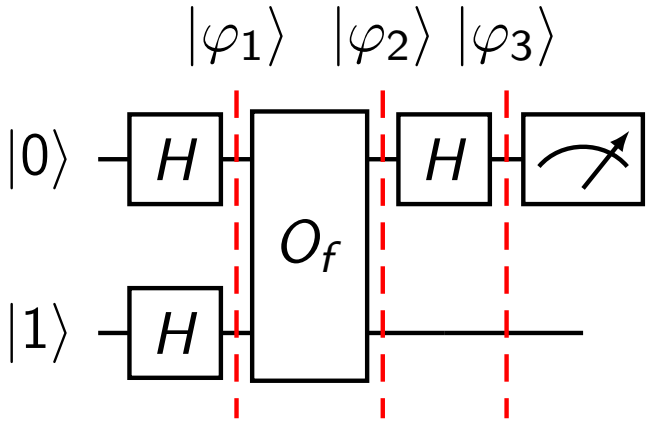


avec

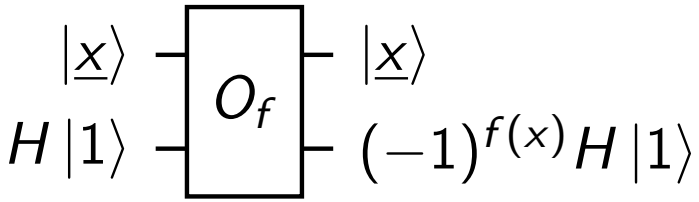


$$
\begin{aligned}
|\varphi_3\rangle &= (H \otimes I)\,|\varphi_2\rangle \\
&= \frac{1}{\sqrt{2}}(H \otimes I)\left(\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right) \otimes H|1\rangle\right) \\
&= \tfrac{1}{\sqrt{2}}\left((-1)^{f(0)}\tfrac{|0\rangle+|1\rangle}{\sqrt{2}} + (-1)^{f(1)}\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \otimes H|1\rangle \\
&= \tfrac{1}{2}\left(\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\right) \otimes H|1\rangle
\end{aligned}
$$

Mesure



avec



$$|\varphi_3\rangle = \frac{1}{2}\left(\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\right) \otimes H|1\rangle$$

- Si f est constante, mesurer $|\varphi_3\rangle$ donnerait 00 ou 01. Le premier qbit vaut 0.
- Si f est équilibrée, mesurer $|\varphi_3\rangle$ donnerait 10 ou 11. Le premier qbit vaut 1.

Cas général

$$|\varphi_3\rangle = \frac{1}{2^n} \sum_{k=0}^{2^n-1} \sum_{l=0}^{2^n-1} (-1)^{f(\underline{l})+\underline{l}\odot\underline{k}} |\underline{k}\rangle \otimes H|1\rangle$$

avec $\underline{l} \odot \underline{k} = l_1 k_1 \oplus l_2 k_2 \oplus \cdots \oplus l_n k_n$

Proba de mesurer 0 sur les n premiers qbits :

$$\frac{1}{2^n} \sum_{l=0}^{2^n-1} (-1)^{f(\underline{l})+\underline{l}\odot 0} = \frac{1}{2^n} \sum_{l=0}^{2^n-1} (-1)^{f(\underline{l})}$$

- Si f est constante, cette probabilité vaut 1.
- Si f est équilibrée, cette probabilité vaut 0.

Comment fabriquer l'oracle ?

Comment construire O_f à partir de f

- Hypothèse : je dispose d'un circuit logique qui calcule f.
- Question : comment construire O_f ?

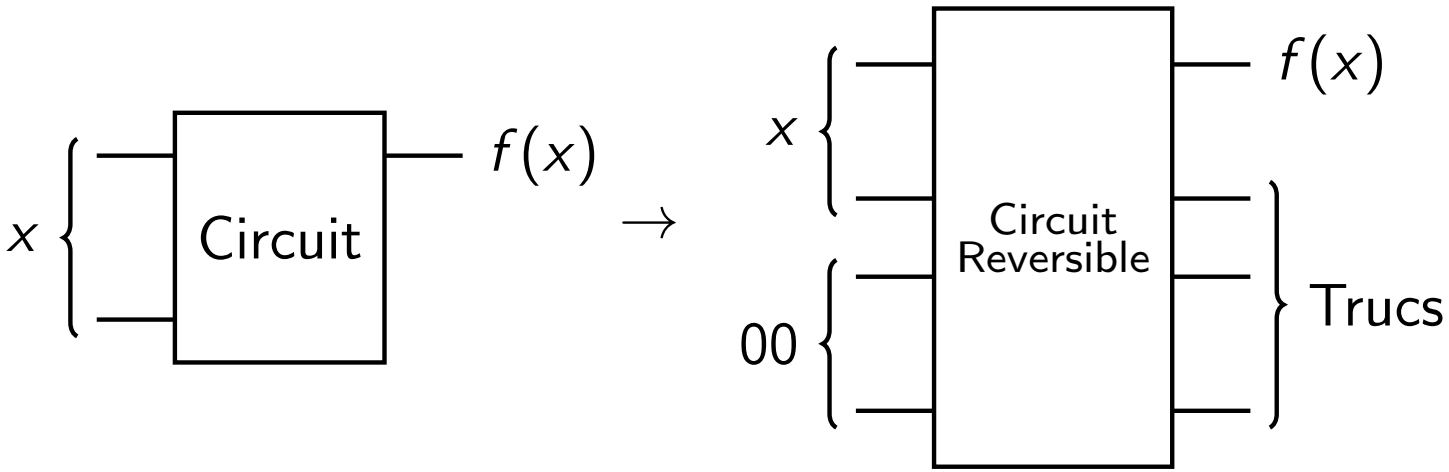
Plusieurs difficultés :

- L'informatique quantique est réversible
- Faire apparaître $f(x)$ dans la phase du qbit (*i.e.* en exponentielle de -1)

Rendre le circuit de f réversible

Théorème

Tout circuit logique peut être rendu réversible en multipliant le nombre de bits d'entrée et la profondeur par un facteur constant.

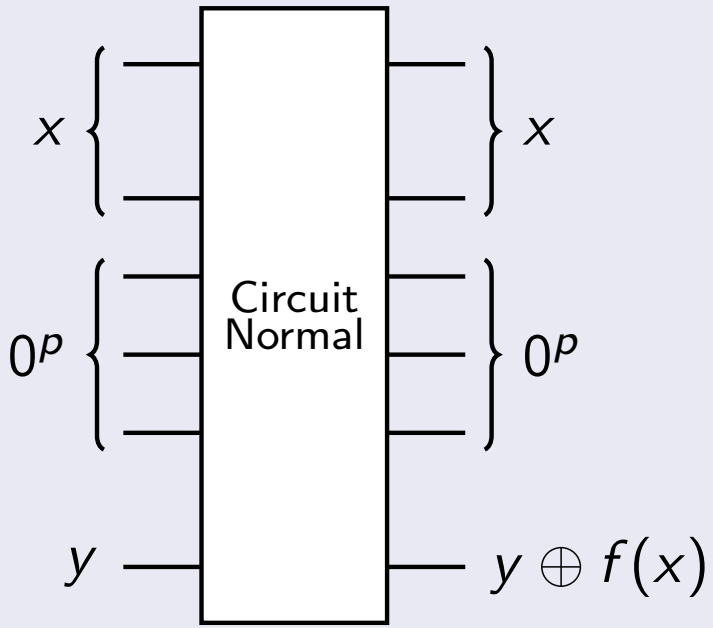


Preuve : rendre la porte AND réversible avec 1 bit supplémentaire.
Puis utiliser le fait que NAND est universelle.

Porte sous forme normale

Théorème

Tout circuit logique peut être rendu réversible et sous la forme normale suivante.

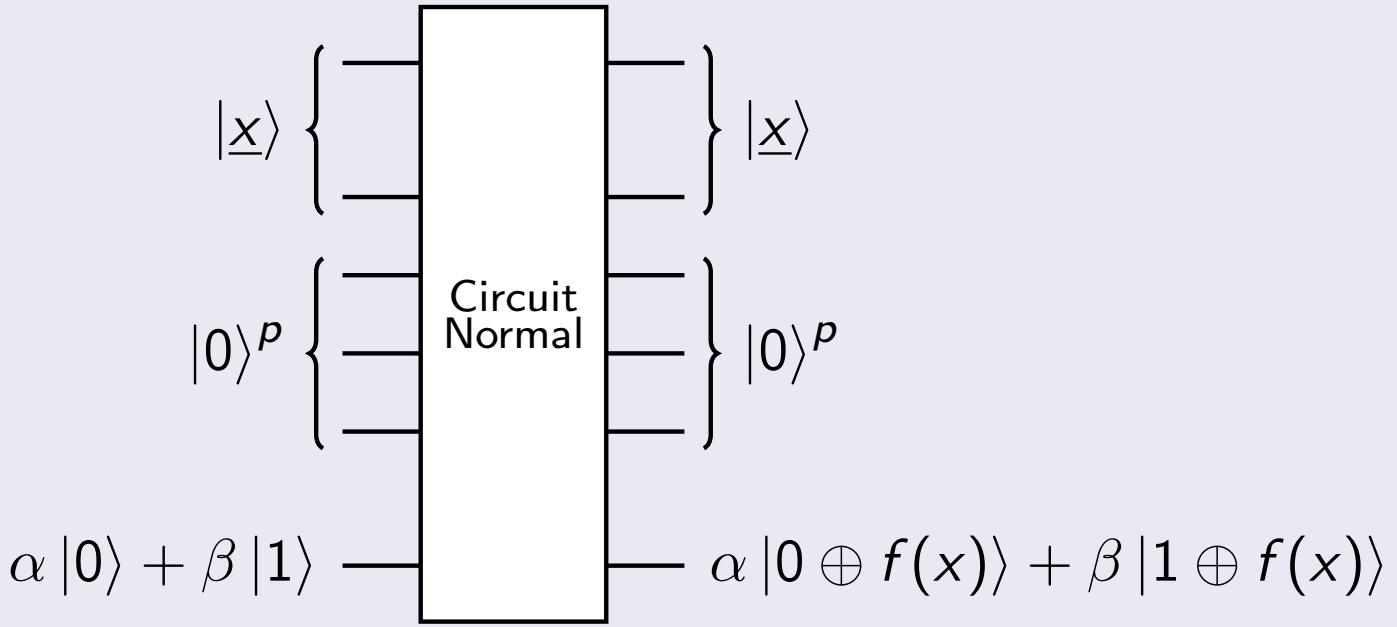


Indice : utiliser le circuit pour calculer $f(x)$, utiliser une porte CNOT au bon endroit, puis remettre x et 0^p dans leur état d'origine.

Rendre le circuit quantique

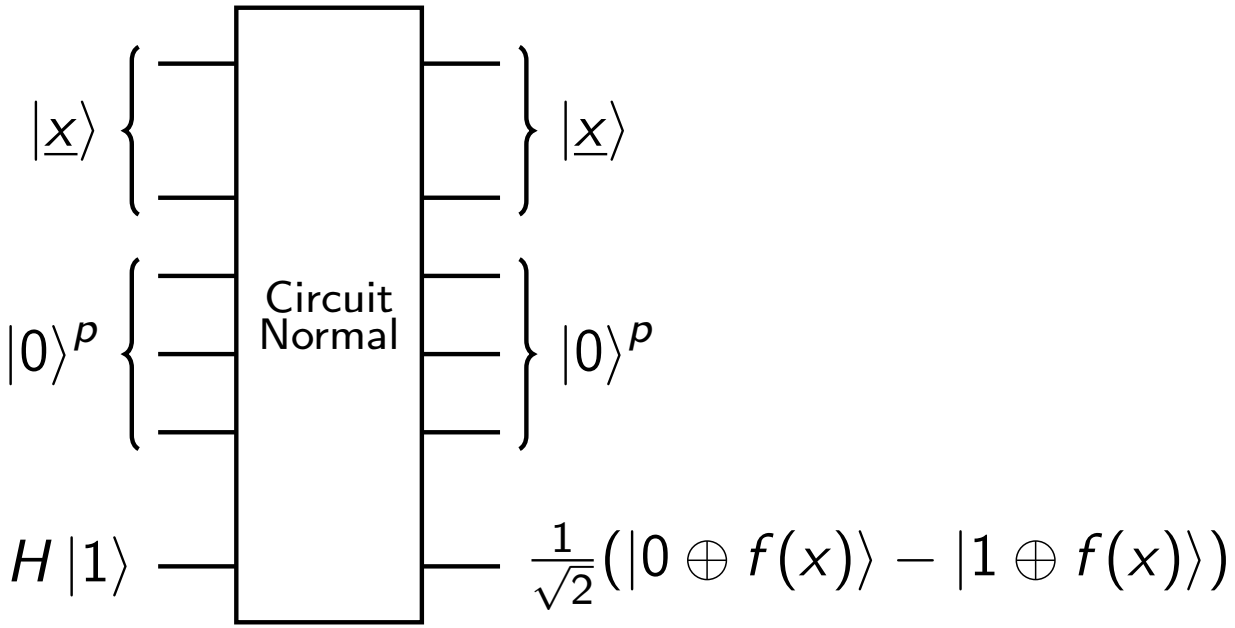
Théorème

Toute porte logique réversible peut être écrite avec des portes quantiques.



