Informatique Quantique

Simon Perdrix

Pépites Algorithmiques
simon.perdrix@loria.fr

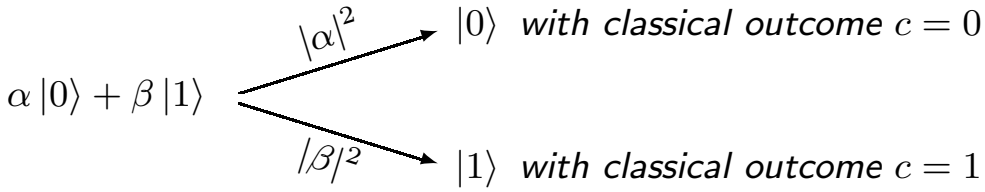
28 février 2017

Postulates of QM :

P1 : n-qubit state : $\mathbf{\Phi} = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$, $\sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$

P2 : Composed systems : $\mathbf{\Phi_1} \otimes \mathbf{\Phi_2}$. If $\mathbf{\Phi}$ cannot be decomposed into $\mathbf{\Phi_1} \otimes \mathbf{\Phi_2}$, then $\mathbf{\Phi}$ is **entangled**.

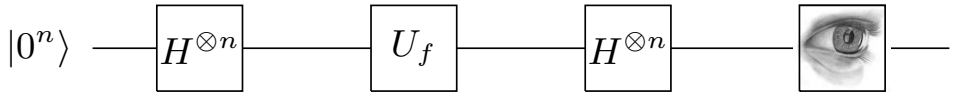
P3 : Measurement : Probabilistic and Irreversible.



P4 : Unitary Evolutions U.

Un 1er algorithme quantique : Bernstein-Vazirani

Donnée : $f : \{0,1\}^n \to \{0,1\}$ t.q. $\exists a \in \{0,1\}^n, f(x) = x \bullet a = \sum_{i=1}^{n} x_i a_i \bmod 2$.
Problème : Trouver $a \in \{0,1\}^n$.
Algorithme classique : n appels à f sont nécessaires et suffisants.
Algorithme quantique : 1 appel à U_f.



Algorithme de Deutsch-Jozsa

Promesse : $f : \{0,1\}^n \to \{0,1\}$ est constante ou équilibrée ($|f^{-1}(0)| = |f^{-1}(1)|$)
Problème : décider si f est constante ou équilibrée.
Algorithme classique :
Algorithme quantique :

Algorithme de Deutsch-Jozsa

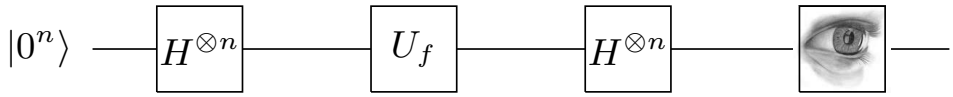
Promesse : $f : \{0,1\}^n \to \{0,1\}$ est constante ou équilibrée ($|f^{-1}(0)| = |f^{-1}(1)|$)
Problème : décider si f est constante ou équilibrée.
Algorithme classique : nécessite $N/2+1$ appels à f avec $N=2^n$
Algorithme quantique :

Algorithme de Deutsch-Jozsa

Promesse : $f : \{0,1\}^n \to \{0,1\}$ est constante ou équilibrée ($|f^{-1}(0)| = |f^{-1}(1)|$)
Problème : décider si f est constante ou équilibrée.
Algorithme classique : nécessite $N/2+1$ appels à f avec $N=2^n$
Algorithme quantique : 1 appel à U_f.

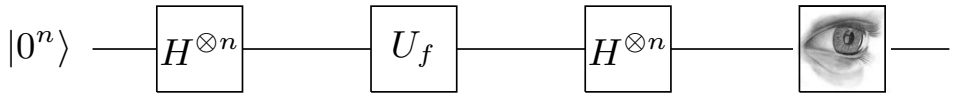
Algorithme de Deutsch-Jozsa

Promesse : $f : \{0,1\}^n \to \{0,1\}$ est constante ou équilibrée ($|f^{-1}(0)| = |f^{-1}(1)|$)
Problème : décider si f est constante ou équilibrée.
Algorithme classique : nécessite $N/2+1$ appels à f avec $N=2^n$
Algorithme quantique : 1 appel à U_f.



Algorithme de Deutsch-Jozsa

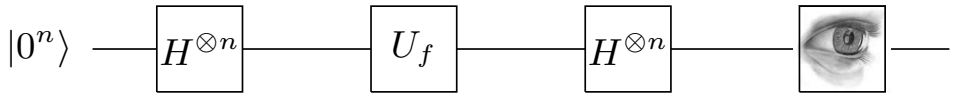
Promesse : $f : \{0,1\}^n \to \{0,1\}$ est constante ou équilibrée ($|f^{-1}(0)| = |f^{-1}(1)|$)
Problème : décider si f est constante ou équilibrée.
Algorithme classique : nécessite $N/2+1$ appels à f avec $N=2^n$
Algorithme quantique : 1 appel à U_f.



$$
\begin{aligned}
|0^n\rangle &\mapsto^{H_n} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \\
&\mapsto^{U_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle \\
&\mapsto^{H_n} \frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{f(x)} (-1)^{x\cdot y} |y\rangle
\end{aligned}
$$

Algorithme de Deutsch-Jozsa

Promesse : $f : \{0,1\}^n \to \{0,1\}$ est constante ou équilibrée ($|f^{-1}(0)| = |f^{-1}(1)|$)
Problème : décider si f est constante ou équilibrée.
Algorithme classique : nécessite $N/2+1$ appels à f avec $N=2^n$
Algorithme quantique : 1 appel à U_f.



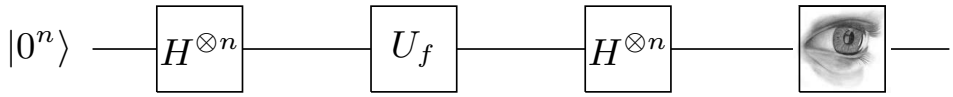
$$
\begin{array}{lll}
|0^n\rangle & \mapsto^{H_n} & \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \\
& \mapsto^{U_f} & \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle \\
& \mapsto^{H_n} & \frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{f(x)} (-1)^{x\cdot y} |y\rangle
\end{array}
$$

L'amplitude de $|0^n\rangle$ est $\alpha_0 = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}$

- Si f est équilibrée, $\alpha_0 = 0 \implies$ on ne mesure jamais 0^n.
- Si f est constante, $\alpha_0 = \pm 1 \implies$ on mesure toujours 0^n.

Algorithme de Deutsch-Jozsa

Promesse : $f : \{0,1\}^n \to \{0,1\}$ est constante ou équilibrée ($|f^{-1}(0)| = |f^{-1}(1)|$)
Problème : décider si f est constante ou équilibrée.
Algorithme classique : nécessite $N/2+1$ appels à f avec $N=2^n$
Algorithme quantique : 1 appel à U_f.
Algorithme erreur bornée :



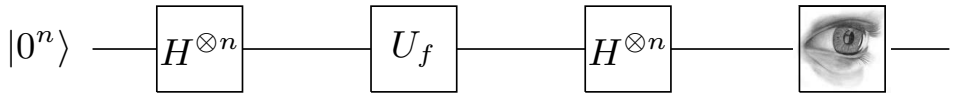
$$
\begin{array}{lll}
|0^n\rangle & \mapsto^{H_n} & \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \\
& \mapsto^{U_f} & \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle \\
& \mapsto^{H_n} & \frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{f(x)} (-1)^{x\cdot y} |y\rangle
\end{array}
$$

L'amplitude de $|0^n\rangle$ est $\alpha_0 = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}$

- Si f est équilibrée, $\alpha_0 = 0 \implies$ on ne mesure jamais 0^n.
- Si f est constante, $\alpha_0 = \pm 1 \implies$ on mesure toujours 0^n.

Algorithme de Deutsch-Jozsa

Promesse : $f : \{0,1\}^n \to \{0,1\}$ est constante ou équilibrée ($|f^{-1}(0)| = |f^{-1}(1)|$)
Problème : décider si f est constante ou équilibrée.
Algorithme classique : nécessite $N/2+1$ appels à f avec $N=2^n$
Algorithme quantique : 1 appel à U_f.
Algorithme erreur bornée : $O(1)$ appels à f.



$$
\begin{aligned}
|0^n\rangle &\mapsto^{H_n} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \\
&\mapsto^{U_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle \\
&\mapsto^{H_n} \frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{f(x)} (-1)^{x\cdot y} |y\rangle
\end{aligned}
$$

L'amplitude de $|0^n\rangle$ est $\alpha_0 = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}$

- Si f est équilibrée, $\alpha_0 = 0 \implies$ on ne mesure jamais 0^n.
- Si f est constante, $\alpha_0 = \pm 1 \implies$ on mesure toujours 0^n.

