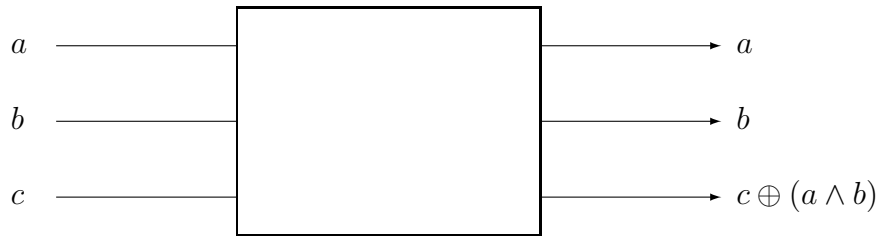
6.1 Calcul réversible

6.1.1 Circuit réversible

On rappelle qu'une porte logique est une fonction de $\{0,1\}^n \to \{0,1\}^m$. Elle a n entrées et m sorties.

Définition 6.1. *Une porte est **réversible** si elle est une bijection.*

Par exemple, la porte NOT est une porte réversible, alors que la porte ET ne l'est pas. Mais on peut rendre cette dernière réversible en ajoutant une troisième entrée :



Pour obtenir $a \wedge b$ il faut mettre $c = 0$ et lire la sortie 3. De plus cette porte est bien réversible puisqu'elle est son propre inverse. Cette porte est appelée porte *Toffoli* ou porte *c-c-NOT*.

Cette métode peut être étendue à n'importe quelle porte logique : si l'on a une porte représentée par la fonction $f : \{0,1\}^n \to \{0,1\}^m$, on peut lui associer une porte logique réversible $f_\oplus : \{0,1\}^{m+n} \to \{0,1\}^{m+n}$ telle que $f_\oplus(x,y) = (x, y \oplus f(x))$

Définition 6.2. *Un circuit logique est dit **réversible** s'il n'utilise que des portes réversibles.*

Théorème 6.3. *Toute fonction F calculable par un circuit logique de taille L est aussi calculable par un circuit réversible de taille $O(L)$*

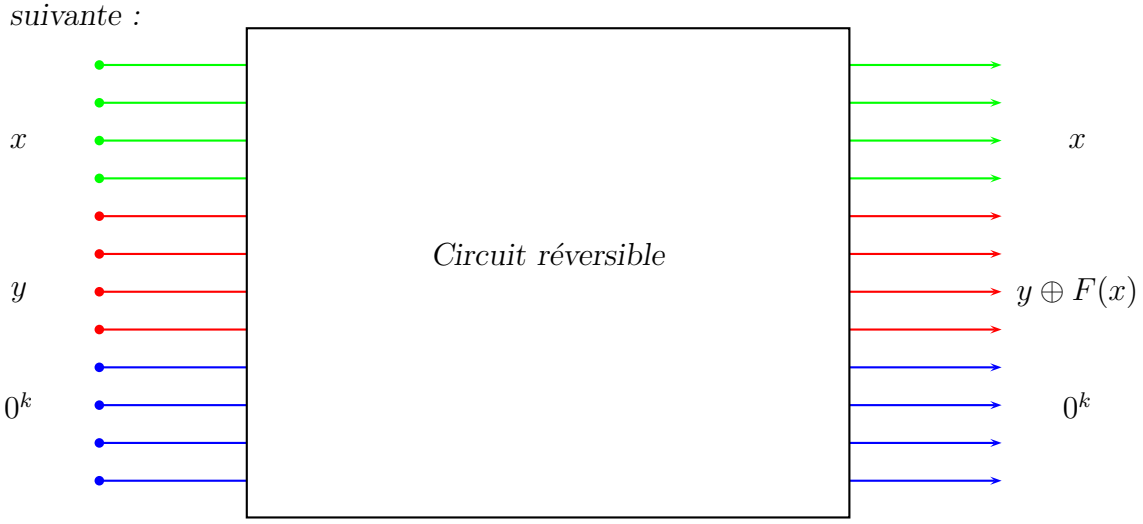
Preuve: Il suffit de remplacer les portes f par les portes réversibles $f_\oplus$ et des portes *C-NOT* □

La porte *Toffoli*(*c-c-NOT*) est universelle pour le calcul réversible, si l'on autorise 1 comme entrée. Sinon on a besoin de combiner avec la porte NOT pour générer des 1.

