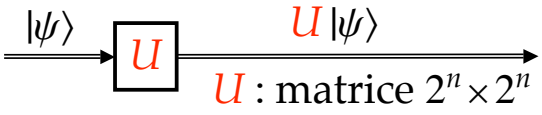
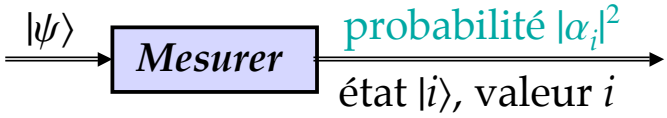
Registre de n qubits : état et évolution

L'état d'un registre de n qubits est un vecteur dans un espace à 2^n dimensions :

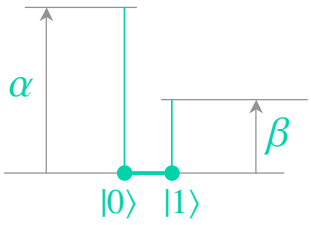
- l'un des 2^n états de base : $|00..00\rangle$ (c.à.d. $|0\rangle$), $|00..01\rangle$ (c.à.d. $|1\rangle$), $|00..10\rangle$ (c.à.d. $|2\rangle$), ..., $|11..11\rangle$ (c.à.d. $|2^n-1\rangle$)
- ou, plus généralement, une superposition d'états de base :
  $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \ .. \ + \alpha_{2^n-1}|2^n-1\rangle$,
  avec $|\alpha_0|^2 + |\alpha_1|^2 + \ .. \ + |\alpha_{2^n-1}|^2 = 1$



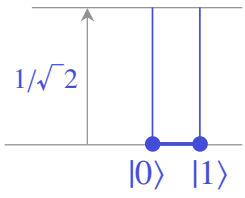


Représentation graphique d'amplitudes réelles

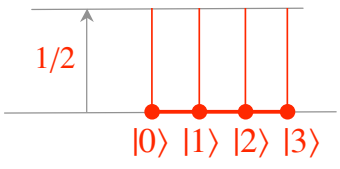
$\alpha\,|0\rangle + \beta\,|1\rangle$



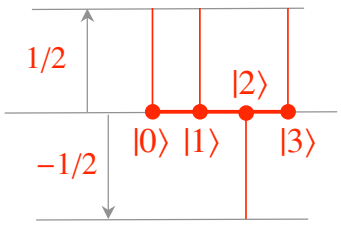
$1/\sqrt{2}\,(|0\rangle+|1\rangle)$



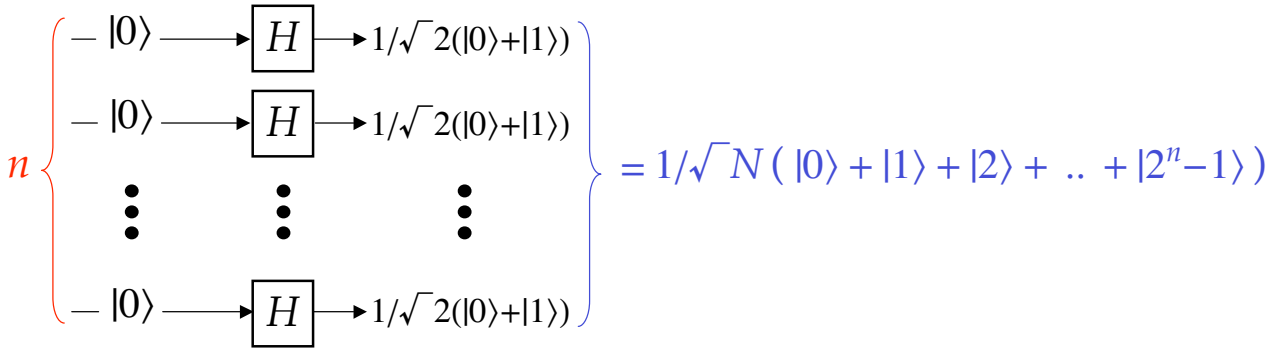
$1/2\,(\,|0\rangle + |1\rangle + |2\rangle + |3\rangle\,)$