Faire apparaître $f(x)$ dans la phase

Reprenons le circuit précédent et donnons $H|1\rangle$ à la place de y.

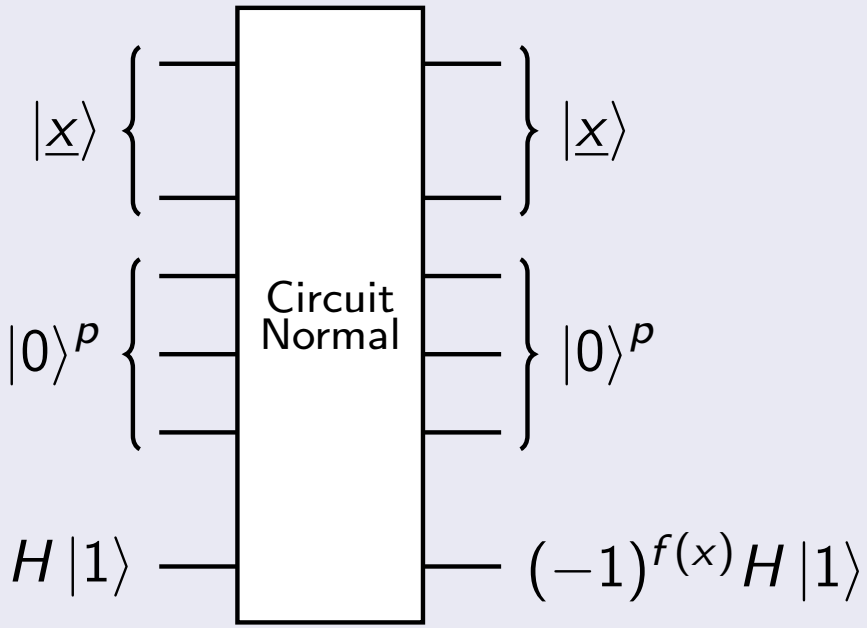


- Si $f(x) = 0$ alors $|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle = (|0\rangle - |1\rangle)$
- Si $f(x) = 1$ alors $|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle = (|1\rangle - |0\rangle)$
- Donc $H|1\rangle \oplus f(x) = (-1)^{f(x)} H|1\rangle$

Construire un oracle

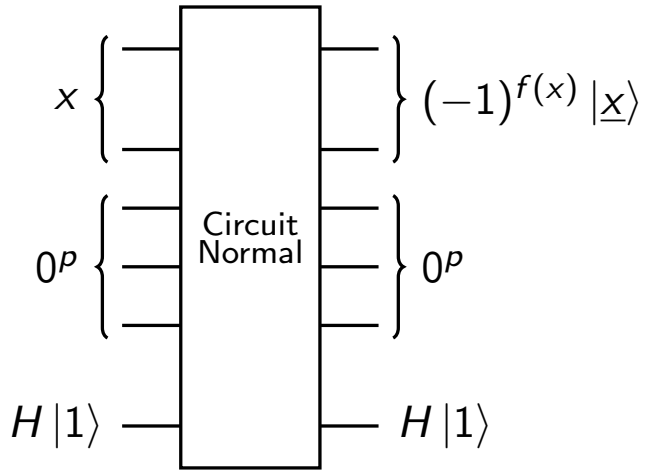
Théorème

Si je dispose d'un circuit logique qui calcule f, je peux calculer l'oracle suivant où le nombre de bits d'entrée et la profondeur sont linéaires en ceux de f.



Dernière remarque

$|\underline{x}\rangle \otimes \alpha\,|y\rangle = \alpha\,|\underline{x}\rangle \otimes |y\rangle$ Donc on a également:



Les $p+1$ derniers qbits n'interviennent donc pas dans les calculs.

Alerte confusion

Dans la version précédente de l'oracle, $|\underline{x}\rangle$ n'était pas modifié mais intervient malgré tout dans les calculs de l'algorithme de Deutsch-Jozsa.
Raison : car $(-1)^{f(x)}$ apparait dans le dernier qbit, donc l'état de x est important pour connaître l'état de ce dernier qbit.

Plan

Problème résolu par l'algorithme de Bernstein-Vazirani

Soit un nombre binaire secret $s \in \{0,1\}^n$ et $f(x) = \underline{x} \odot \underline{s} = \bigoplus_{i=1}^{n} x_i s_i$.

Problème à résoudre

Trouver s.

Efficacité de l'algorithme

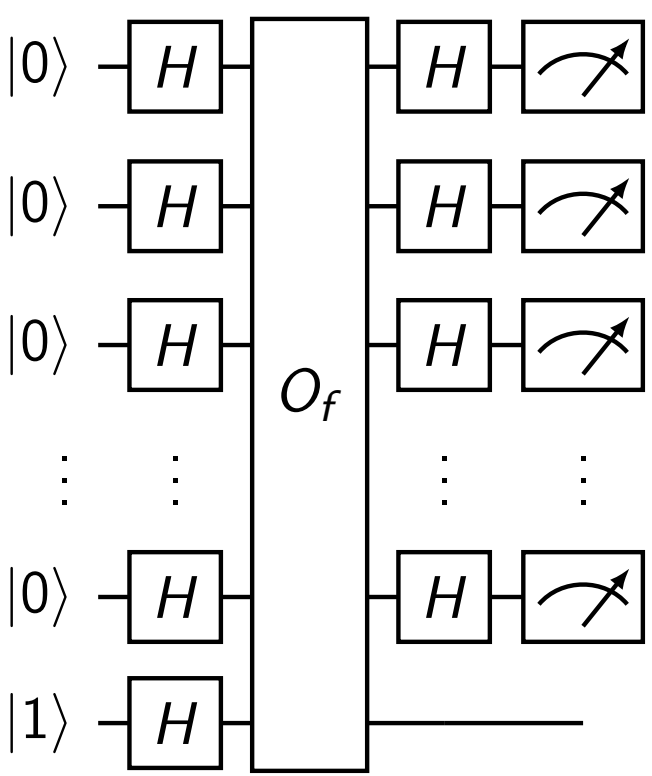
- Meilleure complexité classique : $O(n)$ appels à f
- Complexité de l'algorithme de Bernstein-Vazirani :

$$O(1) \text{ appels à } f + O(n)$$

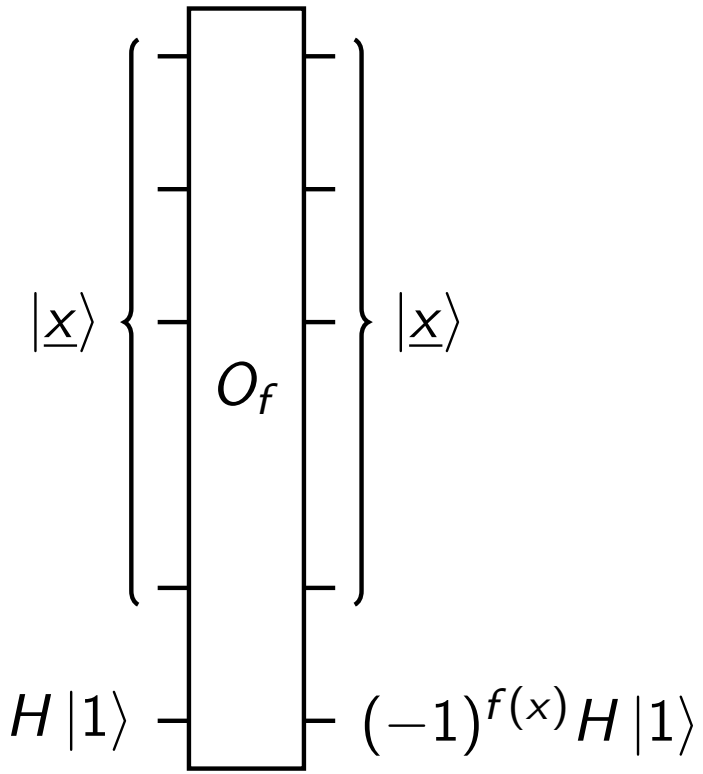
Intérêt ?

On verra plus tard.

Description de l'algorithme

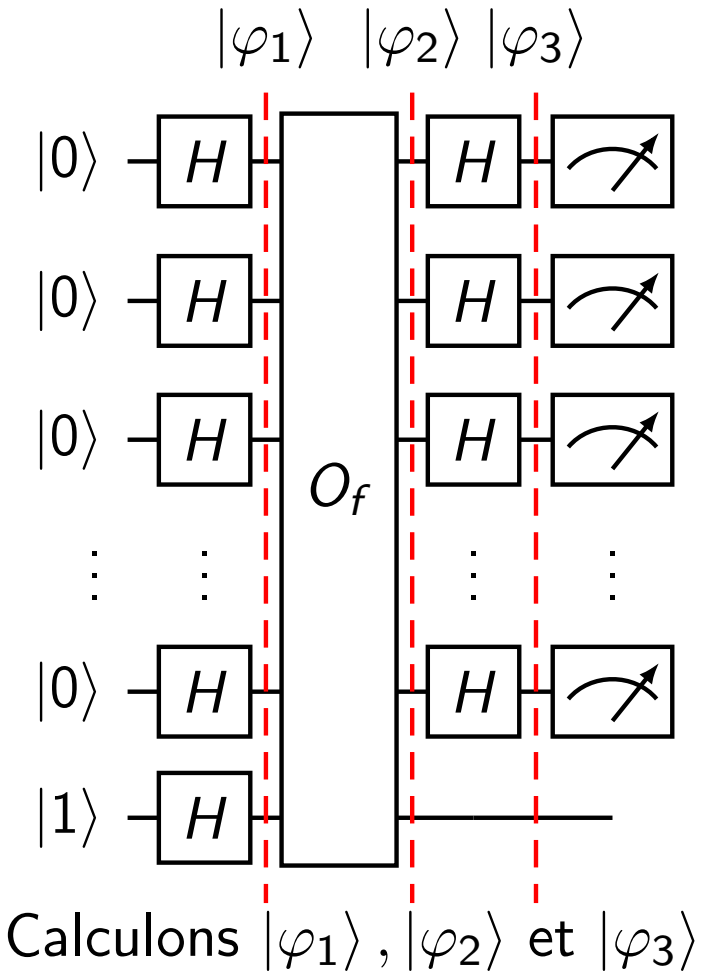


avec



Ce circuit est identique à celui de Deutsch-Jozsa, à l'oracle près. La sortie mesurée est s avec une probabilité égale à 1.