Algorithme de Grover

Promesse : $f : \{0,1\}^n \to \{0,1\}$ telle que $|f^{-1}(1)| = 1$.
Problème : Trouver x_0 tel que $f(x_0) = 1$.
Algorithme classique : $\Theta(N)$ appels à f avec $N = 2^n$. ($N/2$ en moyenne)
Algorithme quantique : $O(\sqrt{N})$ appels à U_f.

1. Préparer un registre de n qubits dans l'état $\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = H^{\otimes n} |0 \dots 0\rangle$
2. Répéter $\frac{\pi\sqrt{N}}{4}$ fois :
   - (a) Appliquer $U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$
   - (b) Appliquer $D : |x\rangle \mapsto -|x\rangle + \frac{2}{N} \sum_{y \in \{0,1\}^n} |y\rangle$
3. Mesurer le registre. Si le résultat z ne vérifie pas $f(z) = 1$, recommencer à l'étape 1.

Algorithme de Grover

Promesse : $f : \{0,1\}^n \to \{0,1\}$ telle que $|f^{-1}(1)| = 1$.
Problème : Trouver x_0 tel que $f(x_0) = 1$.
Algorithme classique : $\Theta(N)$ appels à f avec $N = 2^n$. ($N/2$ en moyenne)
Algorithme quantique : $O(\sqrt{N})$ appels à U_f.

1. Préparer un registre de n qubits dans l'état $\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = H^{\otimes n} |0 \dots 0\rangle$
2. Répéter $\frac{\pi\sqrt{N}}{4}$ fois :
   - (a) Appliquer $U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$
   - (b) Appliquer $D : |x\rangle \mapsto -|x\rangle + \frac{2}{N} \sum_{y \in \{0,1\}^n} |y\rangle$
3. Mesurer le registre. Si le résultat z ne vérifie pas $f(z) = 1$, recommencer à l'étape 1.

Algorithme de Grover

Promesse : $f : \{0,1\}^n \to \{0,1\}$ telle que $|f^{-1}(1)| = 1$.
Problème : Trouver x_0 tel que $f(x_0) = 1$.
Algorithme classique : $\Theta(N)$ appels à f avec $N = 2^n$. ($N/2$ en moyenne)
Algorithme quantique : $O(\sqrt{N})$ appels à U_f.

1. Préparer un registre de n qubits dans l'état $\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = H^{\otimes n} |0 \dots 0\rangle$
2. Répéter $\frac{\pi\sqrt{N}}{4}$ fois :
   - (a) Appliquer $U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$
   - (b) Appliquer $D : |x\rangle \mapsto -|x\rangle + \frac{2}{N} \sum_{y \in \{0,1\}^n} |y\rangle$
3. Mesurer le registre. Si le résultat z ne vérifie pas $f(z) = 1$, recommencer à l'étape 1.

Algorithme de Grover

Promesse : $f : \{0,1\}^n \to \{0,1\}$ telle que $|f^{-1}(1)| = 1$.
Problème : Trouver x_0 tel que $f(x_0) = 1$.
Algorithme classique : $\Theta(N)$ appels à f avec $N = 2^n$. ($N/2$ en moyenne)
Algorithme quantique : $O(\sqrt{N})$ appels à U_f.

1. Préparer un registre de n qubits dans l'état $\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = H^{\otimes n} |0 \dots 0\rangle$
2. Répéter $\frac{\pi\sqrt{N}}{4}$ fois :
   - (a) Appliquer $U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$
   - (b) Appliquer $D : |x\rangle \mapsto -|x\rangle + \frac{2}{N} \sum_{y \in \{0,1\}^n} |y\rangle$
3. Mesurer le registre. Si le résultat z ne vérifie pas $f(z) = 1$, recommencer à l'étape 1.

Algorithme de Grover

Promesse : $f : \{0,1\}^n \to \{0,1\}$ telle que $|f^{-1}(1)| = 1$.
Problème : Trouver x_0 tel que $f(x_0) = 1$.
Algorithme classique : $\Theta(N)$ appels à f avec $N = 2^n$. ($N/2$ en moyenne)
Algorithme quantique : $O(\sqrt{N})$ appels à U_f.

1. Préparer un registre de n qubits dans l'état $\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = H^{\otimes n} |0 \dots 0\rangle$
2. Répéter $\frac{\pi\sqrt{N}}{4}$ fois :
   - (a) Appliquer $U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$
   - (b) Appliquer $D : |x\rangle \mapsto -|x\rangle + \frac{2}{N} \sum_{y \in \{0,1\}^n} |y\rangle$

$$D\left(\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle\right) =$$

3. Mesurer le registre. Si le résultat z ne vérifie pas $f(z) = 1$, recommencer à l'étape 1.

Algorithme de Grover

Promesse : $f : \{0,1\}^n \to \{0,1\}$ telle que $|f^{-1}(1)| = 1$.
Problème : Trouver x_0 tel que $f(x_0) = 1$.
Algorithme classique : $\Theta(N)$ appels à f avec $N = 2^n$. ($N/2$ en moyenne)
Algorithme quantique : $O(\sqrt{N})$ appels à U_f.

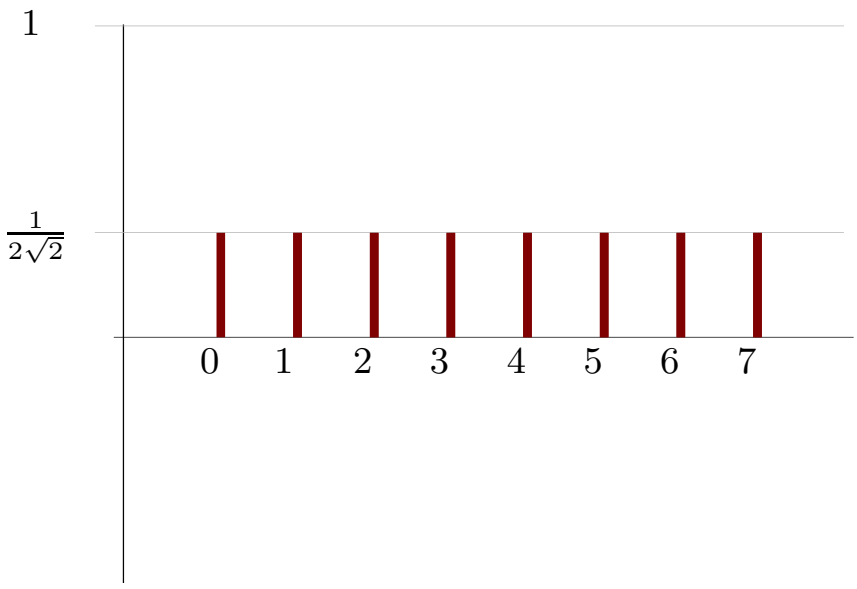
1. Préparer un registre de n qubits dans l'état $\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = H^{\otimes n} |0 \dots 0\rangle$
2. Répéter $\frac{\pi\sqrt{N}}{4}$ fois :
   - (a) Appliquer $U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$
   - (b) Appliquer $D : |x\rangle \mapsto -|x\rangle + \frac{2}{N} \sum_{y \in \{0,1\}^n} |y\rangle$

$$D\left(\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle\right) = \sum_{x \in \{0,1\}^n} (2\mu - \alpha_x) |x\rangle \quad \text{où } \mu = \frac{1}{N} \sum_{x \in \{0,1\}^n} \alpha_x$$