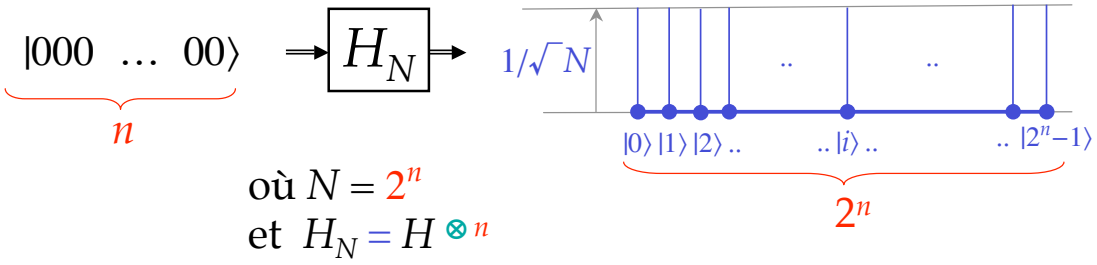


$1/2\,(\,|0\rangle + |1\rangle - |2\rangle + |3\rangle\,)$



2^n valeurs superposées dans un registre de n qubits

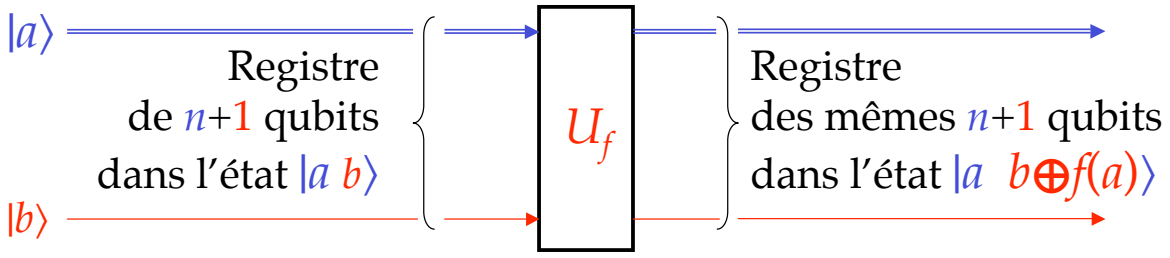


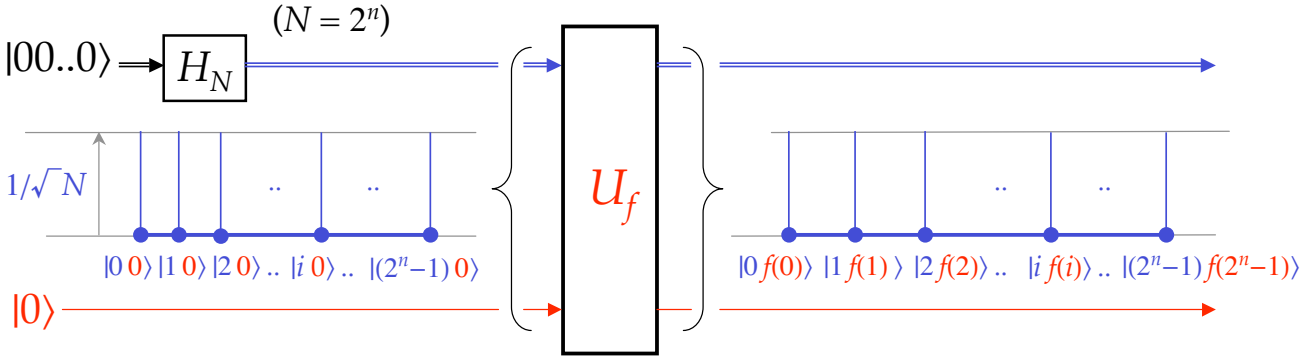


où $N = 2^n$