Preuve de l'exactitude



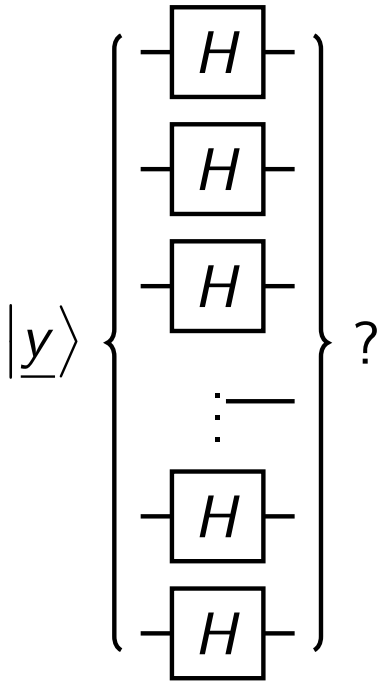
$|\varphi_1\rangle$

$$|\varphi_1\rangle = H^{\otimes n} |00\ldots0\rangle \otimes H |1\rangle$$
$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\underline{x}\rangle \otimes H |1\rangle$$

$|\varphi_2\rangle$

$$
\begin{aligned}
|\varphi_2\rangle &= O_f\,|\varphi_1\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\underline{x}\rangle \otimes (-1)^{f(x)} H\,|1\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}\,|\underline{x}\rangle \otimes H\,|1\rangle \\
&= \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{\underline{s}\cdot\underline{x}}\,|\underline{x}\rangle \right) \otimes H\,|1\rangle
\end{aligned}
$$

Petite pause : transformée de fourrier discrète $H^{\otimes n}$



Exercice : soit $\underline{y} \in \{0,1\}^n$ montrer que

$$H^{\otimes n} |\underline{y}\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{\underline{k} \odot \underline{y}} |\underline{k}\rangle.$$

On reviendra dessus une autre fois.

On reprend, $|\varphi_2\rangle$

$$
\begin{aligned}
|\varphi_2\rangle &= O_f\,|\varphi_1\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\underline{x}\rangle \otimes (-1)^{f(x)} H\,|1\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}\,|\underline{x}\rangle \otimes H\,|1\rangle \\
&= \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{\underline{s}\cdot\underline{x}}\,|\underline{x}\rangle \right) \otimes H\,|1\rangle \\
&= \left(H^{\otimes n}\,|\underline{s}\rangle\right) \otimes H\,|1\rangle
\end{aligned}
$$

On reprend, $|\varphi_3\rangle$

$$\begin{aligned}
|\varphi_3\rangle &= \left(H^{\otimes n} \otimes Id\right) |\varphi_2\rangle \\
&= \left(H^{\otimes n} \otimes Id\right) \left(H^{\otimes n} |\underline{s}\rangle\right) \otimes H|1\rangle \\
&= \left(H^{\otimes n} H^{\otimes n} |\underline{s}\rangle\right) \otimes H|1\rangle \\
&= |\underline{s}\rangle \otimes H|1\rangle
\end{aligned}$$

Ainsi la mesure des n premiers qbits donne s.

Plan

Problème résolu par l'algorithme de Grover

Soit un nombre binaire secret $s \in \{0,1\}^n$ et $f(x) = 1$ si $x = s$ et 0 sinon.

Problème à résoudre

Trouver s.

Applications importantes par exemple en bases de données ou en cassage de fonction de hachage.

Efficacité de l'algorithme

- Meilleure complexité classique : $O(2^n)$ appels à f
- Complexité de l'algorithme de Grover :

$$O(\sqrt{2^n}) \text{ appels à } f + O(\sqrt{2^n} n^2)$$

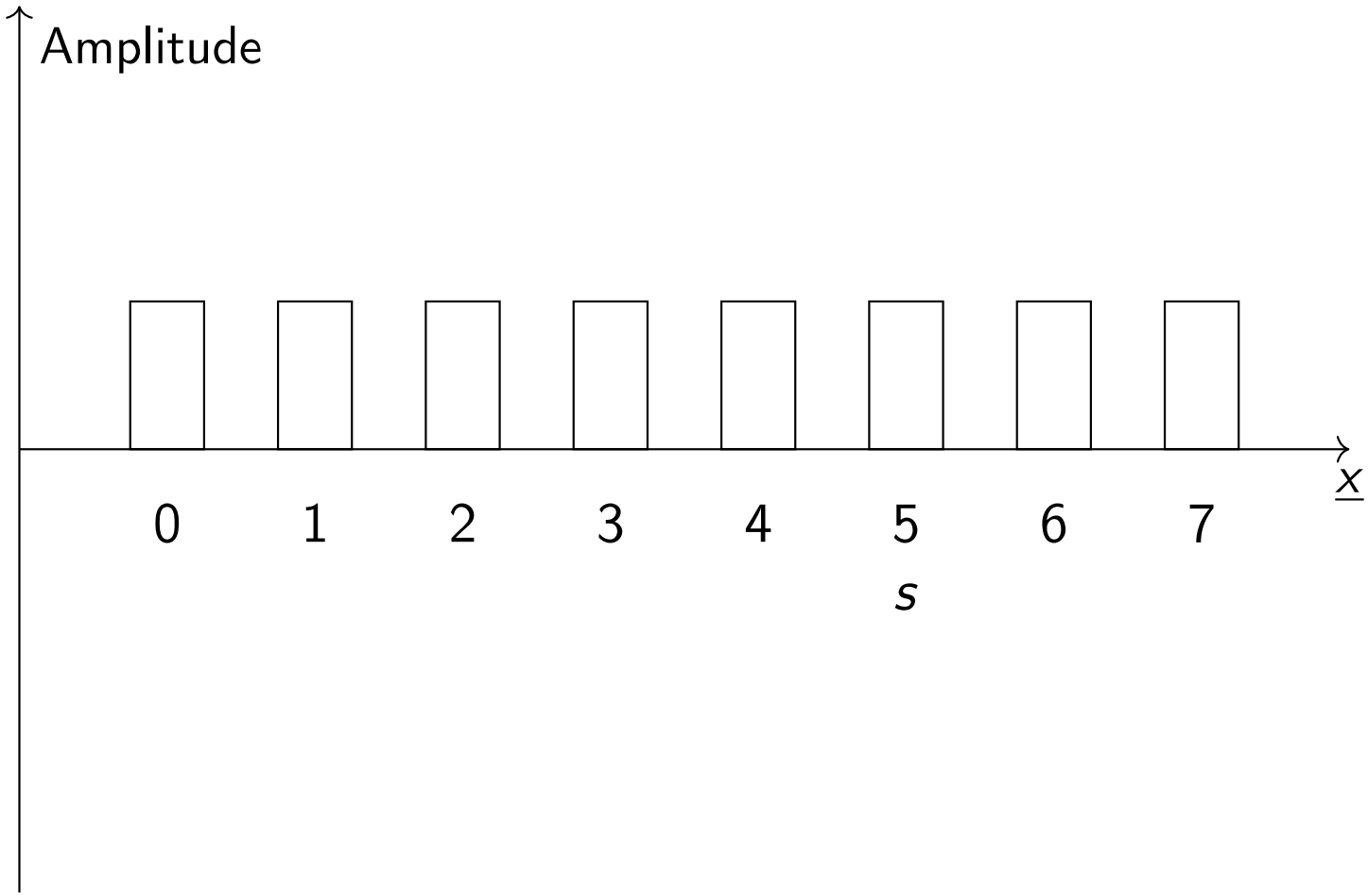
L'accélération est quadratique, mais pas exponentielle.

Description de l'algorithme

- Entrée de taille $n+1$: $|000\ldots01\rangle$
- Effectuer une transformation de Hadamard
- Appliquer un *oracle*
- Appliquer une *transformation de Grover*
- Recommencer ces 2 applications *environ* $\frac{\pi}{4}\sqrt{2^n}$ fois
- Mesurer les n premiers qbits pour trouver s avec une probabilité supérieur à $1 - \frac{4}{2^n}$

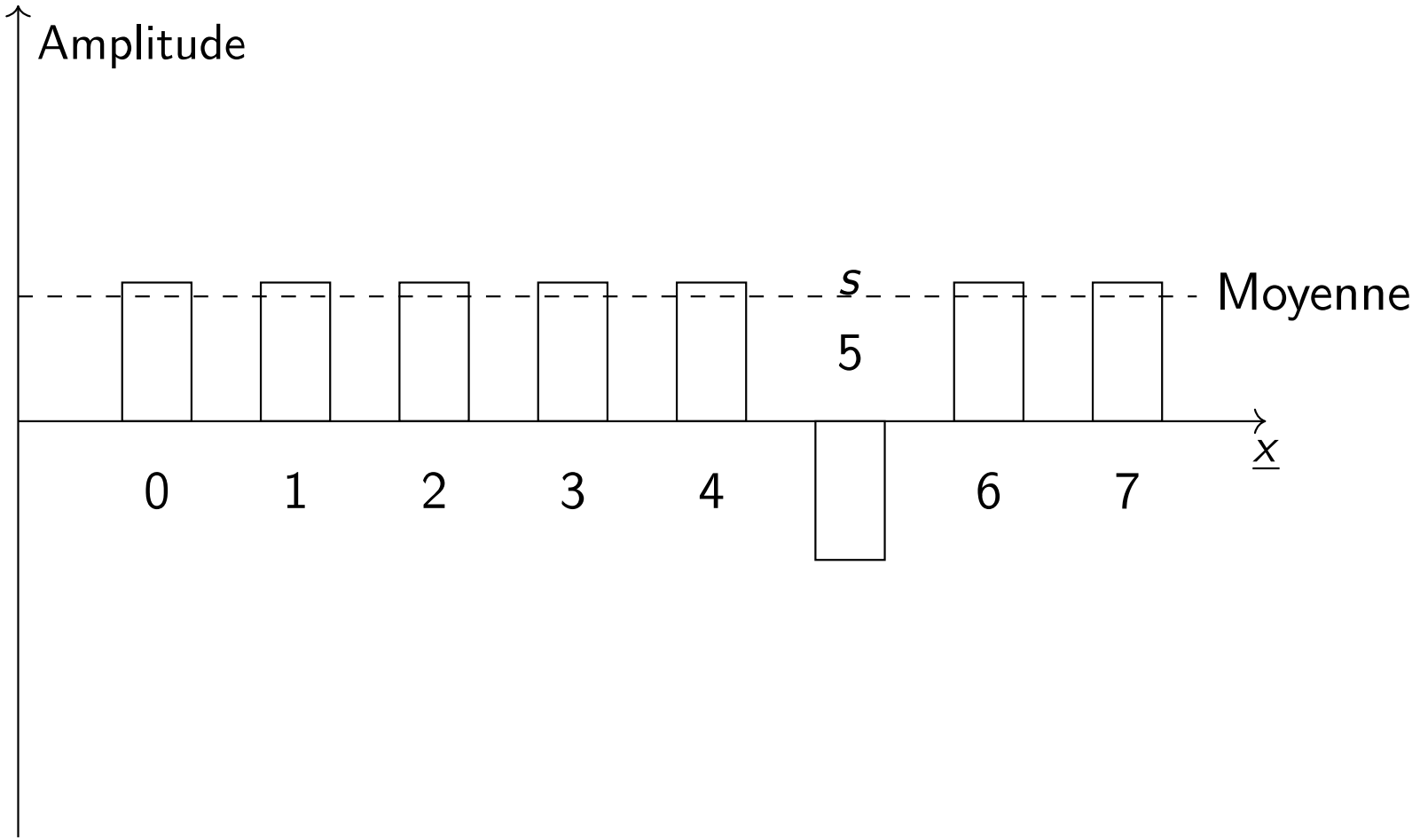
Description de l'algorithme en dessin

Après Hadamard, chaque qbit a la même amplitude $1/\sqrt{2^n}$.