6.1.2 Forme normale d'un calcul réversible

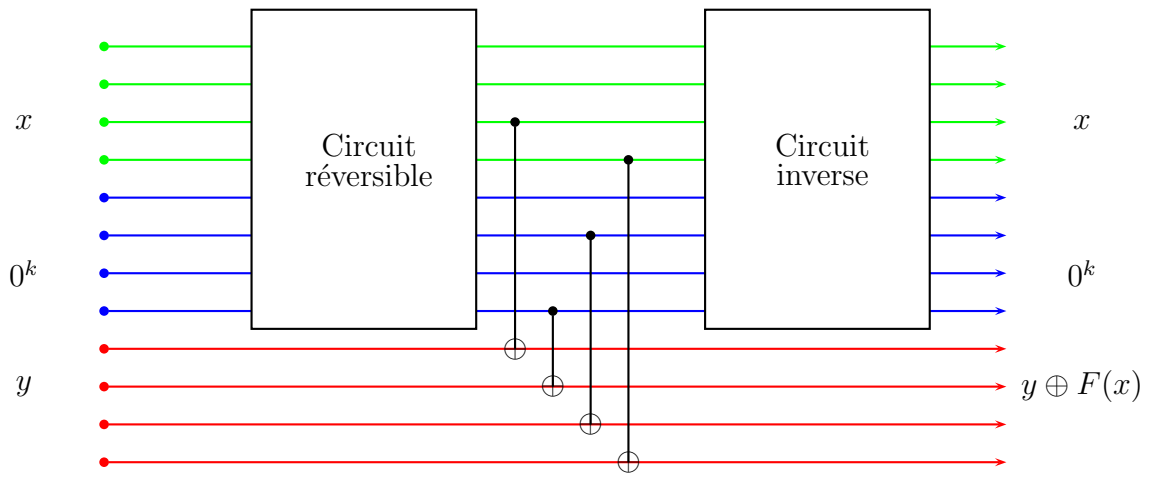
Dans le théorème 6.3, on voit que pour chaque porte logique, on doit ajouter des entrées et des sorties pour rendre le calcul réversible. Ainsi, si l'on combine plusieurs portes logiques, le nombre d'entrées et de sorties va augmenter linéairement avec le nombre de portes. On aimerait alors pouvoir effacer l'espace de travail, c'est à dire que les bits auxiliaires reviennent à 0 en fin de calcul, afin de pouvoir les réutiliser comme entrée auxiliaires pour d'autres portes.

Définition 6.4. *On appelle* ***forme normale*** *d'un calcul réversible un circuit sous la forme suivante :*



Théorème 6.5. *Si $F : \{0,1\}^n \to \{0,1\}^m$ est calculable avec un circuit réversible qui a $n+w$ entrées et sorties, alors il est calculable par un circuit réversible sous forme normale avec $n + m + w$ entrées et sorties.*

Preuve: Il suffit de rajouter m qbits (y) et de faire un *C-not* sur ces qbits contrôlés par les qbits en sortie du circuit réversible codant $F(x)$. Puis d'appliquer le circuit inverse aux autres qbits :



□

6.1.3 Calcul quatique et calcul réversible

Un circuit réversible est un circuit quantique car il est une transformation unitaire.