et $H_N = H^{\otimes n}$

Calculer une fonction : parallélisme quantique

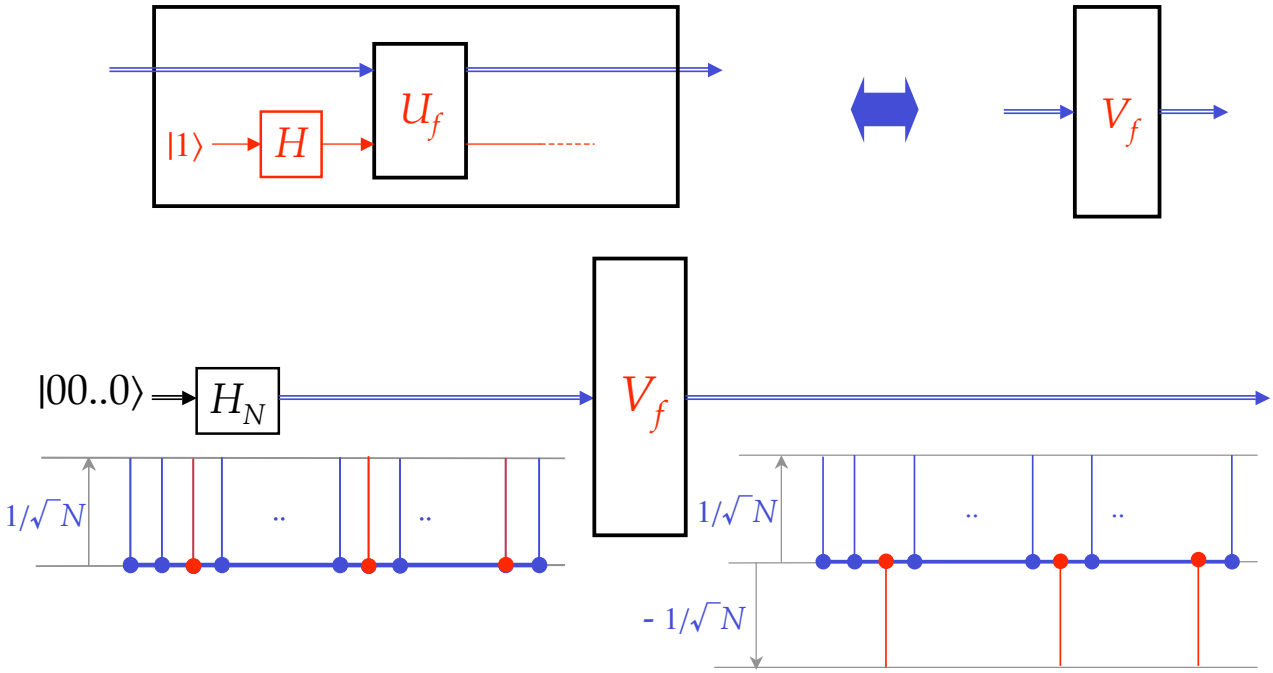
$a \in [0,2^n-1]$ $f(a) \in \{0,1\}$ $b \in \{0,1\}$





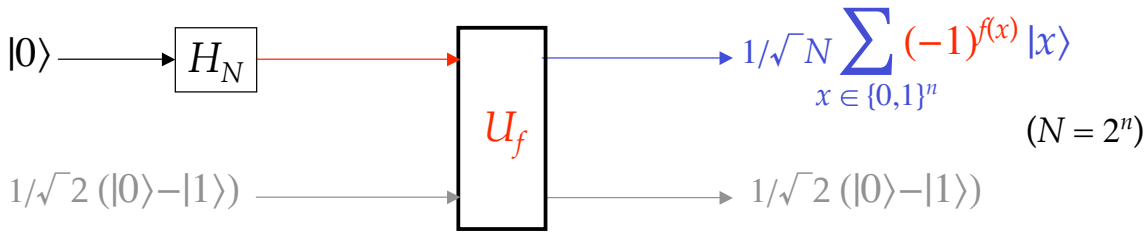
Inverser les amplitudes des a tels que $f(a) = 1$