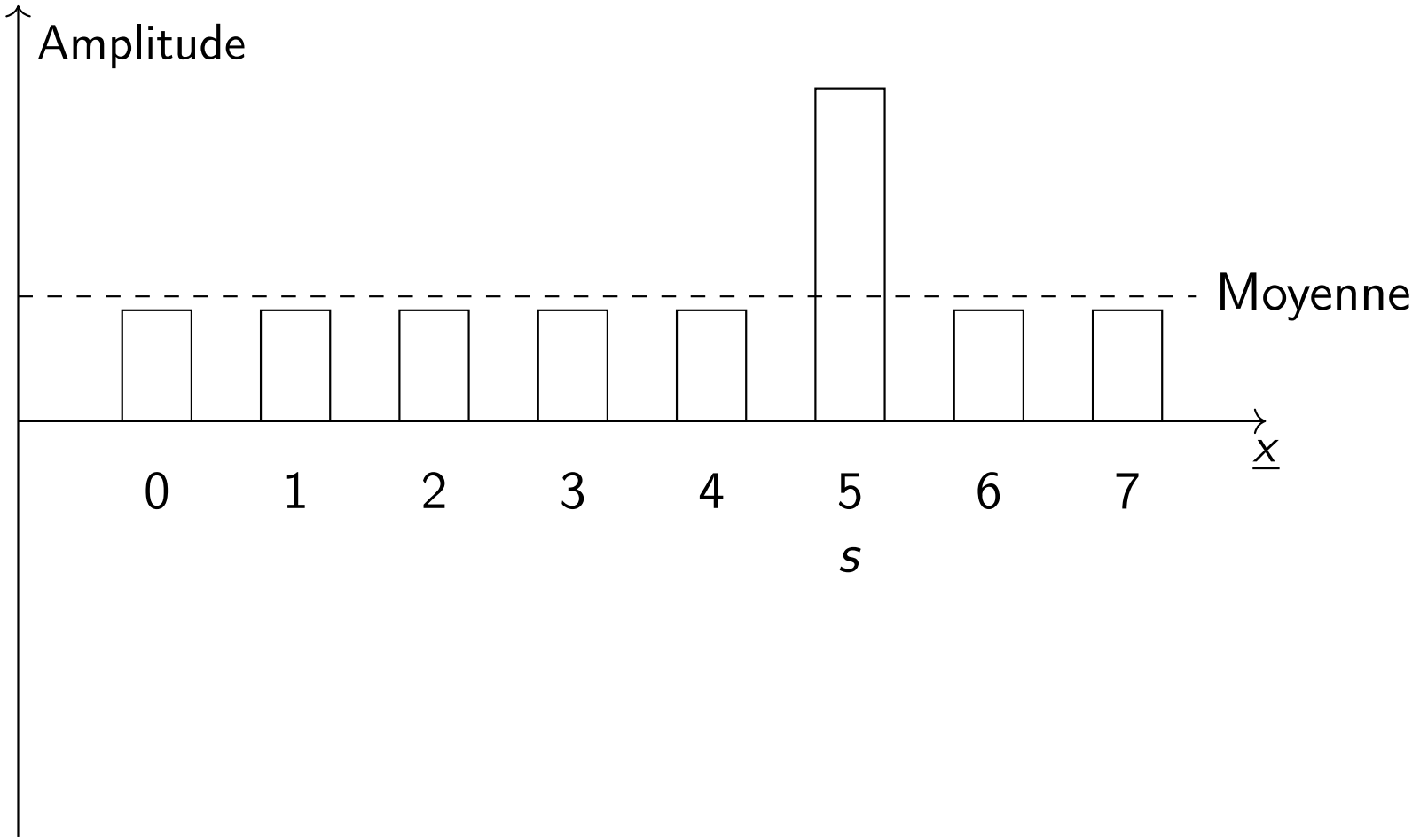
Description de l'algorithme en dessin

Après l'oracle, l'amplitude de s est inversée.

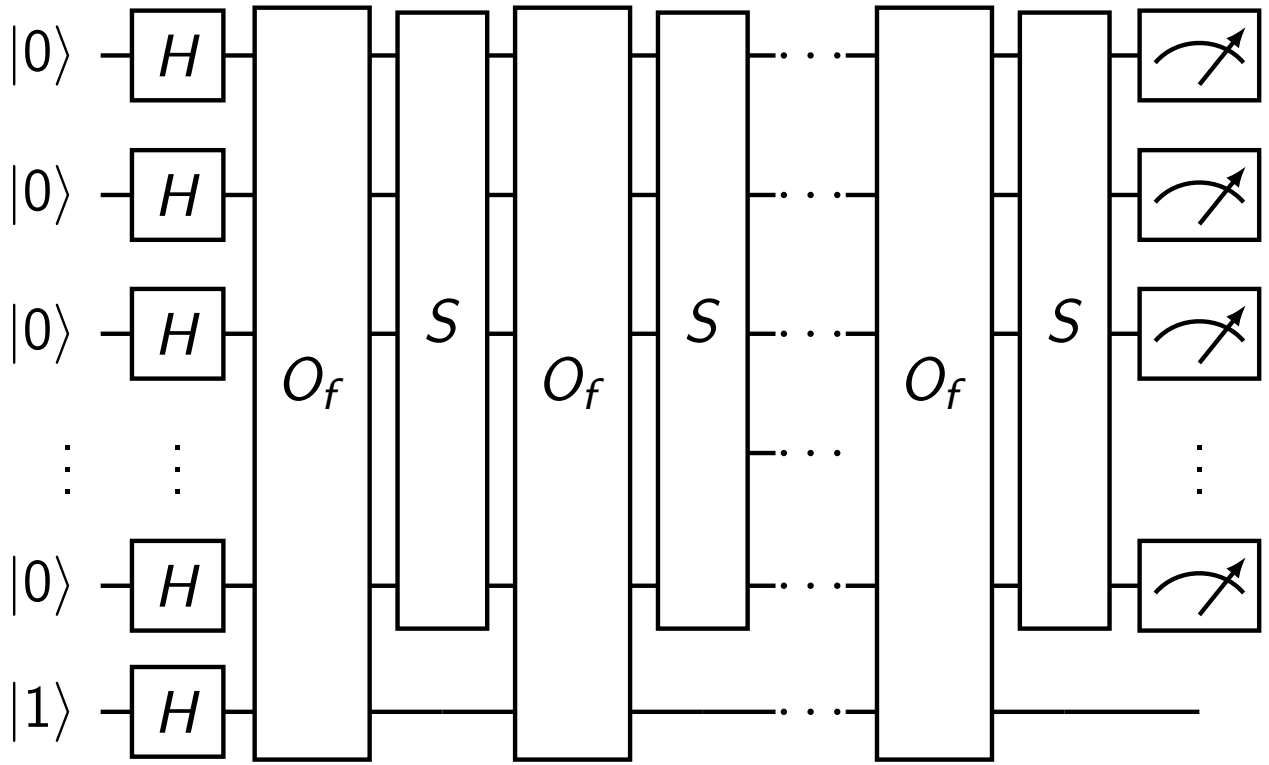


Description de l'algorithme en dessin

Puis on effectue une symétrie par rapport à la moyenne.

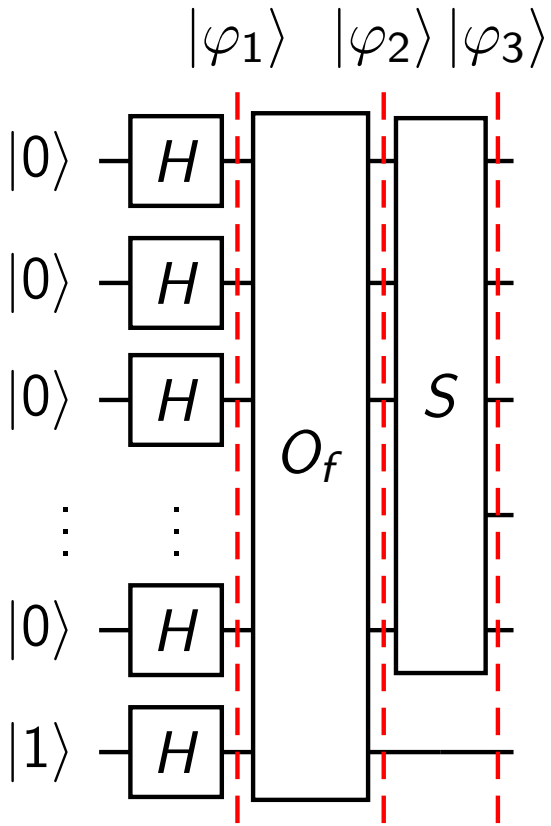


Description de l'algorithme



O_f est nommé l'oracle, S est la transformation de Grover, la mesure renvoie s avec une forte probabilité.

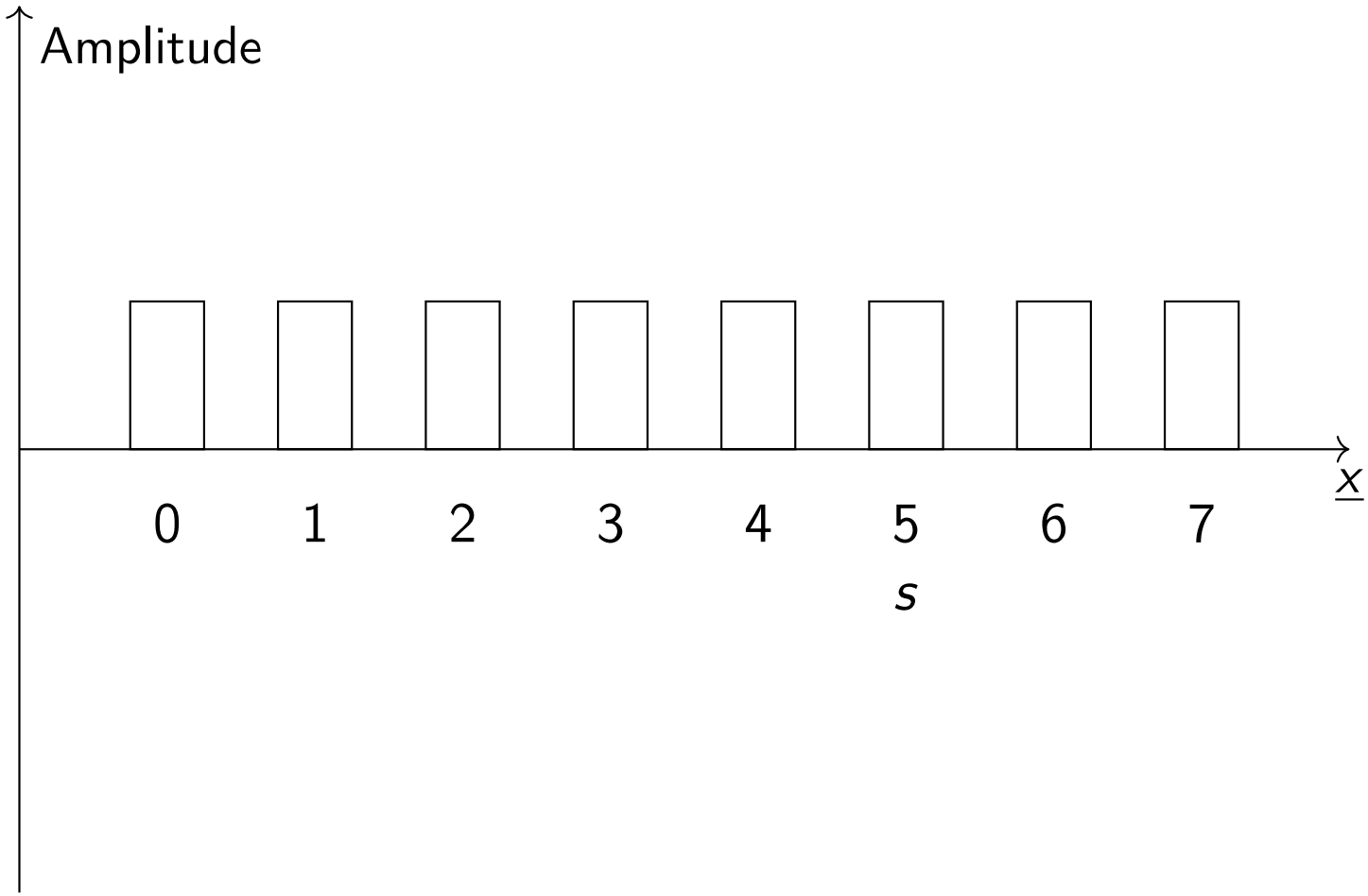
Preuve de l'algorithme



Etudions une itération de l'algorithme.