3. Mesurer le registre. Si le résultat z ne vérifie pas $f(z) = 1$, recommencer à l'étape 1.

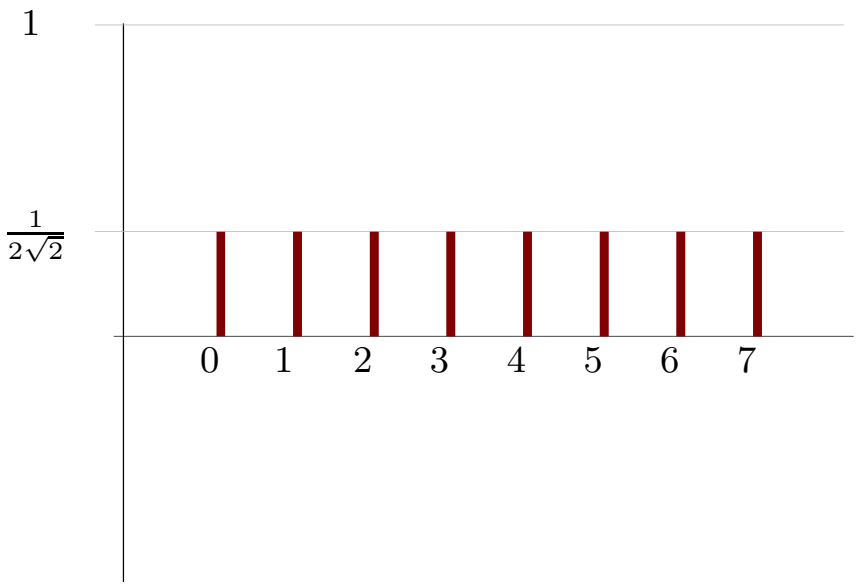
1ère Interprétation Graphique

Sur un exemple : $N = 8$ et $f(5) = 1$. $\frac{\pi\sqrt{8}}{4} \approx 2.2$.
Etape 1 : $\frac{1}{\sqrt{N}} \sum_x |x\rangle$:



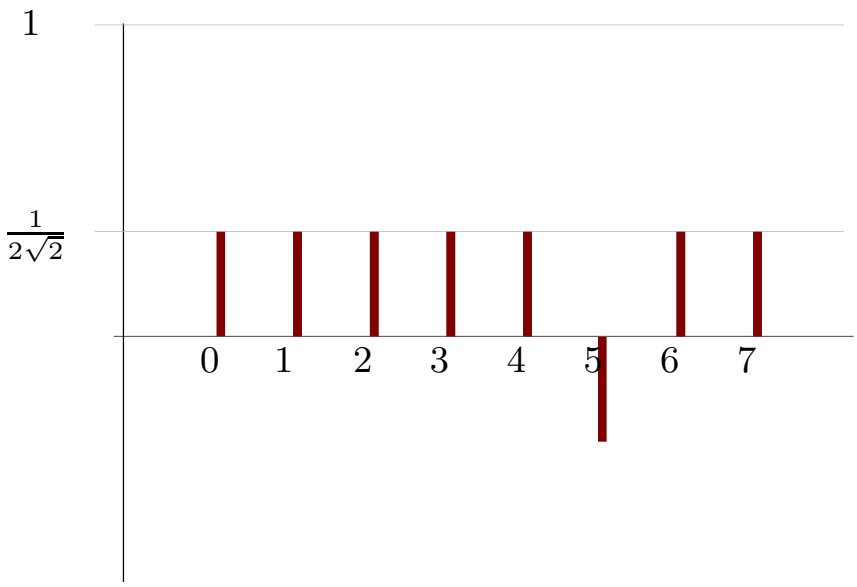
1ère Interprétation Graphique

Sur un exemple : $N = 8$ et $f(5) = 1$. $\frac{\pi\sqrt{8}}{4} \approx 2.2$.
Etape $2.a$: Appliquer U_f : $|x\rangle \mapsto (-1)^{f(x)} |x\rangle$



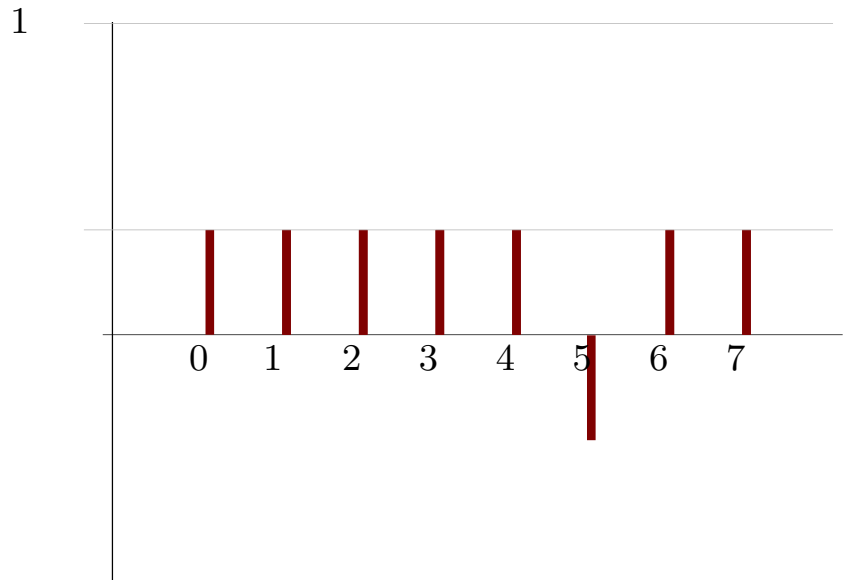
1ère Interprétation Graphique

Sur un exemple : $N = 8$ et $f(5) = 1$. $\frac{\pi\sqrt{8}}{4} \approx 2.2$.
Etape $2.a$: Appliquer U_f : $|x\rangle \mapsto (-1)^{f(x)} |x\rangle$



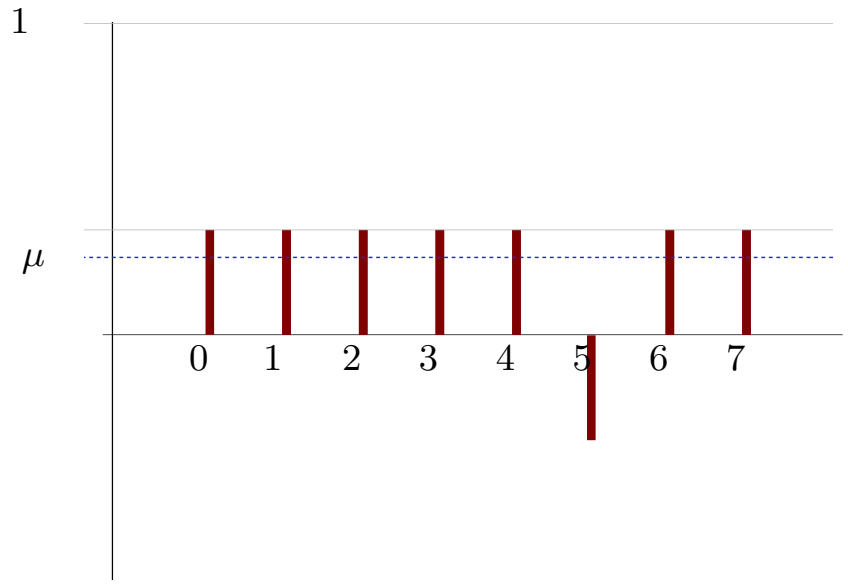
1ère Interprétation Graphique

Sur un exemple : $N = 8$ et $f(5) = 1$. $\frac{\pi\sqrt{8}}{4} \approx 2.2$.
Etape $2.b$: $D = \sum_x \alpha_x |x\rangle \mapsto \sum_x (2\mu - \alpha_x) |x\rangle$, où $\mu = \frac{1}{N} \sum_y \alpha_y$



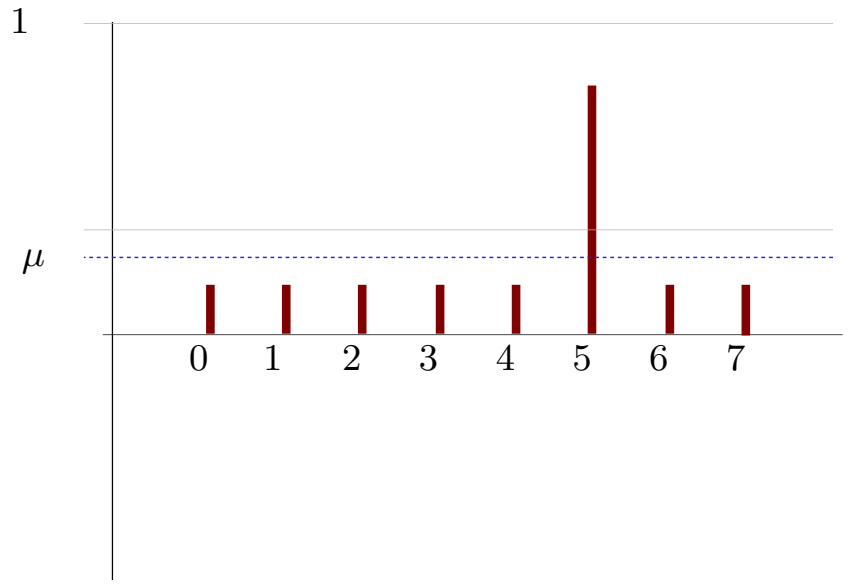
1ère Interprétation Graphique

Sur un exemple : $N = 8$ et $f(5) = 1$. $\frac{\pi\sqrt{8}}{4} \approx 2.2$.
Etape $2.b$: $D = \sum_x \alpha_x |x\rangle \mapsto \sum_x (2\mu - \alpha_x) |x\rangle$, où $\mu = \frac{1}{N} \sum_y \alpha_y$