$a \in [0,2^n-1]$ $f(a) \in \{0,1\}$



Implémentation de l'inversion des amplitudes

$f: \{0,1\}^n \rightarrow \{0,1\}$

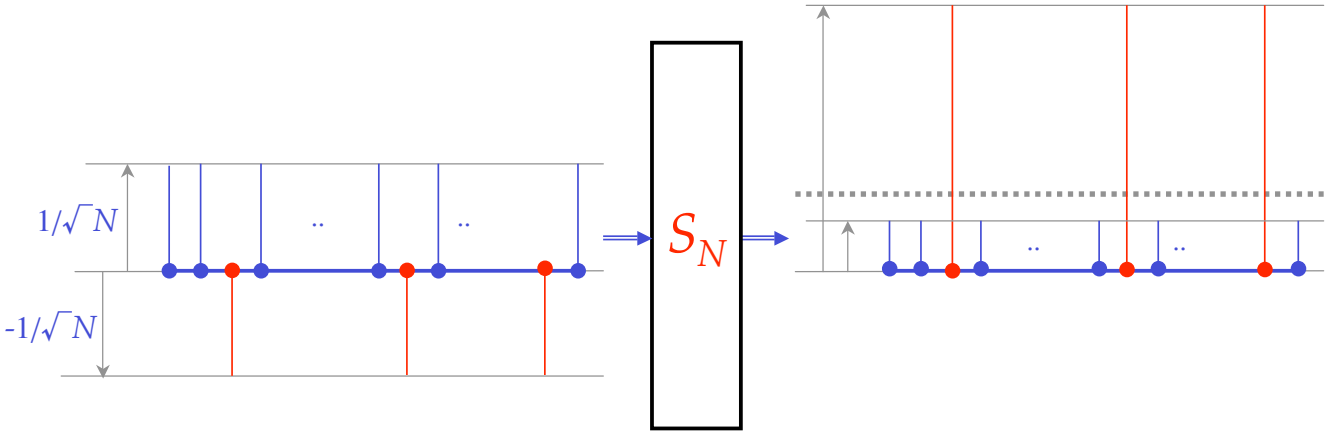


$$1/\sqrt{N}\,1/\sqrt{2}\Big(\sum_{x \in X_0} |x\rangle(|0 \oplus 0\rangle - |1 \oplus 0\rangle) + \sum_{x \in X_1} |x\rangle(|0 \oplus 1\rangle - |1 \oplus 1\rangle)\Big)$$

$$= 1/\sqrt{N}\,1/\sqrt{2}\Big(\sum_{x \in X_0} |x\rangle(|0\rangle - |1\rangle) - \sum_{x \in X_1} |x\rangle(|0\rangle - |1\rangle)\Big)$$

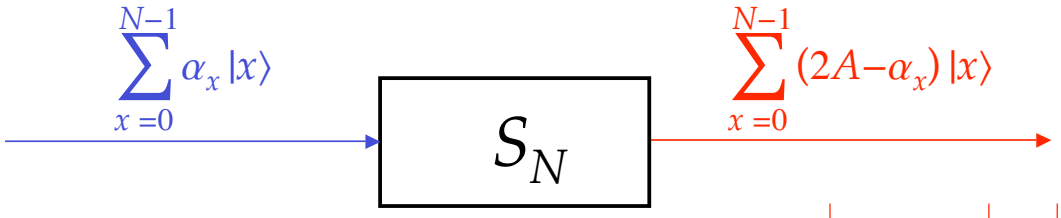
$$= 1/\sqrt{N}\,1/\sqrt{2}\sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle\,(|0\rangle - |1\rangle) \quad = 1/\sqrt{N} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \otimes 1/\sqrt{2}(|0\rangle - |1\rangle)$$