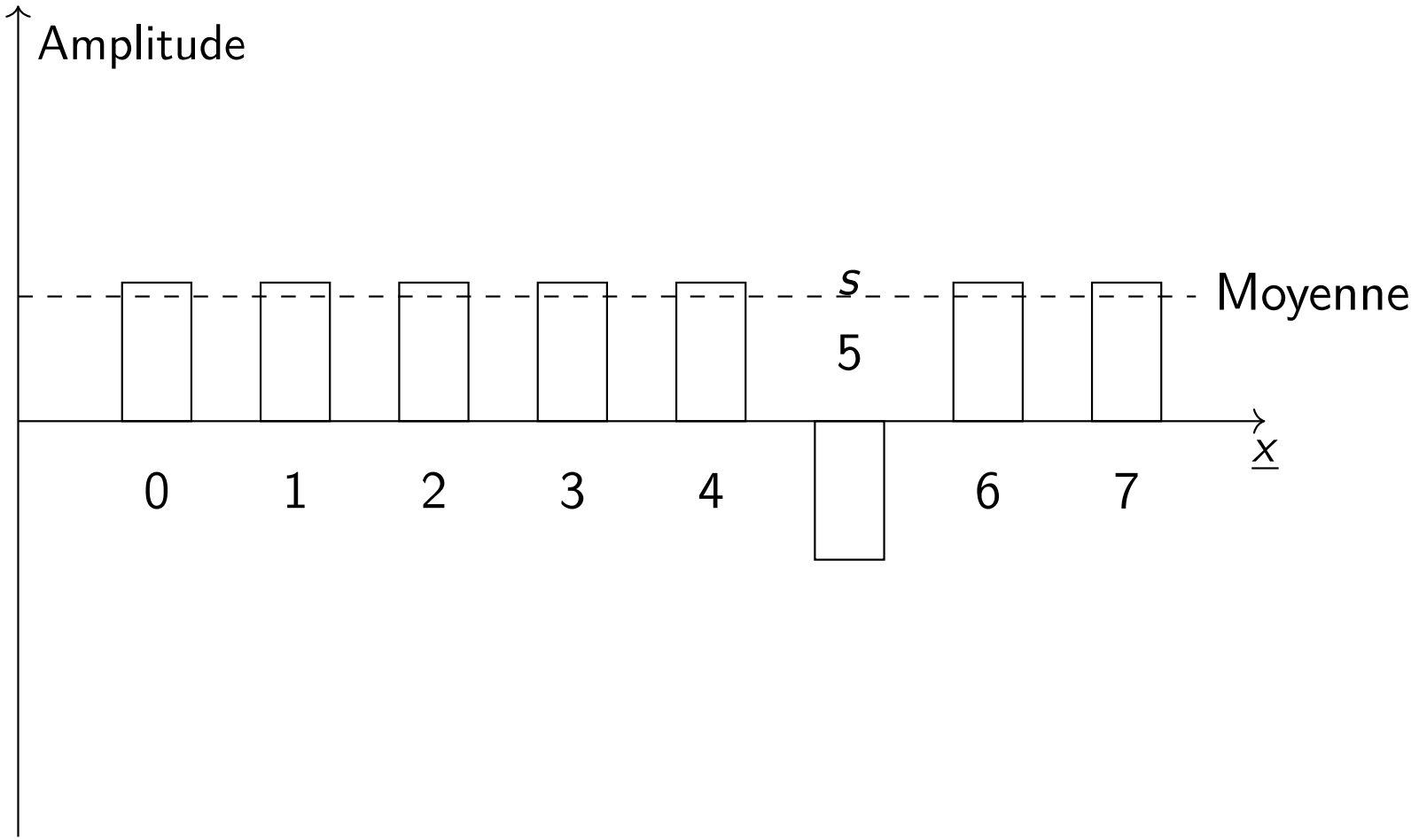
Description de l'algorithme en dessin

$|\varphi_1\rangle$ ressemble à ça.



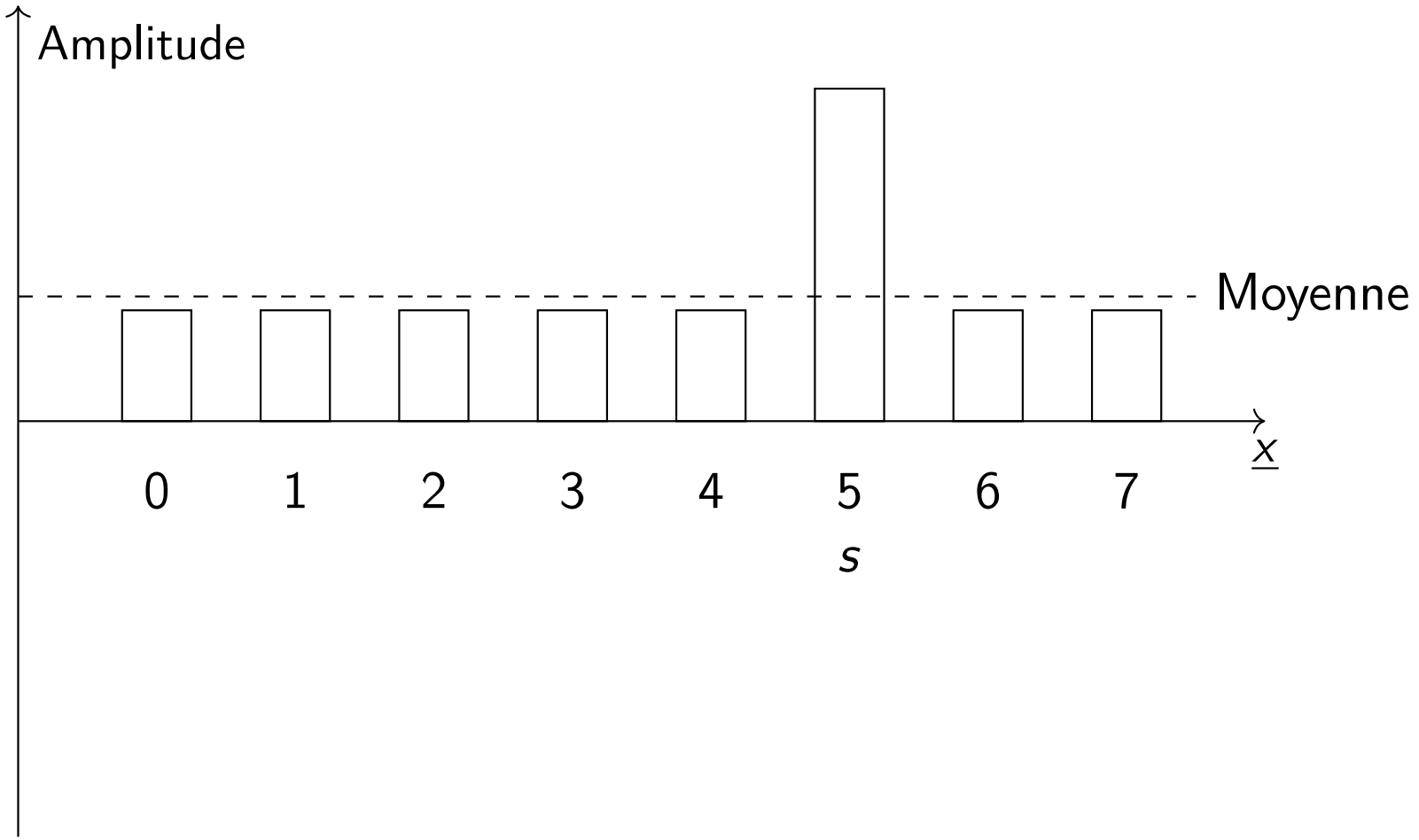
Description de l'algorithme en dessin

$|\varphi_2\rangle$ devrait ressembler à ça.



Description de l'algorithme en dessin

$|\varphi_3\rangle$ devrait ressembler à ça.



$|\varphi_1\rangle$

$$|\varphi_1\rangle = H^{\otimes n} |00\ldots0\rangle \otimes H |1\rangle$$
$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\underline{x}\rangle \otimes H |1\rangle$$

$|\varphi_2\rangle$

$$
\begin{aligned}
|\varphi_2\rangle &= O_f \, |\varphi_1\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\underline{x}\rangle \otimes (-1)^{f(x)} H \, |1\rangle \\
&= \frac{1}{\sqrt{2^n}} \left(\sum_{x=0}^{2^n-1} (-1)^{f(x)} \, |\underline{x}\rangle \right) \otimes H \, |1\rangle \\
&= \frac{1}{\sqrt{2^n}} \left(- |\underline{s}\rangle + \sum_{x \neq s} |\underline{x}\rangle \right) \otimes H \, |1\rangle
\end{aligned}
$$

On observe bien sur le calcul ici que l'amplitude de s est inversée, comme annoncé au départ.

$|\varphi_3\rangle$

$$|\varphi_3\rangle = (S \otimes Id)\,|\varphi_2\rangle$$

Que vaut S ? S est une symétrie par rapport au vecteur $H^{\otimes n}\,|00\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\underline{x}\rangle$.

Opérateur de Symétrie

Définition

La symétrie S_φ par rapport au qbit $|\varphi\rangle$ est la matrice suivante :

$$S_\varphi = 2\,|\varphi\rangle\langle\varphi| - Id$$

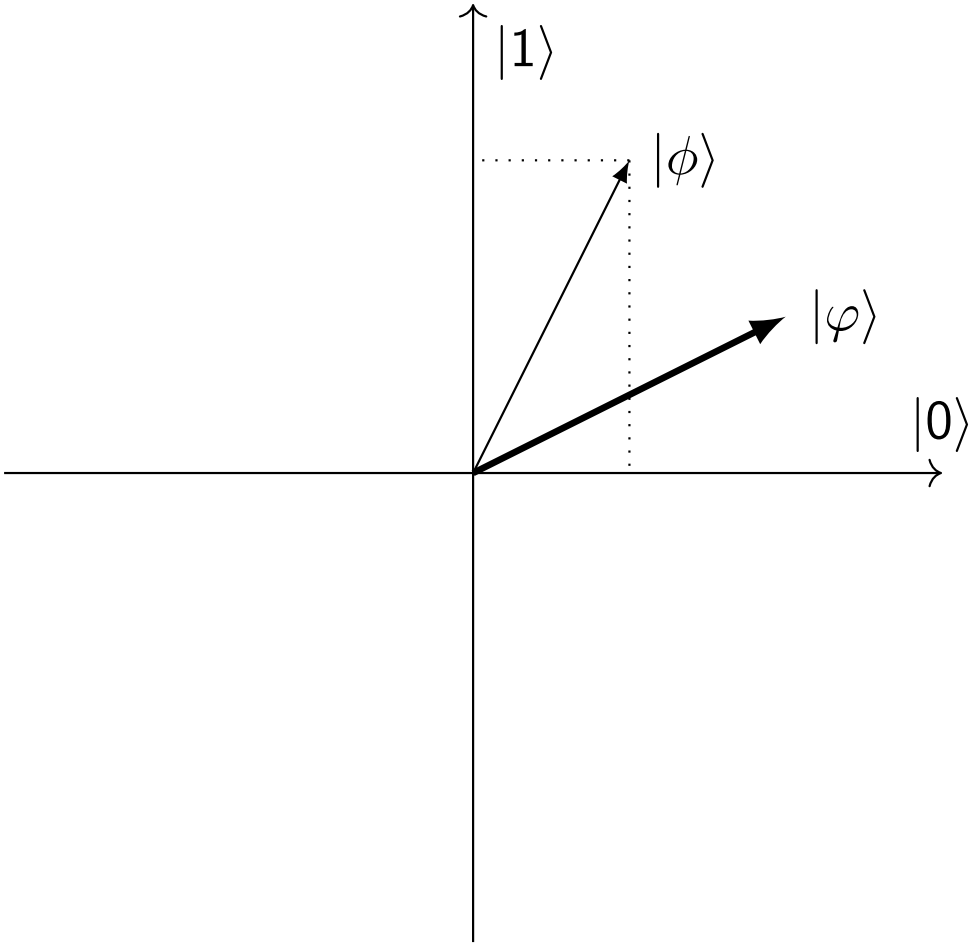
Propriété

$S_\varphi\,|\varphi\rangle = |\varphi\rangle$.
Si $|\phi\rangle \perp |\varphi\rangle$ alors $S_\varphi\,|\phi\rangle = -\,|\phi\rangle$.