Corollaire 6.6. *Si F a une complexité classique L alors sa complexité quantique est au plus $O(L)$, et F et $c - F$ ont des complexités classiques (resp. quantiques) équivalentes.*

Théorème 6.7.
- *La porte* Toffoli *(avec la porte* NOT *pour générer des 1) est universelle pour le calcul réversible.*
- *La porte* Toffoli *et la porte de Hadamard (*H*) sont universelles pour le calcul quantique avec amplitude réelle.*
- *La porte* c-Not *et la porte $\sqrt{H}$ sont universelles pour le calcul quantique.*

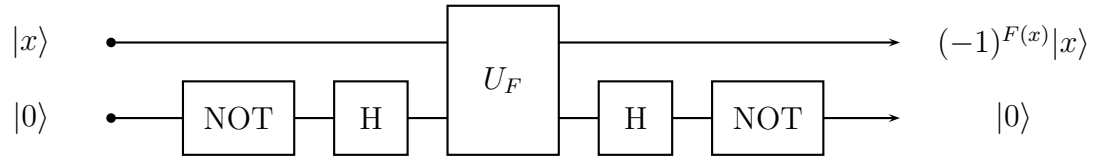
6.1.4 Exemple

Soit F une fonction à valeurs booléennes. On a souvent besoin d'un circuit S_F tel que $S_F|x\rangle = (-1)^{F(x)}|x\rangle$. Il est possible de réaliser un tel circuit en utilisant une fois $U_F|x, y\rangle = |F_\oplus(x, y)\rangle = |x, y \oplus F(x)\rangle$.

En effet,

$$\begin{aligned} U_F|x\rangle(|0\rangle - |1\rangle) &= |x\rangle(|F(x)\rangle - |\overline{F(x)}\rangle) \\ &= |x\rangle(-1)^{F(x)}(|0\rangle - |1\rangle) \end{aligned}$$

Ainsi le circuit suivant résoud le problème :



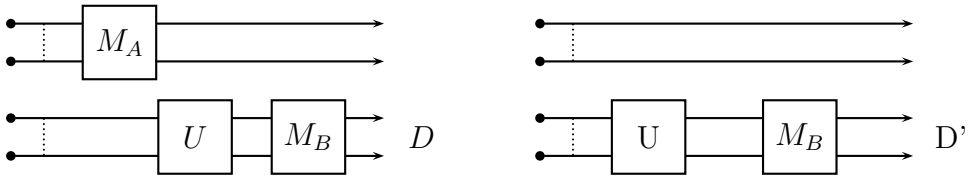
6.2 Mesures intermédiaires

Dans le cas d'un circuit quantique, l'information calculée sur les qbits est ensuite mesurée pour donner une information classique. Ceci se fait donc par une mesure sur certains qbits en sortie du circuit. Mais que se passe-t-il lorsque l'on fait des mesures intermédiaires au milieu du circuit ?

Théorème 6.8. *Une fonction calculable par un circuit avec des mesures intermédiaires l'est aussi par un circuit comparable avec uniquement une mesure à la fin.*

Preuve: Nous allons montrer ce théorème dans deux cas particuliers :

1. Mesure implicite
   Montrons que les deux circuits suivants sont équivalents :



On note A l'ensemble des premiers qbits, (ceux sur lesquels on fait une mesure implicite) et B l'ensemble des qbits sur lesquels on fait la mesure finale. Soit $(|x\rangle_A)_x$ et $(|y\rangle_B)_y$ des bases de A et B. Alors un état quelconque $|\psi\rangle_{AB}$ s'écrit :

$$\begin{aligned}|\psi\rangle_{AB} &= \sum_{x,y} \alpha_{xy}|x\rangle_A \otimes |y\rangle_B \\ &= \sum_x |x\rangle_A \otimes \underbrace{|\psi_x\rangle_B}_{\sum_y \alpha_{xy}|y\rangle_B}\end{aligned}$$

La mesure sur A est une trace partielle sur A. Or $Tr_A|\psi\rangle\langle\psi| = \sum_x |\psi_x\rangle\langle\psi_x|$

– Dans le premier circuit, la matrice densité sera :

Après mesure sur A : $\rho_1 = \sum_x |x\rangle\langle x| \otimes |\psi_x\rangle\langle\psi_x|$