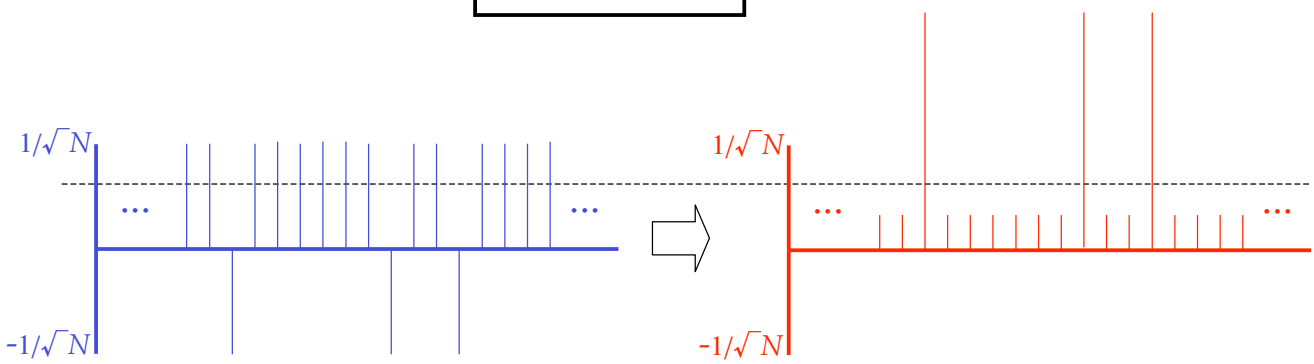
Symétrie par rapport à la moyenne



Définition de la symétrie / à la moyenne

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle \qquad \alpha_x \Rightarrow A - (\alpha_x - A) \qquad A = 1/N \sum_{x=0}^{N-1} \alpha_x$$





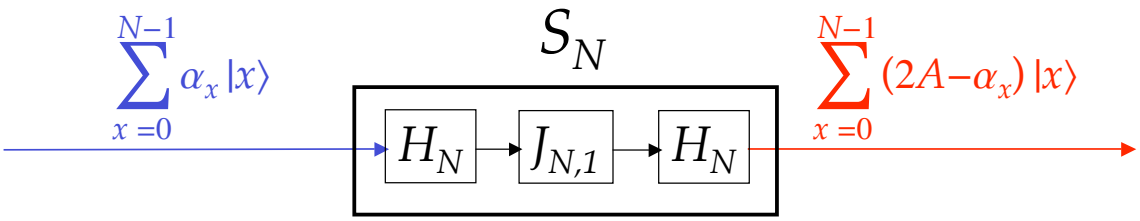
Implémenter la symétrie / à la moyenne

$$H = 1/\sqrt{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H_N = H^{\otimes n}$$

$$J_{N,1} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & -1 & \dots & 0 & 0 \\ \dots & & & & \dots \\ 0 & 0 & \dots & -1 & 0 \\ 0 & 0 & \dots & 0 & -1 \end{pmatrix}$$

$$S_N = H_N \cdot J_{N,1} \cdot H_N = \begin{pmatrix} 2/N-1 & 2/N & \dots & 2/N \\ 2/N & 2/N-1 & \dots & 2/N \\ \dots & & \dots & \dots \\ 2/N & \dots & 2/N-1 & 2/N \\ 2/N & \dots & 2/N & 2/N-1 \end{pmatrix}$$



Recherche dans un annuaire téléphonique quantique

- 1,000,000 de noms listés dans un annuaire, en ordre alphabétique :
  NOM nnn nn nn
- Etant donné un numéro xxx xx xx, trouver le NOM unique tel que :
  nnn nn nn = xxx xx xx
- Informatique classique (c.à.d. physique classique) :
  jusqu'à 1,000,000 d'appels à « nnn nn nn = xxx xx xx ? »
- Informatique quantique (c.à.d. physique quantique) :
  seulement 1,000 appels à « nnn nn nn = xxx xx xx ? »