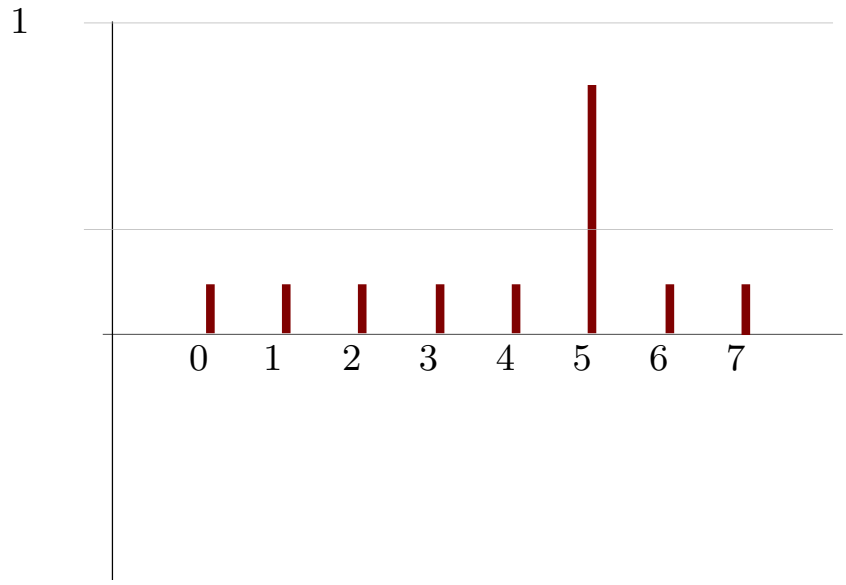
1ère Interprétation Graphique

Sur un exemple : $N = 8$ et $f(5) = 1$. $\frac{\pi\sqrt{8}}{4} \approx 2.2$.
Etape $2.b$: $D = \sum_x \alpha_x |x\rangle \mapsto \sum_x (2\mu - \alpha_x) |x\rangle$, où $\mu = \frac{1}{N} \sum_y \alpha_y$



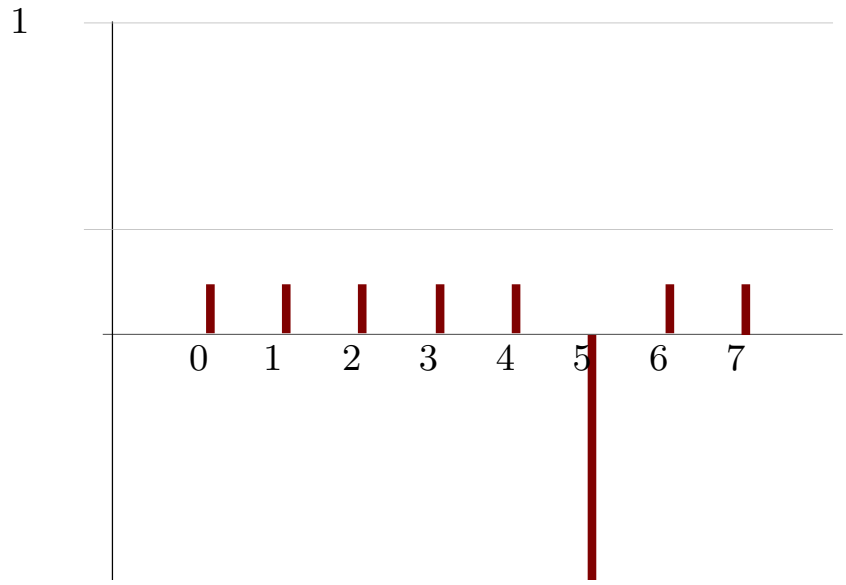
1ère Interprétation Graphique

Sur un exemple : $N = 8$ et $f(5) = 1$. $\frac{\pi\sqrt{8}}{4} \approx 2.2$.
Etape $2.a$: Appliquer U_f : $|x\rangle \mapsto (-1)^{f(x)} |x\rangle$



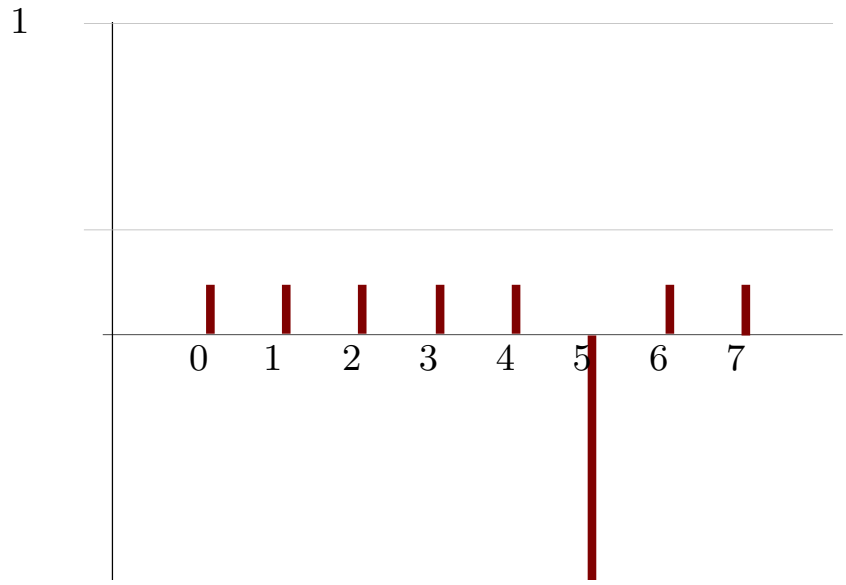
1ère Interprétation Graphique

Sur un exemple : $N = 8$ et $f(5) = 1$. $\frac{\pi\sqrt{8}}{4} \approx 2.2$.
Etape $2.a$: Appliquer U_f : $|x\rangle \mapsto (-1)^{f(x)} |x\rangle$



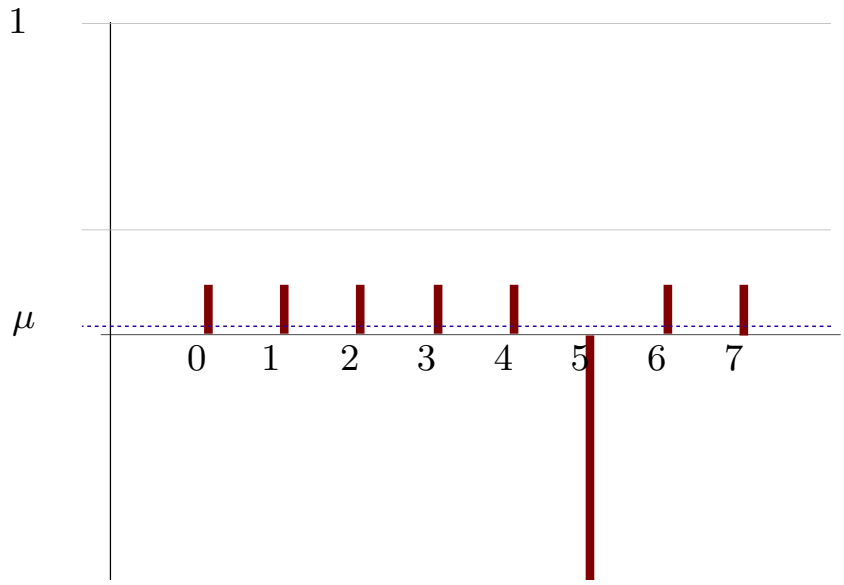
1ère Interprétation Graphique

Sur un exemple : $N = 8$ et $f(5) = 1$. $\frac{\pi\sqrt{8}}{4} \approx 2.2$.
Etape $2.b$: $D = \sum_x \alpha_x |x\rangle \mapsto \sum_x (2\mu - \alpha_x) |x\rangle$, où $\mu = \frac{1}{N} \sum_y \alpha_y$