Après U : $\rho_2 = \sum_x |x\rangle\langle x| \otimes |\psi'_x\rangle\langle\psi'_x|$ (avec $|\psi'_x\rangle = U|\psi_x\rangle$)

Après mesure sur B : $\rho_3 = \sum_{x,y} |x\rangle\langle x| \otimes \langle y|\psi'_x\rangle\langle\psi'_x|y\rangle\langle y|y\rangle$

La probabilité d'obtenir y est donc $\sum_x \|\langle y|\psi'_x\rangle\|^2$

– Dans le second circuit, on aura :

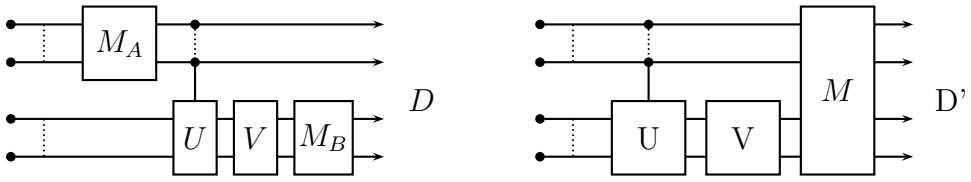
Après U **:** $\sum_x |x\rangle \otimes |\psi'_x\rangle$

Après mesure sur B **:** La probabilité d'obtenir y est $\|\langle y| \sum_x |x\rangle_A |\psi'_x\rangle_B\|^2 = \sum_x \|\langle y|\psi'_x\rangle\|^2$

Dans ce cas, la quantité mesurée en sortie des deux circuits a donc la même distribution de probabilité.

2. Mesure de contrôle

Montrons que les deux circuits suivants sont équivalents :



On note toujours $|\psi\rangle_{AB} = \sum_x |x\rangle_A \otimes |\psi_x\rangle_B$

– Dans le premier circuit, la matrice densité sera :

Après mesure sur A **:** $\rho_1 = \sum_x |x\rangle\langle x| \otimes |\psi_x\rangle\langle\psi_x|$

Après $c-U$ **:** On a $c-U = \sum |x\rangle\langle x| \otimes U_x$

$$\begin{aligned}
\rho_2 &= (c-U)\rho_1(c-U)^* \\
&= (\sum_{x'} |x'\rangle\langle x'| \otimes U_{x'})(\sum_x |x\rangle\langle x| \otimes |\psi_x\rangle\langle\psi_x|)(\sum_{x''} |x''\rangle\langle x''| \otimes U^*_{x''}) \\
&= \sum_{x,x',x''} |x'\rangle \underbrace{\langle x'|x\rangle\langle x|x''\rangle}_{\delta_{xx'x''}} \langle x''| \otimes U_{x'}|\psi_x\rangle\langle\psi_x|U^*_{x''} \\
&= \sum_x |x\rangle\langle x| \otimes U_x|\psi_x\rangle\langle\psi_x|U^*_x
\end{aligned}$$

Après V **:** $\rho_3 = \sum_x |x\rangle\langle x| \otimes VU_x|\psi_x\rangle\langle\psi_x|U^*_x V^*$

Après mesure sur B **:** $\rho_4 = \sum_{x,y} |x\rangle\langle x| \otimes \langle y|VU_x|\psi_x\rangle\langle\psi_x|U^*_x V^*|y\rangle|y\rangle\langle y|$

– Dans le second circuit,
On a $\rho_0 = \sum_{x,x'} |x\rangle\langle x'| \otimes |\psi_x\rangle\langle\psi_{x'}|$.