Trouver l'élément qui, parmi $N=2^n$, satisfait f

$a \in [0,2^n-1]$ $f(a) \in \{0,1\}$

$f(a)=1$ pour un et un seul $a_0 \in [0,2^n-1]$

Aucune autre information disponible sur f

Problème : trouver ce a_0

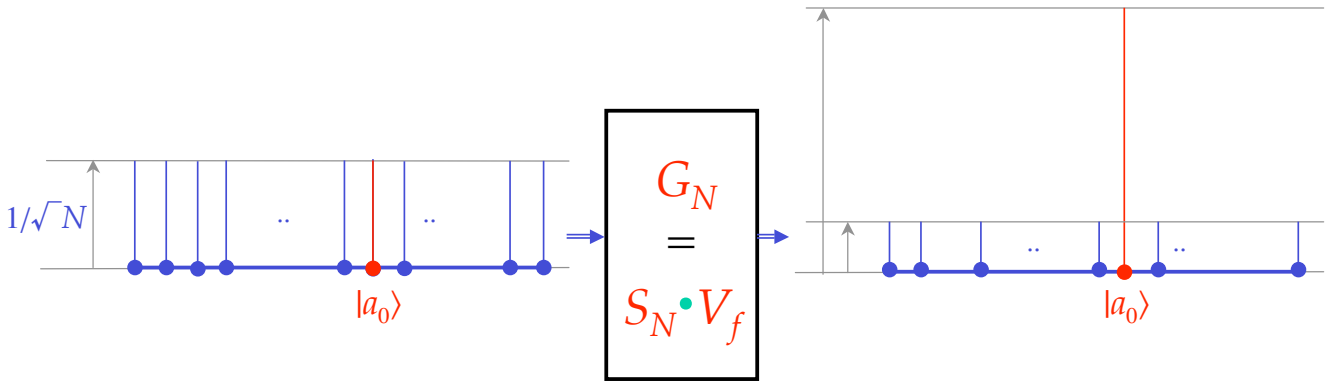
Calcul classique :
- au pire, N appels à f
- en moyenne, $N/2$ appels à f

Calcul quantique :
- exactement $\sqrt{N}$ appels à f,
- hors d'accès du calcul classique

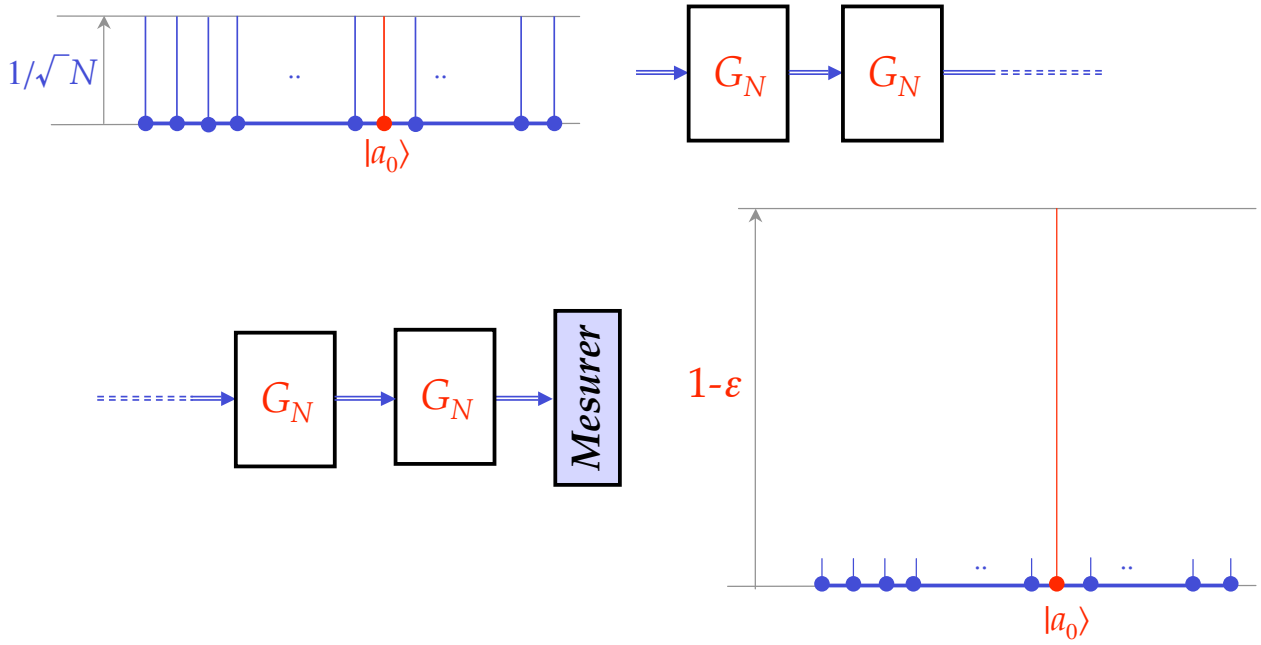
Amplification de l'amplitude de $|a_0\rangle$