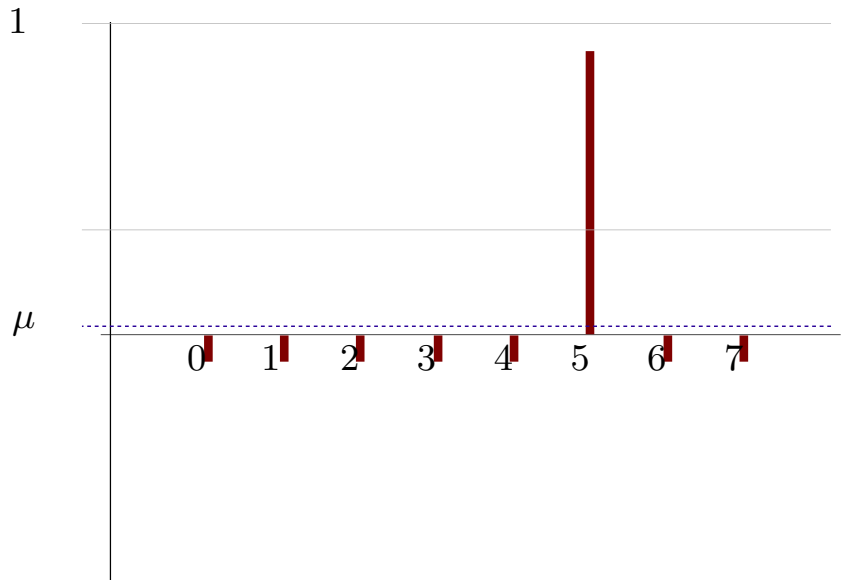
1ère Interprétation Graphique

Sur un exemple : $N = 8$ et $f(5) = 1$. $\frac{\pi\sqrt{8}}{4} \approx 2.2$.
Etape $2.b$: $D = \sum_x \alpha_x |x\rangle \mapsto \sum_x (2\mu - \alpha_x) |x\rangle$, où $\mu = \frac{1}{N} \sum_y \alpha_y$



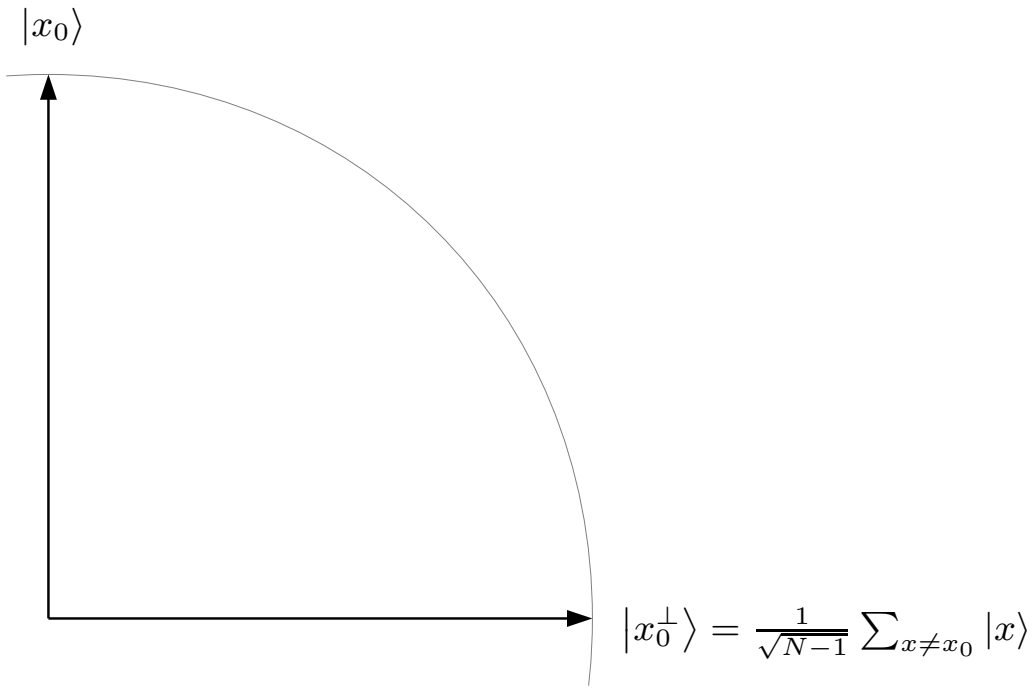
1ère Interprétation Graphique

Sur un exemple : $N = 8$ et $f(5) = 1$. $\frac{\pi\sqrt{8}}{4} \approx 2.2$.
Etape $2.b$: $D = \sum_x \alpha_x |x\rangle \mapsto \sum_x (2\mu - \alpha_x) |x\rangle$, où $\mu = \frac{1}{N} \sum_y \alpha_y$



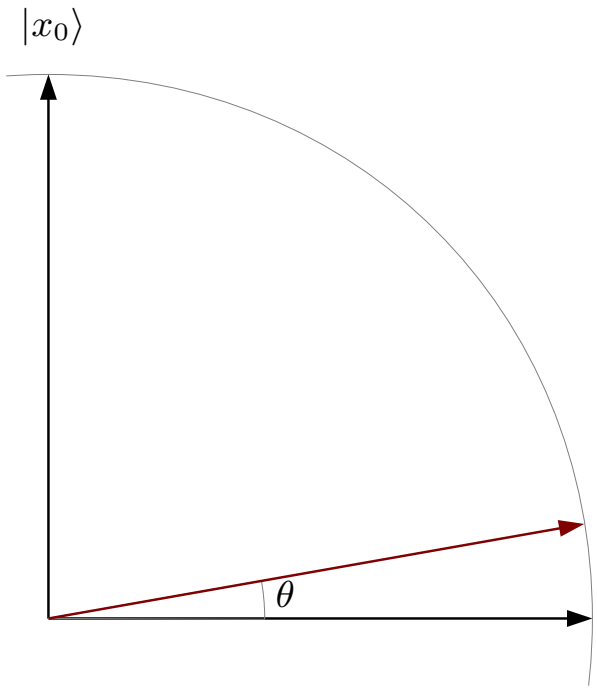
2ème Interprétation Graphique

Etape 1 : $\frac{1}{\sqrt{N}} \sum_x |x\rangle$



2ème Interprétation Graphique

Etape 1 : $\frac{1}{\sqrt{N}} \sum_x |x\rangle = \frac{1}{\sqrt{N}} |x_0\rangle + \sqrt{\frac{N-1}{N}} |x_0^\perp\rangle$



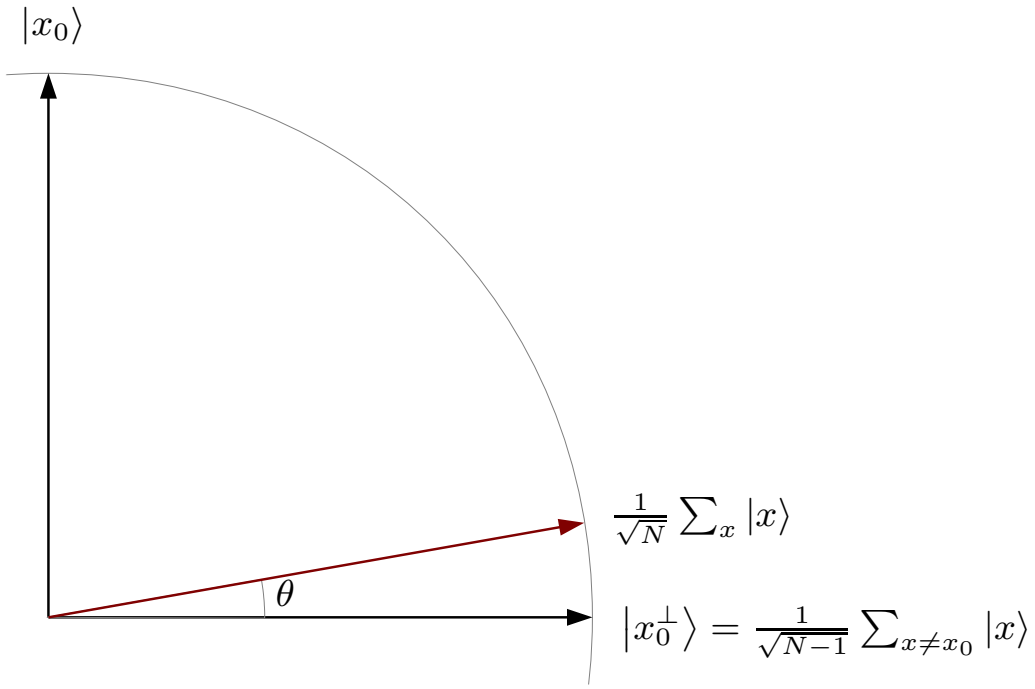
$\theta = \arcsin(\frac{1}{\sqrt{N}}) \approx \frac{1}{\sqrt{N}}$