(Rappel : $\langle\varphi|\varphi\rangle = \||\varphi\rangle\| = 1$ et $\langle\varphi|\phi\rangle = 0 \Leftrightarrow |\phi\rangle \perp |\varphi\rangle$)

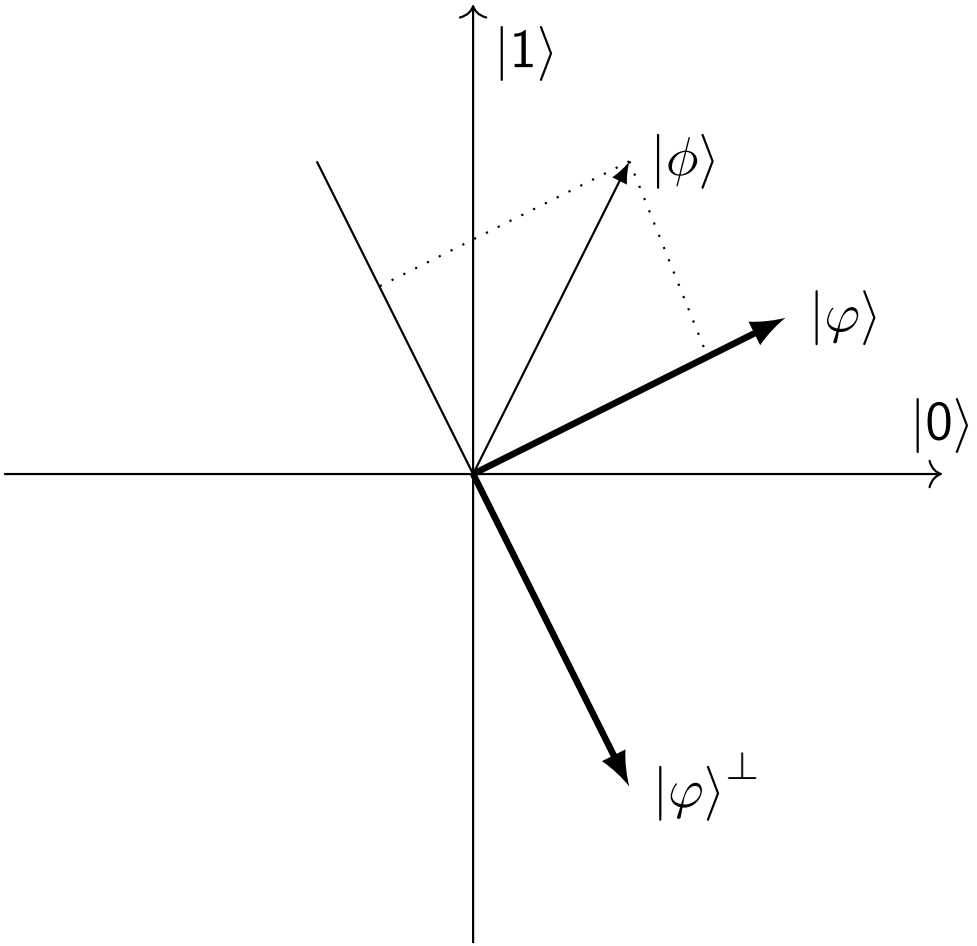
Opérateur de Symétrie : exemple à 1 qbit

Soient $|\phi\rangle$ et $|\varphi\rangle$ dans la base $|0\rangle, |1\rangle$.



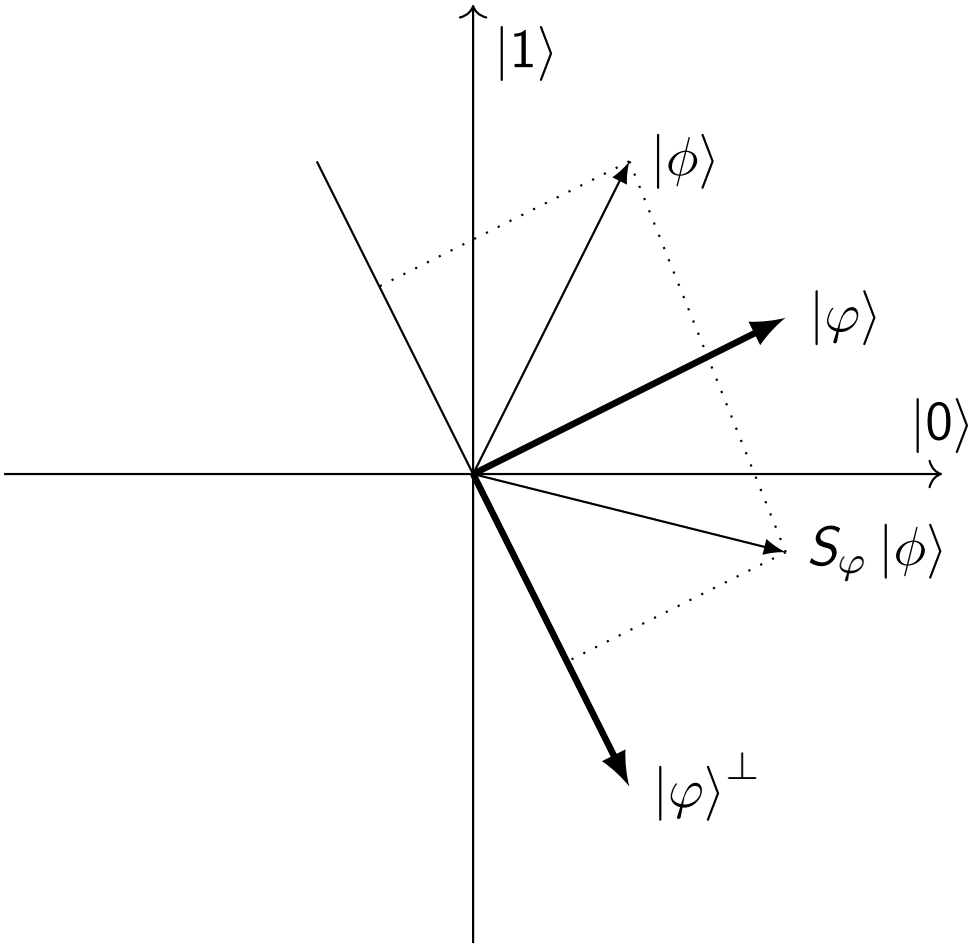
Opérateur de Symétrie : exemple à 1 qbit

Changement de base orthonormée, nouvelle base : $|\varphi\rangle, |\varphi\rangle^{\perp}$.



Opérateur de Symétrie : exemple à 1 qbit

La symétrie inverse la composante de $|\varphi\rangle^{\perp}$.



Exercice : $S\left|\underline{x}\right\rangle$ dans le cas général

$$\begin{aligned} S &= 2\left(H^{\otimes n}\left|00\ldots0\right\rangle\left\langle 00\ldots0\right|H^{\otimes n}\right) - Id \\ &= 2\left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}\left|\underline{x}\right\rangle \cdot \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}\left\langle\underline{x}\right|\right) - Id \end{aligned}$$

Exercice

Montrer que $S\left|\underline{x}\right\rangle = \frac{2}{2^n}\sum_{y}\left|\underline{y}\right\rangle - \left|\underline{x}\right\rangle$ pour tout $x \in [\![0; 2^n - 1]\!]$.

$|\varphi_3\rangle$

$$
\begin{aligned}
|\varphi_3\rangle &= (S \otimes Id)\,|\varphi_2\rangle \\
&= (S \otimes Id)\left(\frac{1}{\sqrt{2^n}}\left(-|\underline{s}\rangle + \sum_{x\neq s}|\underline{x}\rangle\right) \otimes H\,|1\rangle\right) \\
&= \left(\frac{1}{\sqrt{2^n}}\left(-S\,|\underline{s}\rangle + \sum_{x\neq s} S\,|\underline{x}\rangle\right)\right) \otimes H\,|1\rangle \\
&= \frac{1}{2^n\sqrt{2^n}}\left((2^n-4)\sum_{y\neq s}|\underline{y}\rangle + (3\cdot 2^n - 4)\,|\underline{s}\rangle\right) \otimes H\,|1\rangle
\end{aligned}
$$

On observe que l'amplitude de $|\underline{s}\rangle$ dépasse le triple de l'amplitude des autres qbits de base.

Exercice : vérifier que $\||\varphi_3\rangle\| = 1$.

Petite vérification

Amplitude de $|\underline{s}\rangle$

Comme annoncé dans les graphiques en début de section, l'opération S effectue une symétrie par rapport à la moyenne des amplitudes de $|\varphi_2\rangle$.

Preuve :

- dans $|\varphi_2\rangle$: $2^n - 1$ amplitudes égales à $\frac{1}{\sqrt{2^n}}$ et 1 amplitude égale $-\frac{1}{\sqrt{2^n}}$
- moyenne : $M = \frac{1}{\sqrt{2^n}} \cdot \frac{(2^n-2)}{2^n}$
- Le symétrique de $\frac{1}{\sqrt{2^n}}$ par rapport à M est $\frac{1}{2^n\sqrt{2^n}} \cdot (2^n - 4)$
- Le symétrique de $\frac{-1}{\sqrt{2^n}}$ par rapport à M est $\frac{1}{2^n\sqrt{2^n}} \cdot (3 \cdot 2^n - 4)$

Comment implanter la porte S

Exercice

Coder la porte S avec $O(n)$ portes H et des portes de toffoli.

Indice :

- coder la porte S_0 qui inverse tout qbit orthogonal à $|\underline{0}\rangle$, pour cela utiliser un oracle avec une fonction f bien choisie
- des qbits supplémentaires sont nécessaires pour coder cet oracle.
- autour de S_0, effectuer un changement de base orthonormée pour envoyer $H^{\otimes n}|00\ldots0\rangle$ sur $|00\ldots0\rangle$.

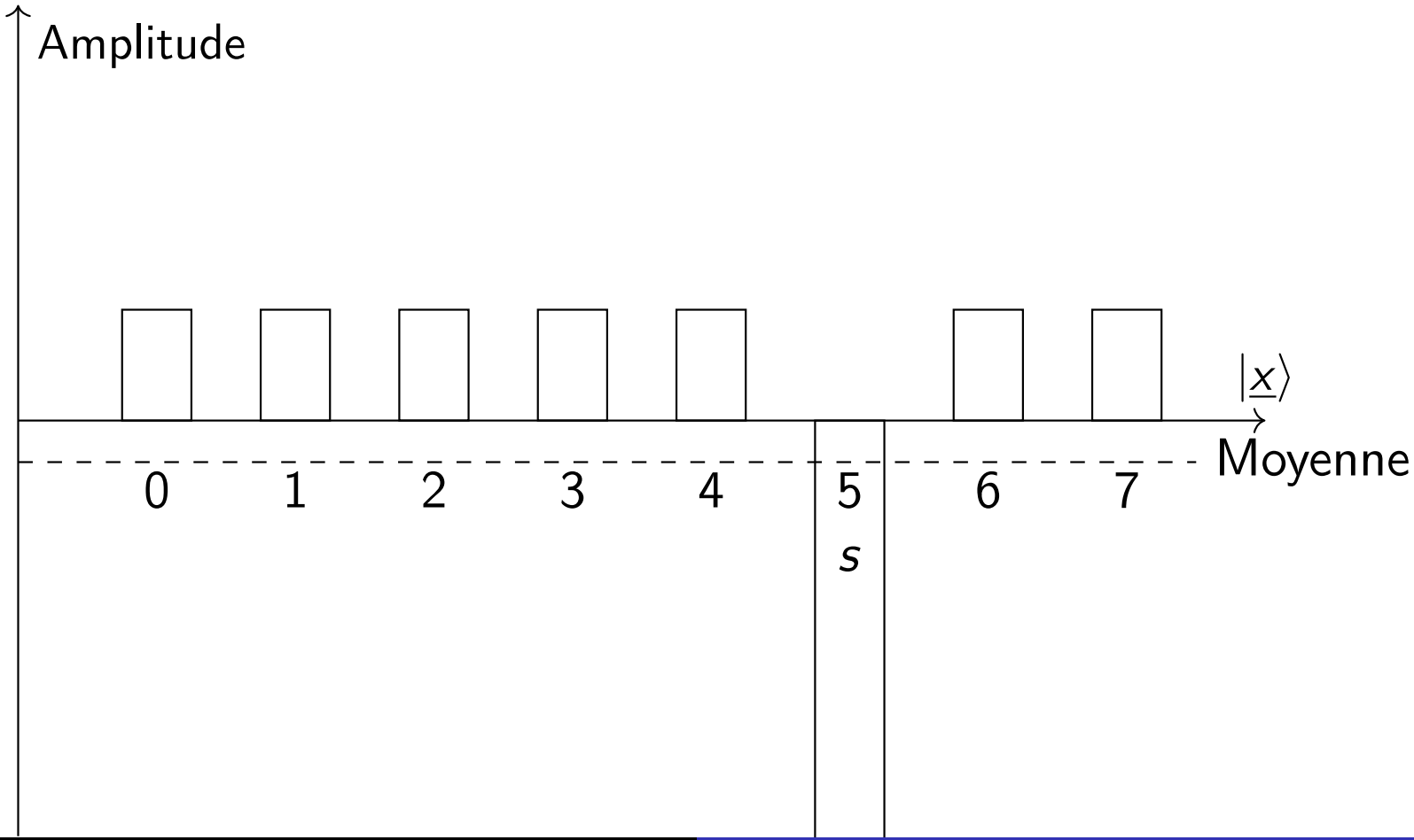
Généralisation à n'importe quelle itération

On peut montrer qu'à chaque itération, l'opérateur $S \circ O_f$ effectue ces deux opérations d'inversion de l'amplitude de $|\underline{s}\rangle$ suivie de la symétrie par rapport à la moyenne.