Après $c-U$ **:**

$$\begin{aligned}
\rho_1 &= (c-U)\rho_0(c-U)^* \\
&= (\sum_{x''} |x''\rangle\langle x''| \otimes U_{x''})(\sum_{x,x'} |x\rangle\langle x'| \otimes |\psi_x\rangle\langle\psi'_x|)(\sum_{x'''} |x'''\rangle\langle x'''| \otimes U^*_{x'''}) \\
&= \sum_{x,x',x'',x'''} |x''\rangle \underbrace{\langle x''|x\rangle\langle x'|x'''\rangle}_{\delta_{x''x}\delta_{x'x'''}} \langle x'''| \otimes U_{x''}|\psi_x\rangle\langle\psi_{x'}|U^*_{x'''} \\
&= \sum_{x,x'} |x\rangle\langle x'| \otimes U_x|\psi_x\rangle\langle\psi_{x'}|U^*_{x'}
\end{aligned}$$

Après V : $\rho_2 = \sum_{x,x'} |x\rangle\langle x'| \otimes VU_x|\psi_x\rangle\langle\psi_{x'}|U_{x'}^*V^*$

Après mesure totale :

$$\rho_3 = \sum_{x,x',x'',y} \underbrace{\langle x''|x\rangle\langle x'|x''\rangle}_{\delta_{xx'x''}} |x''\rangle\langle x''| \otimes \langle y|VU_x|\psi_x\rangle\langle\psi_{x'}|U_{x'}^*V^*|y\rangle|y\rangle\langle y|$$
$$= \sum_{x,y} |x\rangle\langle x| \otimes \langle y|VU_x|\psi_x\rangle\langle\psi_x|U_x^*V^*|y\rangle|y\rangle\langle y|$$

Les matrices densités sont identique en sortie des deux circuits, ils sont donc équivalents.

□

6.3 Problème de recherche abstrait

6.3.1 Présentation

Soit un ensemble X, et M un sous ensemble de X, le problème de recherche abstrait est de trouver un élément $x \in M$ en utilisant la requête : *Est-ce que $x \in M$?*. On note $\epsilon = Pr(M)$. La complexité de ce problème en nombre de requêtes dépend du mode de résolution :

Recherche exhaustive : Dans ce cas la complexité est de $|X|$ requêtes.

Recherche aléatoire Dans ce cas, un élément de M est trouvé en $O(1/\epsilon)$ requêtes.

Recherche quantique Dans ce cas, un élément de M est trouvé en $O(1/\sqrt{\epsilon})$ requêtes.

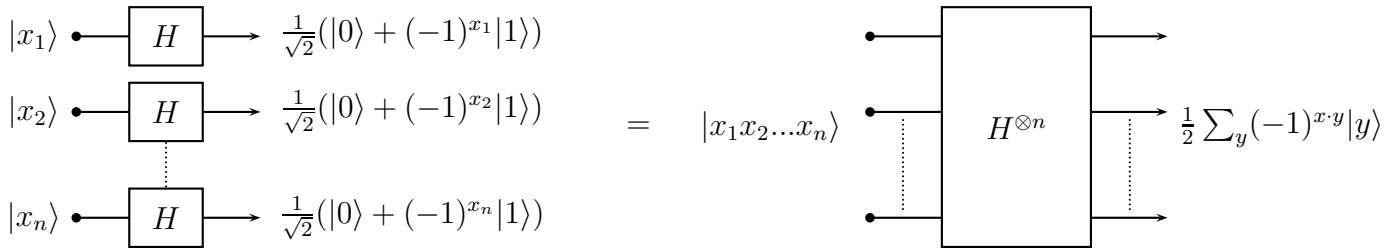
Dans la suite, on modélise le problème par :
- $f : \{0,1\}^n \to \{0,1\}$
- $X = \{0,1\}^n$, on note $N = |X| = 2^n$
- $M = \{x_0 \in X \backslash f(x_0) = 1\}$

6.3.2 Solution quantique quand $N = 4$

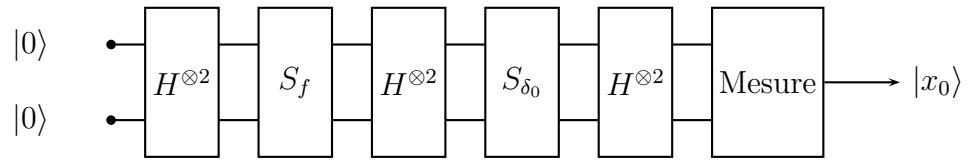
On suppose qu'il y a un unique élément x_0 tel que $f(x_0) = 1$.
On implémentera f par le circuit S_f vu en 6.1.4 :

$$\sum_x \alpha_x|x\rangle \longrightarrow \boxed{S_f} \longrightarrow \sum_x (-1)^{f(x)}\alpha_x|x\rangle = \sum_x \alpha_x|x\rangle - 2\alpha_{x_0}|x_0\rangle$$