$\frac{1}{\sqrt{N}} \sum_x |x\rangle$

$|x_0^\perp\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$

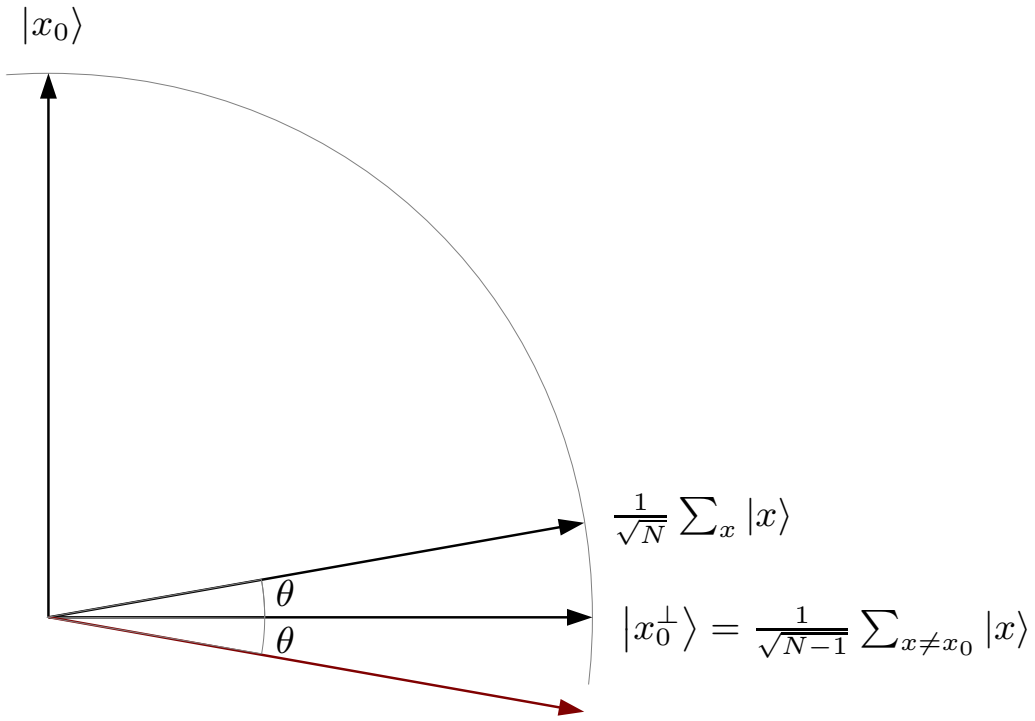
2ème Interprétation Graphique

Etape $2.a$: Appliquer $U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$



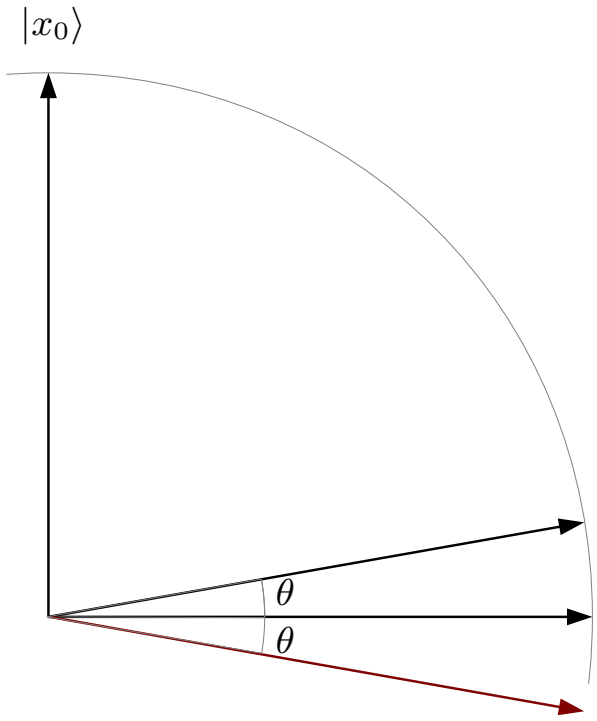
2ème Interprétation Graphique

Etape $2.a$: Appliquer $U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$



2ème Interprétation Graphique

Etape $2.b$: $D = \sum_x \alpha_x |x\rangle \mapsto \sum_x (2\mu - \alpha_x) |x\rangle$, où $\mu = \frac{1}{N} \sum_y \alpha_y$



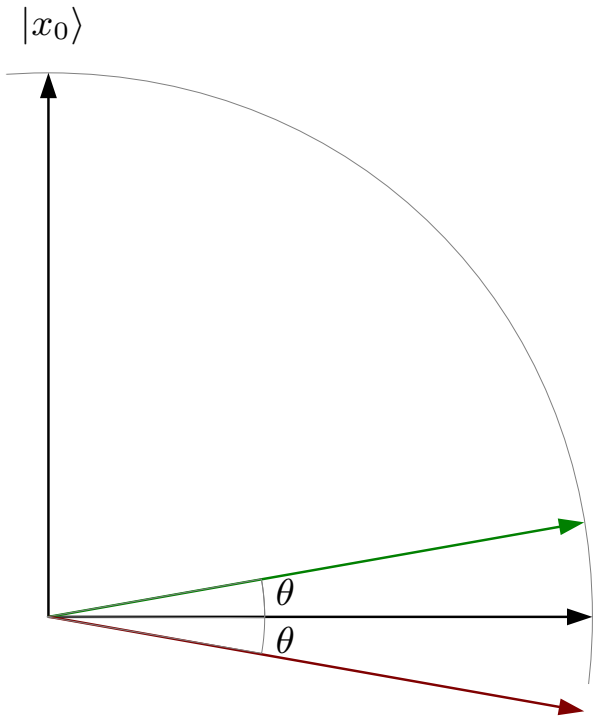
D est une réflexion

$\frac{1}{\sqrt{N}} \sum_x |x\rangle$

$|x_0^\perp\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$

2ème Interprétation Graphique

Etape $2.b$: $D = \sum_x \alpha_x |x\rangle \mapsto \sum_x (2\mu - \alpha_x) |x\rangle$, où $\mu = \frac{1}{N} \sum_y \alpha_y$



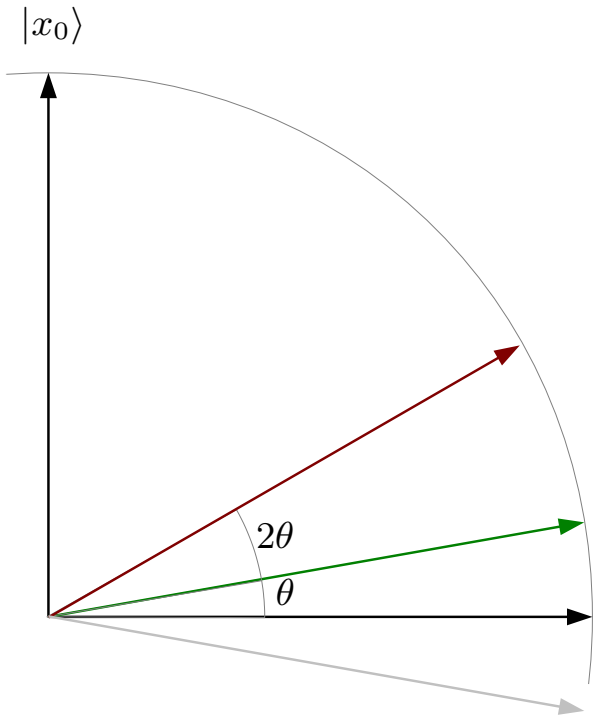
D est une réflexion par rapport à $\frac{1}{\sqrt{N}} \sum_x |x\rangle$

$\frac{1}{\sqrt{N}} \sum_x |x\rangle$

$|x_0^\perp\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$

2ème Interprétation Graphique

Etape $2.b$: $D = \sum_x \alpha_x |x\rangle \mapsto \sum_x (2\mu - \alpha_x) |x\rangle$, où $\mu = \frac{1}{N} \sum_y \alpha_y$