A chaque itération, l'amplitude de $|\underline{s}\rangle$ augmente et donc la probabilité de mesurer $|\underline{s}\rangle$ aussi.

Généralisation à n'importe quelle itération

Mais, à partir d'un certain rang, on se retrouve dans le cas où la moyenne devient négative.



Généralisation à n'importe quelle itération

On peut montrer qu'à chaque itération, l'opérateur $S \circ O_f$ effectue ces deux opérations d'inversion de l'amplitude de $|\underline{s}\rangle$ suivie de la symétrie par rapport à la moyenne.

Mais!

À partir d'un certain rang, on se retrouve dans le cas où la moyenne devient négative, et l'amplitude de $|\underline{s}\rangle$ diminue.

Après combien d'itérations faut-il s'arrêter ? Réponse : environ $\frac{\pi}{4}\sqrt{2^n}$

- Pourquoi $\frac{\pi}{4}\sqrt{2^n}$?
- $\Rightarrow$ calculs compliqués

$\Rightarrow$ Interprétation des amplitudes non adaptée pour répondre à la question.

Explication par rotation

L'opérateur $S \circ O_f$ peut être également vu comme une rotation dans le plan $\mathcal{P}$ défini par les deux vecteurs $|\underline{s}\rangle$ et $\sum_{x \neq s} |\underline{x}\rangle$.

Théorème

$|\varphi_1\rangle \in \mathcal{P}$

- Si $|\varphi\rangle \in \mathcal{P}$ alors $O_f |\varphi\rangle \in \mathcal{P}$
- Si $|\varphi\rangle \in \mathcal{P}$ alors $S |\varphi\rangle \in \mathcal{P}$

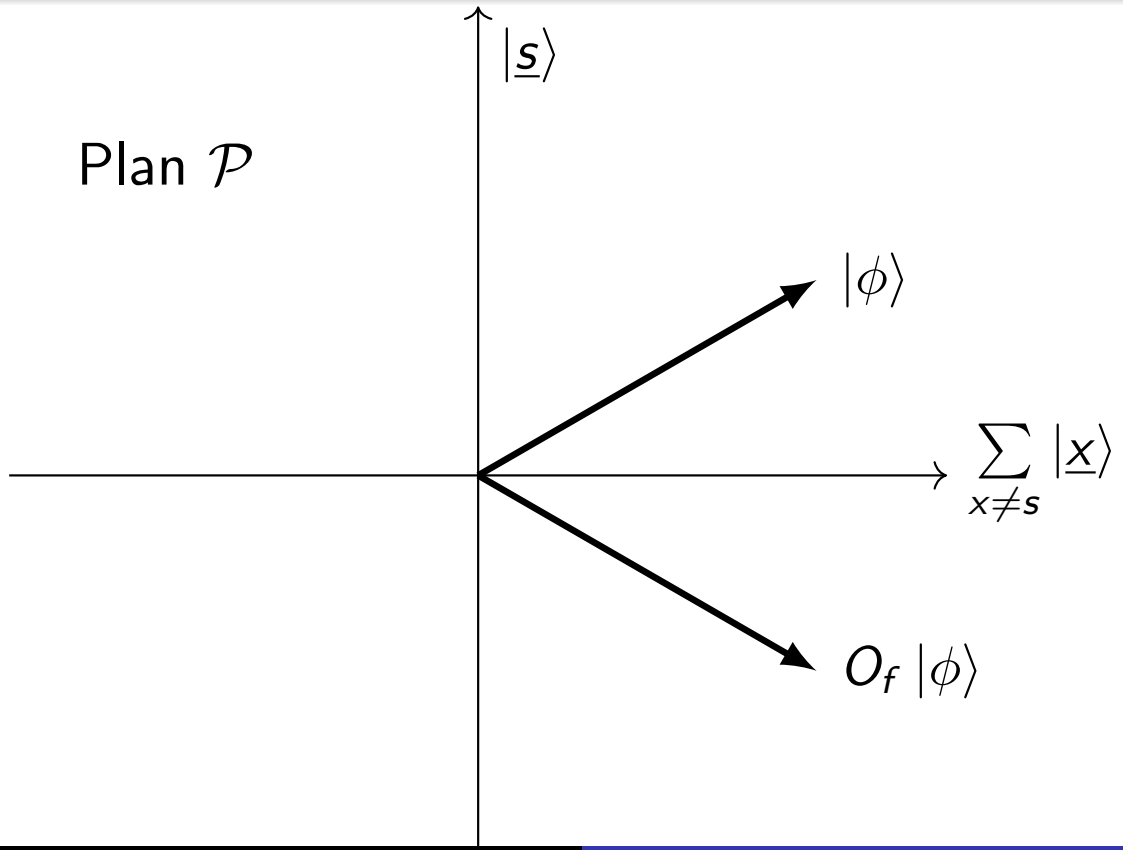
Par récurrence, tous les états successifs des qbits du circuit sont dans $\mathcal{P}$

Explication par rotation

Théorème

Dans $\mathcal{P}$, l'opérateur O_f est une symétrie d'axe $\sum_{x \neq s} |\underline{x}\rangle$.

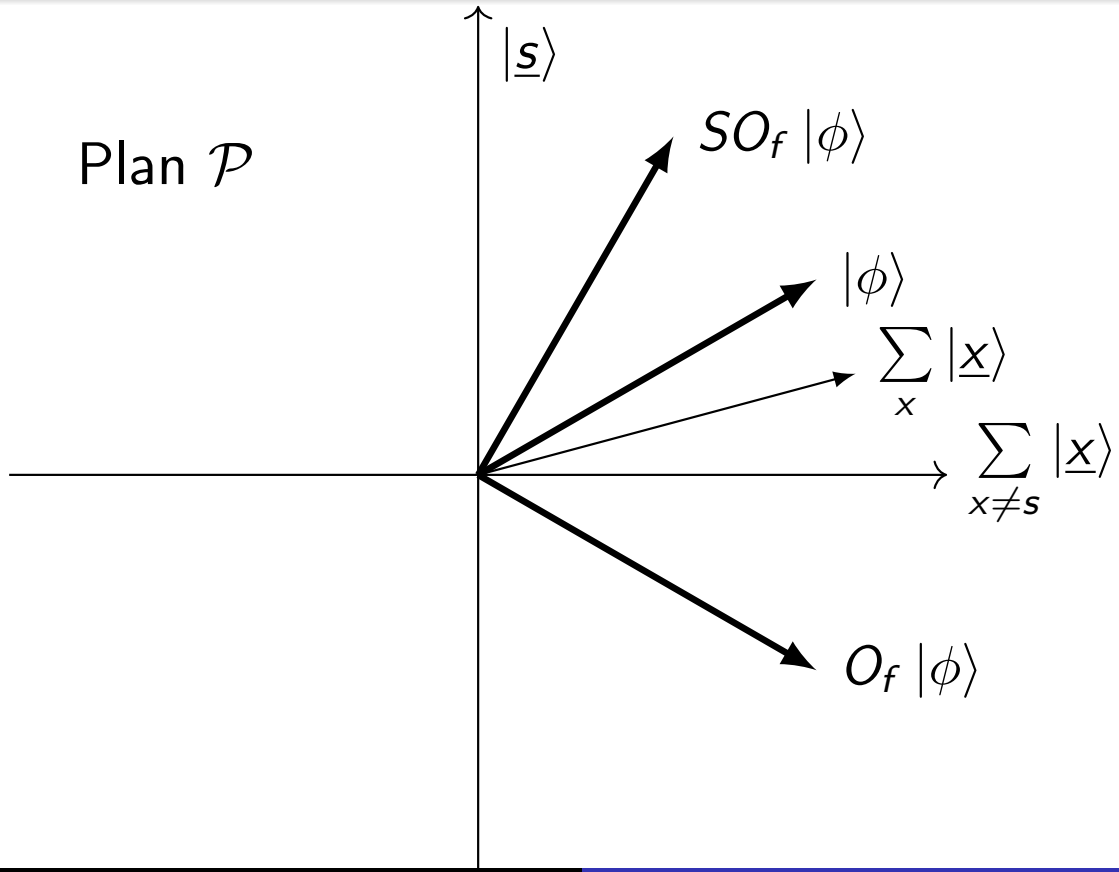
/!\ Dans ce dessin et ceux qui suivent, le dernier qbit est ignoré.



Explication par rotation

Théorème

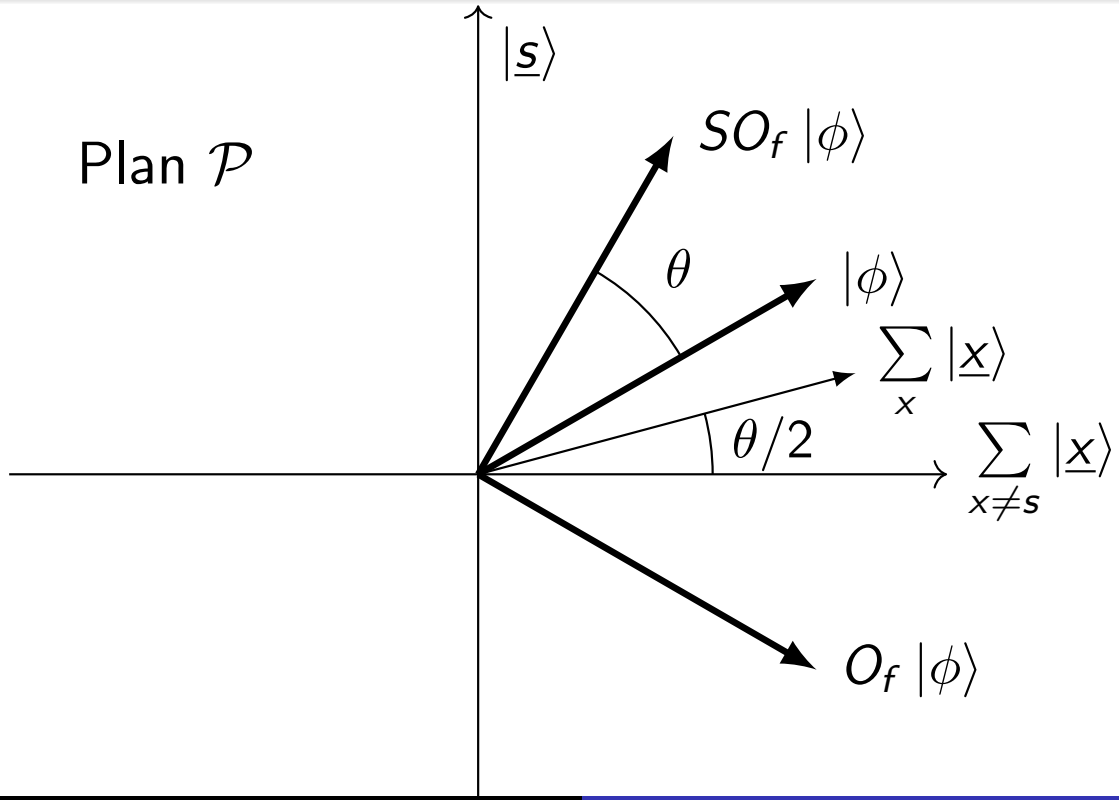
Dans $\mathcal{P}$, l'opérateur S est une symétrie d'axe $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\underline{x}\rangle$.