On utilisera une porte de Hadamard sur chacun des qbits, appelée transformée de Fourrier quantique :



avec $x \cdot y = \sum_{i=1}^{n} x_i y_i \bmod 2$
Le circuit suivant résoud le problème en un appel à f lorsque $N = 4$:



Preuve: On met en entrée du circuit $\psi_0 = |00\rangle$.
après $H^{\otimes 2}$ (parallélisation)

$$\psi_1 = \frac{1}{2} \sum_{x \in \{0,1\}^2} |x\rangle$$

après S_f (appel de f)

$$\psi_2 = \frac{1}{2} \sum_{x \in \{0,1\}^2} |x\rangle - |x_0\rangle = H^{\otimes 2}|00\rangle - |x_0\rangle$$

après $H^{\otimes 2}$ (interférences)

$$\psi_3 = |00\rangle - \frac{1}{2} \sum_{y \in \{0,1\}^2} (-1)^{x_0 \cdot y} |y\rangle$$

après S_{δ_0} ($\delta_0(x) = 1 \Leftrightarrow x = (0,0)$)

$$\psi_3 = -|00\rangle - \frac{1}{2} \sum_{y \in \{0,1\}^2} (-1)^{x_0 \cdot y} |y\rangle - 2|00\rangle = -H^{\otimes 2}|x_0\rangle$$

après $H^{\otimes 2}$ (regroupement)

$$\psi_4 = -|x_0\rangle$$

□

Opérateur de diffusion : Analyse numérique

Notons $D = H^{\otimes 2} S_{\delta_0} H^{\otimes 2}$.$D$ est appelé opérateur de diffusion. Or $S_{\delta_0} = Id - 2|00\rangle\langle 00|$. Donc $D = Id - 2H^{\otimes 2}|00\rangle\langle 00|H^{\otimes 2}$.

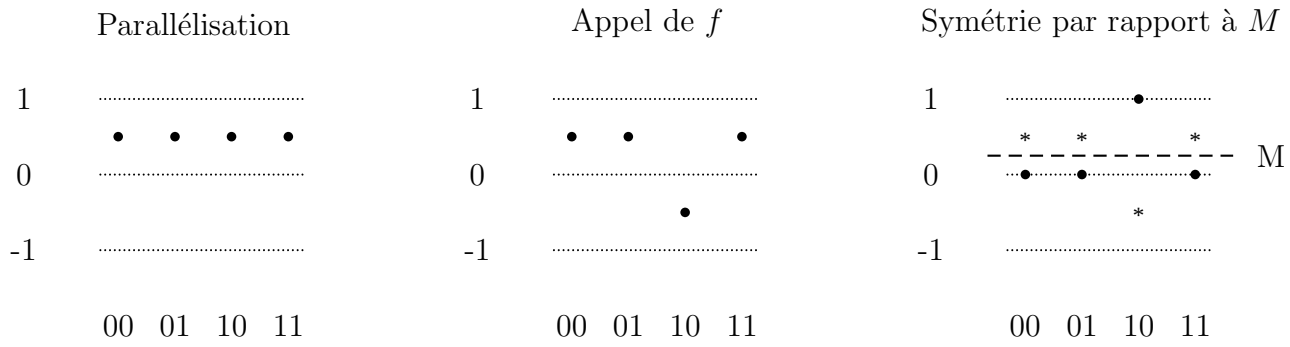
$$H^{\otimes 2} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$\text{d'où } D = \begin{pmatrix} 1/2 & -1/2 & -1/2 & -1/2 \\ -1/2 & 1/2 & -1/2 & -1/2 \\ -1/2 & -1/2 & 1/2 & -1/2 \\ -1/2 & -1/2 & -1/2 & 1/2 \end{pmatrix} = \boxed{Id - \frac{1}{2}\mathbf{1}}$$