$a \in [0,2^n-1]$ $f(a) \in \{0,1\}$

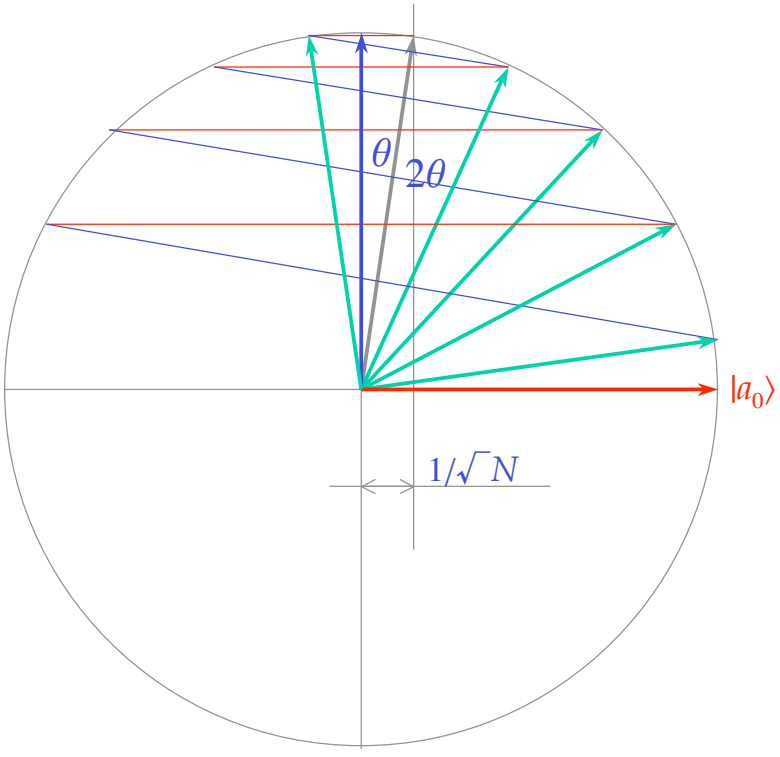
$f(a)=1$ pour un seul $a=a_0 \in [0,2^n-1]$



Recherche de a_0 : algorithme de Grover



Stop à $\sqrt{N}$ fois G_N ! Preuve géométrique



- But : arriver aussi près que possible de $|a_0\rangle$. Pour cela, il faut répéter k fois G_N, où :

$$\pi/2 - \theta \leqslant \theta + k\,2\theta \leqslant \pi/2 + \theta$$

- N est grand, donc θ est petit :

$$\theta \approx \sin\theta = 1/\sqrt{N}$$

- Donc : $k \approx \pi/4\,\sqrt{N}$

- Accélération quadratique