Explication par rotation

Théorème

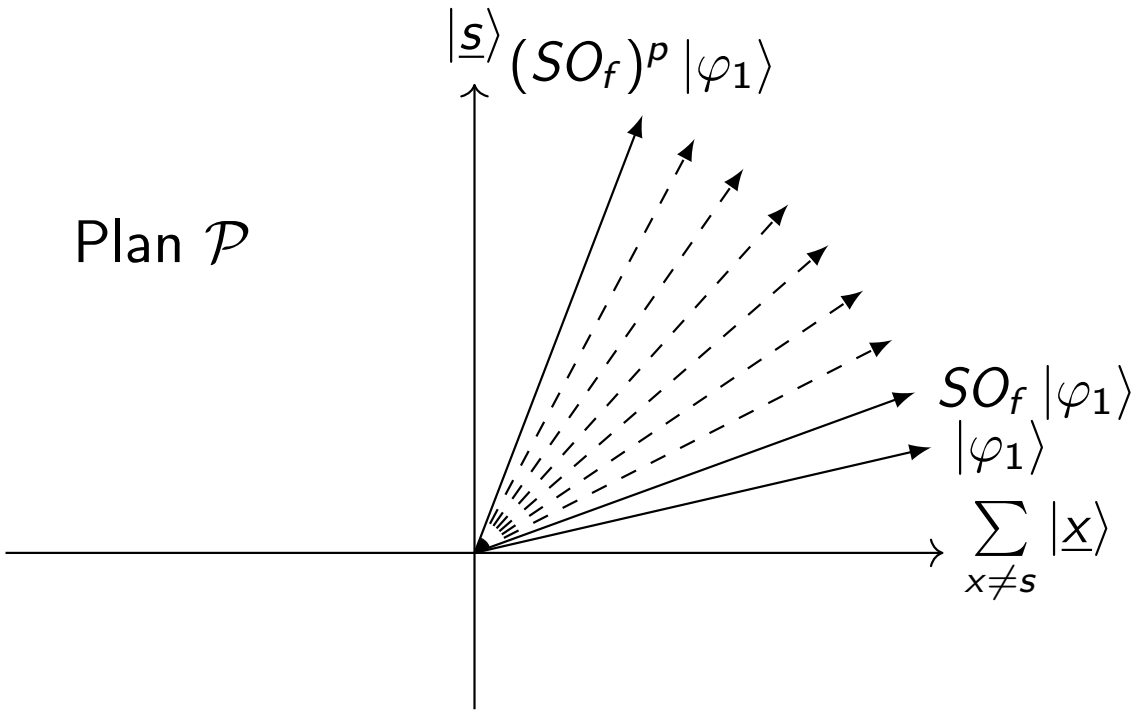
Dans $\mathcal{P}$, l'opérateur $S \circ O_f$ est une rotation centrée en l'origine d'angle θ où $\frac{\theta}{2}$ est l'angle entre $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\underline{x}\rangle$ et $\sum_{x \neq s} |\underline{x}\rangle$.



Explication par rotation : répétition des itérations

Théorème

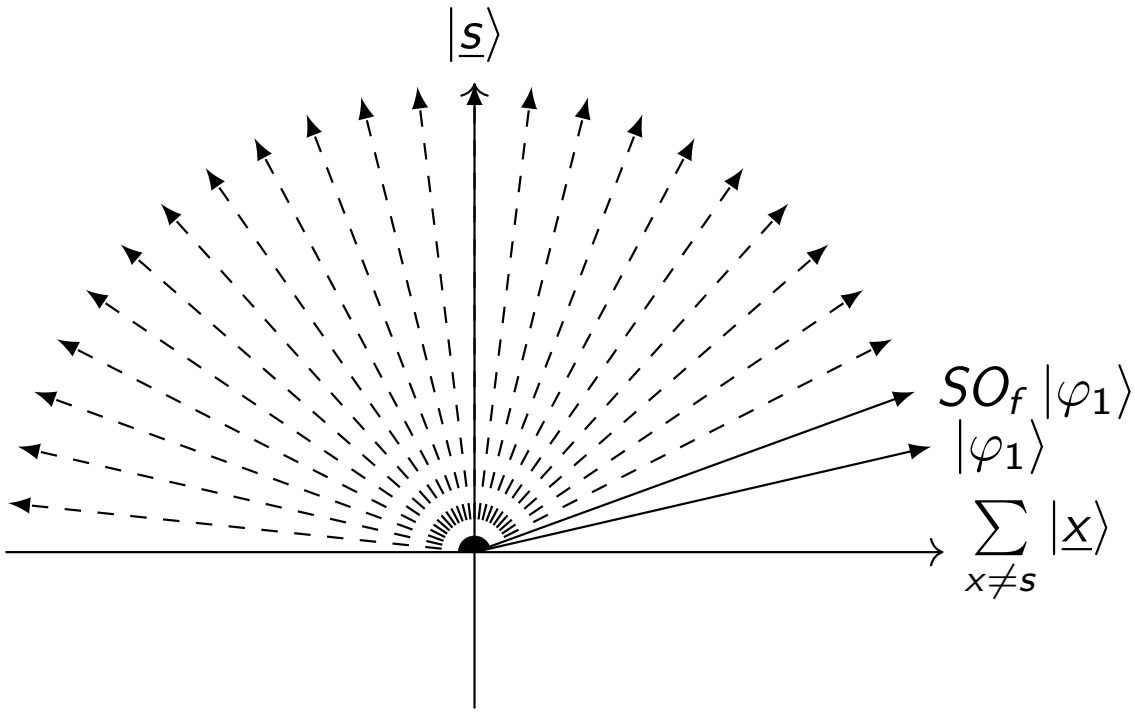
Plus on fait d'itérations, plus on se rapproche de $|\underline{s}\rangle$ et plus la probabilité que la mesure donne $|\underline{s}\rangle$ est proche de 1.



Explication par rotation : répétition des itérations

Théorème

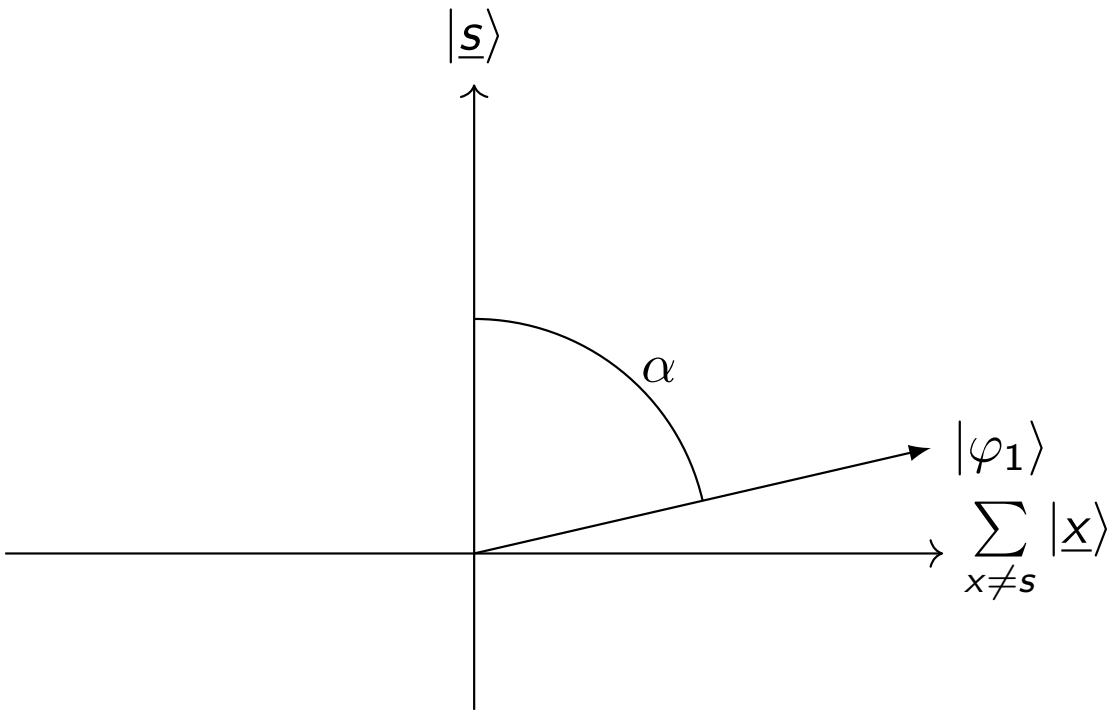
Mais si on fait trop d'itérations, cette probabilité diminue. Combien d'itérations faut-il faire ?



Explication par rotation : combien d'itérations

Théorème

Réponse : $\lfloor \frac{\alpha}{\theta} \rfloor$ ou $\lceil \frac{\alpha}{\theta} \rceil$. Reste à trouver θ et α.



Trouver θ

$\frac{\theta}{2}$ est l'angle entre $|\varphi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\underline{x}\rangle$ et $|X\rangle = \sum_{x \neq s} |\underline{x}\rangle$.

$$|\varphi_1\rangle = \frac{1}{\sqrt{2^n}} |\underline{s}\rangle + \frac{1}{\sqrt{2^n}} |X\rangle$$

$$\cos\left(\frac{\theta}{2}\right) = \frac{\langle\varphi_1|X\rangle}{\||\varphi_1\rangle\| \cdot \||X\rangle\|} = \frac{\sqrt{2^n-1}}{\sqrt{2^n}}$$

$$\cos\left(\frac{\pi-\theta}{2}\right) = \frac{\langle\varphi_1|\underline{s}\rangle}{\||\varphi_1\rangle\| \cdot \||\underline{s}\rangle\|} = \frac{1}{\sqrt{2^n}}$$

$$\sin\left(\frac{\theta}{2}\right) \simeq \frac{\theta}{2} \Rightarrow \theta \simeq \frac{2}{\sqrt{2^n}}$$

Trouver α

α est l'angle entre $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |\underline{x}\rangle$ et $|\underline{s}\rangle$.

$$\alpha = \frac{\pi - \theta}{2}$$
$$\simeq \frac{\pi}{2} - \frac{1}{\sqrt{2^n}}$$

Explication par rotation : combien d'itérations

$$\lfloor \frac{\alpha}{\theta} \rfloor \simeq \frac{\frac{\pi}{2} - \frac{1}{\sqrt{2^n}}}{\frac{2}{\sqrt{2^n}}}$$
$$\simeq \frac{\pi}{4}\sqrt{2^n} - \frac{1}{2}$$

Il faut donc environ $\frac{\pi}{4}\sqrt{2^n}$ itérations pour maximiser les chances de mesurer s.

Probabilité de mesurer s

Théorème

A l'issue de l'algorithme, la probabilité de mesurer s est supérieure à $1 - \frac{4}{2^n}$.

Indices :

- Que vérifie l'angle β entre $(SO_f)^p |\varphi_1\rangle$ et $|\underline{s}\rangle$ à l'issue de l'algorithme ?
- Quelle est la probabilité de mesurer $|\underline{s}\rangle$ en fonction de β.

Extensions

Quelques extensions / questions supplémentaires

- Si $f(x) = 1$ pour k valeurs ?
  Cibler $|s\rangle = \frac{1}{\sqrt{k}} \sum_{x|f(x)=1} |x\rangle$ avec $\sqrt{\frac{2^n}{k}}$ rotations.
- Que faire si on ne sait pas combien de valeurs sont solutions ou s'il n'y a pas de solution ?

Conclusion

Intérêt de l'informatique quantique

- Une accélération évidente par rapport au classique (et au probabiliste).
- Des accélérerations (très souvent quadratiques) à base de boîtes noires pour des algorithmes plus compliqués
  - optimisation, branch and bound
  - méthodes de Monte Carlo
  - collisions dans les fonctions de hashage
  - comptage

Pour aller plus loin $\Rightarrow$ cours de complexité

- Quel intérêt pour Bernstein Vazirani par rapport au classique ?
- Bornes inférieures, peut-on faire mieux que les accélérations proposées ici ?