Soit $|\psi\rangle = \sum_x \alpha_x |x\rangle$, alors

$$\begin{aligned}(-D)|\psi\rangle &= -\sum_x \alpha_x|x\rangle + \sum_x \frac{1}{2}\alpha_x \sum_y |y\rangle \\ &= -\sum_x \alpha_x|x\rangle + \frac{1}{2}\sum_x(\sum_y \alpha_y)|x\rangle \\ &= \sum_x (\underbrace{\frac{1}{2}\sum_y \alpha_y}_{2M} - \alpha_x)|x\rangle\end{aligned}$$

Donc $(-D)$ appliqué à un état $|\psi\rangle$ effectue sur chaque coordonnée une symétrie par raport à la moyenne des amplitudes M. Voici ci-dessous le graphe des amplitudes de l'état du circuit lorsque $x_0 = (1, 0)$:



Opérateur de Grover : Analyse géométrique

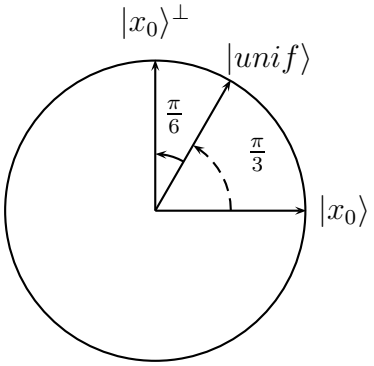
Définition 6.9. *On appele opérateur de* Grover *l'opérateur* $G = H^{\otimes 2}(-S_{\delta_0})H^{\otimes 2}S_f$

Théorème 6.10. *G est une rotation d'angle* $-\frac{\pi}{3}$

Preuve:
- $S_f^2 = Id$ donc S_f est une symétrie. De plus $\forall |y\rangle \in |x_0\rangle^\perp, S_f|y\rangle = |y\rangle$. Donc S_f est une symétrie par rapport à $|x_0\rangle^\perp$.
- De la même manière, $-S_{\delta_0}$ est une symétrie par rapport à $|00\rangle$.
- $H^{\otimes 2}(-S_{\delta_0})H^{\otimes 2}$ est un changement de base de $-S_{\delta_0}$, c'est donc la symétrie par rapport à la superposition uniforme $|unif\rangle = \frac{1}{2}\sum_x |x\rangle$.
- Soit $|\phi\rangle = \alpha|x_0\rangle + \beta|unif\rangle$.

$$\begin{aligned}\text{Alors } G|\phi\rangle &= H^{\otimes 2}(-S_{\delta_0})H^{\otimes 2}S_f|\phi\rangle \\ &= (H^{\otimes 2}(-S_{\delta_0})H^{\otimes 2})(-\alpha|x_0\rangle + |unif\rangle - 2\beta\ \langle x_0|unif\rangle|x_0\rangle) \\ &= (H^{\otimes 2}(-S_{\delta_0})H^{\otimes 2})(\alpha'|x_0\rangle + \beta|unif\rangle) \\ &= \alpha'(-|x_0\rangle + 2\langle x_0|unif\rangle|unif\rangle) + \beta|unif\rangle \\ &\in Vect(|x_0\rangle, |unif\rangle)\end{aligned}$$

Ainsi le plan $Vect(|x_0\rangle, |unif\rangle)$ est stable par G. De plus $\langle x_0|unif\rangle = \frac{1}{2}$. On a donc la situation suivante



– Ainsi, dans ce plan G est la composition de deux symétries séparées d'un angle $-\pi/6$. C'est donc une rotation d'angle $-\pi/3$. On a donc $G|unif\rangle = |x_0\rangle$.

□