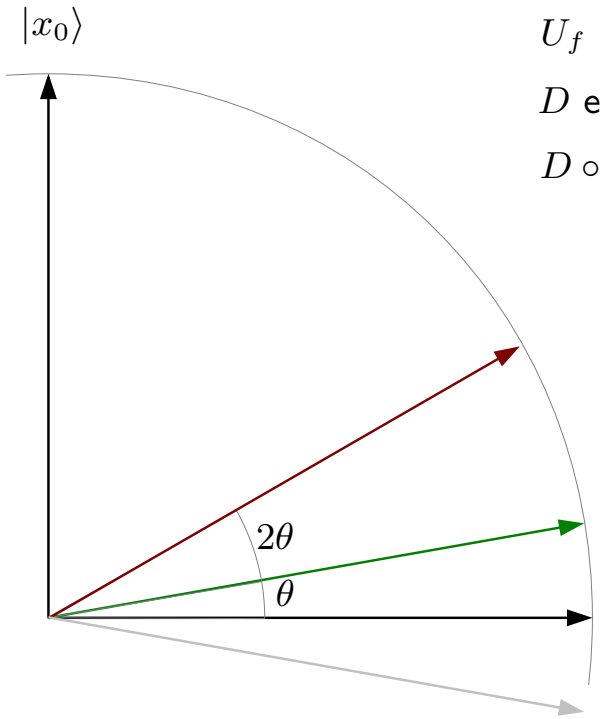
D est une réflexion par rapport à $\frac{1}{\sqrt{N}} \sum_x |x\rangle$

$\frac{1}{\sqrt{N}} \sum_x |x\rangle$

$|x_0^\perp\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$

2ème Interprétation Graphique

Etapes $2.a + 2.b$:



U_f est une réflexion p/r $\left|x_0^{\perp}\right\rangle$

D est une réflexion p/r $\frac{1}{\sqrt{N}} \sum_x |x\rangle$

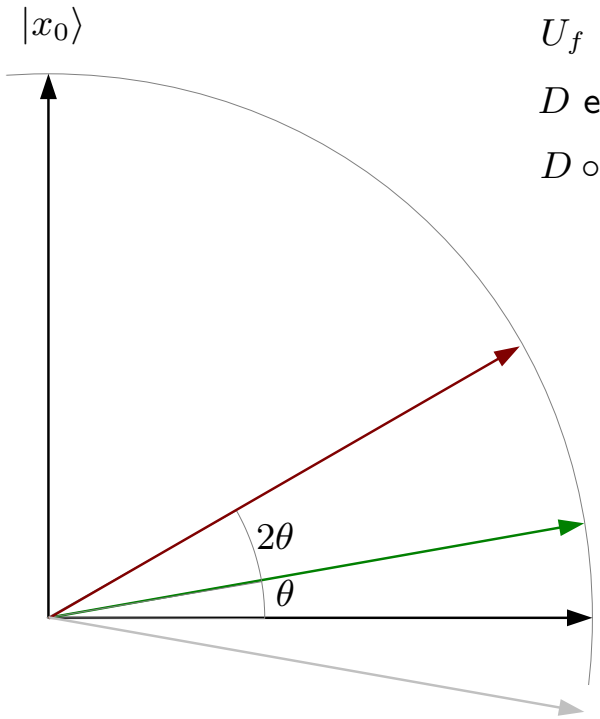
$D \circ U_f$

$\frac{1}{\sqrt{N}} \sum_x |x\rangle$

$\left|x_0^{\perp}\right\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$

2ème Interprétation Graphique

Etapes $2.a + 2.b$:



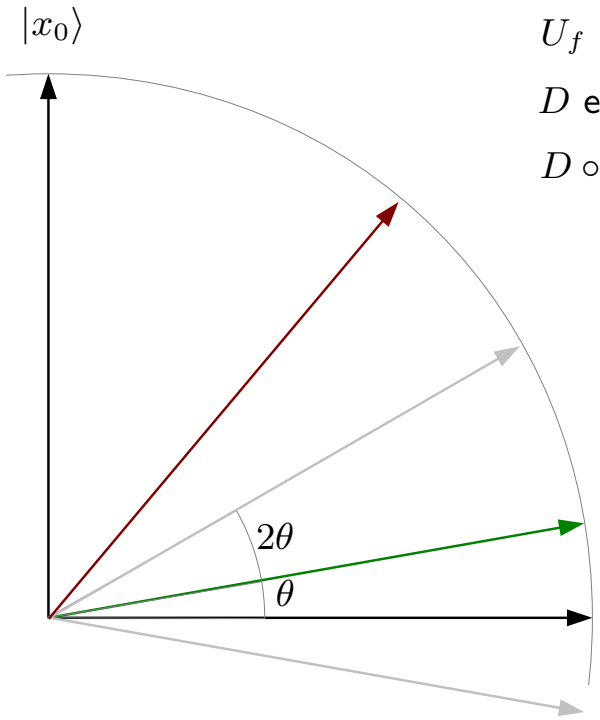
U_f est une réflexion p/r $|x_0^\perp\rangle$

D est une réflexion p/r $\frac{1}{\sqrt{N}} \sum_x |x\rangle$

$D \circ U_f$ est une rotation d'angle 2θ

2ème Interprétation Graphique

Etapes $2.a + 2.b$:



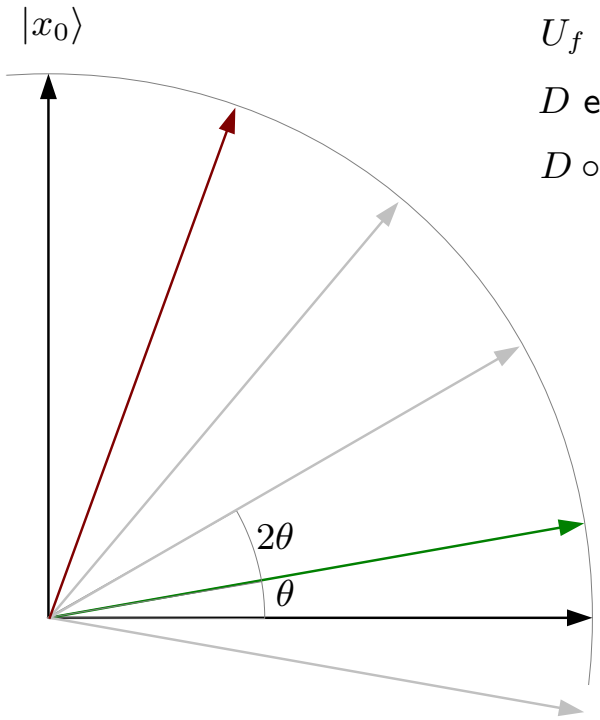
U_f est une réflexion p/r $|x_0^\perp\rangle$

D est une réflexion p/r $\frac{1}{\sqrt{N}} \sum_x |x\rangle$

$D \circ U_f$ est une rotation d'angle 2θ

2ème Interprétation Graphique

Etapes $2.a + 2.b$:



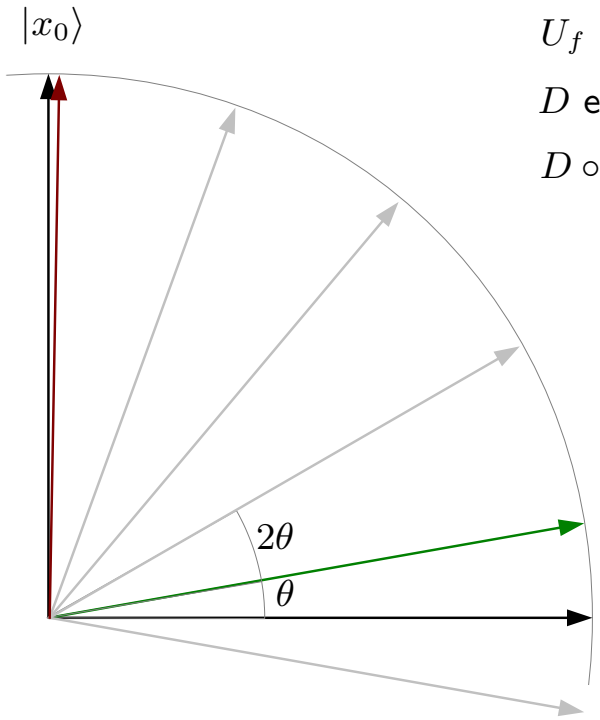
U_f est une réflexion p/r $|x_0^\perp\rangle$

D est une réflexion p/r $\frac{1}{\sqrt{N}} \sum_x |x\rangle$

$D \circ U_f$ est une rotation d'angle 2θ

2ème Interprétation Graphique

Etapes $2.a + 2.b$:



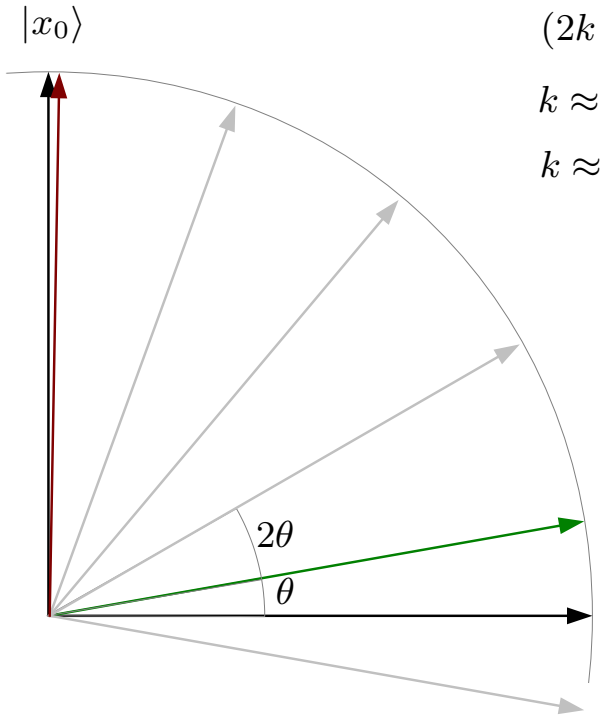
U_f est une réflexion p/r $|x_0^\perp\rangle$

D est une réflexion p/r $\frac{1}{\sqrt{N}} \sum_x |x\rangle$

$D \circ U_f$ est une rotation d'angle 2θ

2ème Interprétation Graphique

Etapes $2.a + 2.b$:



$(2k+1)\theta \approx \frac{\pi}{2}$

$k \approx \frac{\pi}{4\theta}$

$k \approx \frac{\pi\sqrt{N}}{4}$ car $\theta = \arcsin(\frac{1}{\sqrt{N}}) \approx \frac{1}{\sqrt{N}}$

$\frac{1}{\sqrt{N}} \sum_x |x\rangle$

$|x_0^\perp\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$

Algorithme de Grover

Promesse : $f : \{0,1\}^n \to \{0,1\}$ telle que $|f^{-1}(1)| = 1$.
Problème : Trouver x_0 tel que $f(x_0) = 1$.
Algorithme classique : $\Theta(N)$ appels à f avec $N = 2^n$. ($N/2$ en moyenne)
Algorithme quantique : $\Theta(\sqrt{N})$ appel à U_f.

1. Préparer un registre de n qubits dans l'état $\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = H^{\otimes n} |0 \dots 0\rangle$
2. Répéter $\frac{\pi\sqrt{N}}{4}$ fois :
   - (a) Appliquer $U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$
   - (b) Appliquer $D : |x\rangle \mapsto -|x\rangle + \frac{2}{N} \sum_{y \in \{0,1\}^n} |y\rangle$
3. Mesurer le registre. Si le résultat z ne vérifie pas $f(z) = 1$, recommencer à l'étape 1.

Factorisation

Algorithme de factorisation :
Problème : Etant donné un entier de taille n, trouver ses facteurs premiers.
Algorithme classique : pas d'algorithme polynomial connu.
Algorithme quantique : $O(n^3)$ opérations [Shor 94]

Une recette de factorisation...

Pour trouver un facteur non trivial de N :

1. Prendre un nombre aléatoire $a < N$
2. Si $pgcd(a, N) \neq 1$, on a un facteur de N
3. Sinon, trouver la période r de la fonction $f : x \mapsto a^x \bmod N$
4. Si r est impair, aller à l'étape 1,
5. Si $a^{r/2} = -1 \bmod N$, aller à l'étape 1,
6. $pgcd(a^{r/2} \pm 1, N)$ est un facteur non trivial de N.

Une Information Quantique

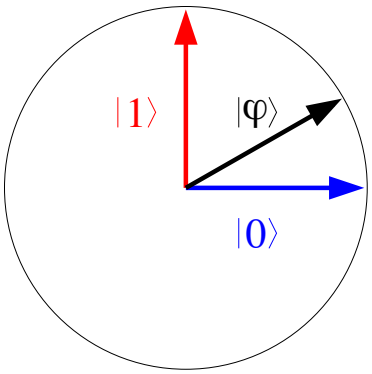
- Brique de base de l'information :

$$\mathbf{0}, \mathbf{1}$$

- Nous vivons dans un monde quantique :

$$\alpha \left|\mathbf{0}\right\rangle + \beta \left|\mathbf{1}\right\rangle$$

avec $\alpha, \beta \in \mathbb{C}$ et $|\alpha|^2 + |\beta|^2 = 1$



Une Information Quantique

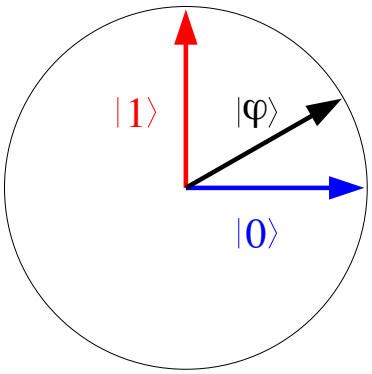
- Brique de base de l'information :

$$\mathbf{0}, \mathbf{1}$$

- Nous vivons dans un monde quantique :

$$\alpha \left|\mathbf{0}\right\rangle + \beta \left|\mathbf{1}\right\rangle$$

avec $\alpha, \beta \in \mathbb{C}$ et $|\alpha|^2 + |\beta|^2 = 1$



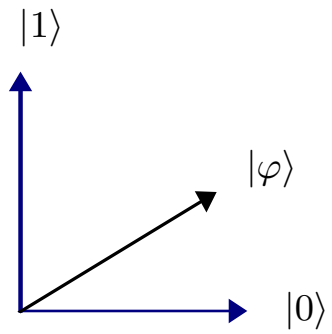
Mesurer, c'est Transformer

$$\alpha\,|0\rangle + \beta\,|1\rangle \xrightarrow{|\alpha|^2} |0\rangle \text{ on mesure } 0$$
$$\alpha\,|0\rangle + \beta\,|1\rangle \xrightarrow{|\beta|^2} |1\rangle \text{ on mesure } 1$$

La mesure est **probabiliste** et **irréversible**.

$$\text{Mesure} \implies \text{Interaction} \implies \text{Transformation}$$

Bases et Mesures



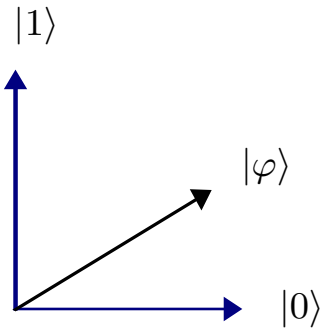
base standard

A chaque base orthonormée correspond une mesure.

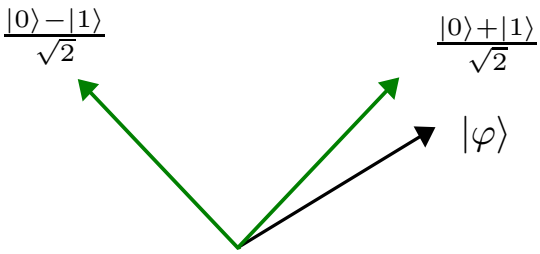
On change de base :

- en tournant l'appareil de mesure (!)
- en mesurant une quantité physique différente (énergie, position, . . .)

Bases et Mesures



base standard



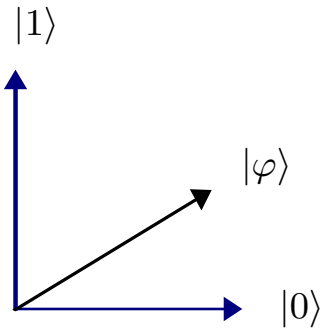
base diagonale

A chaque base orthonormée correspond une mesure.

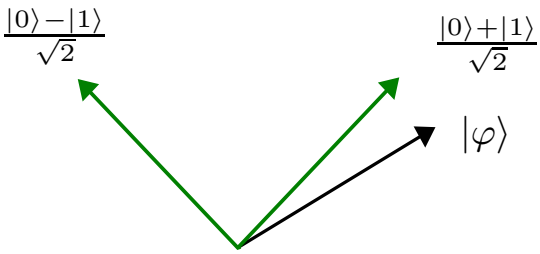
On change de base :

- en tournant l'appareil de mesure (!)
- en mesurant une quantité physique différente (énergie, position, . . .)

Bases et Mesures



base standard



base diagonale

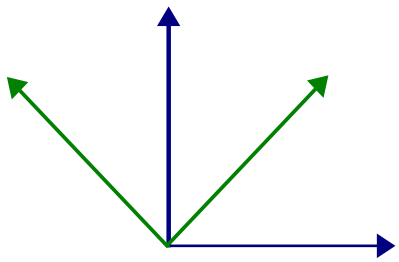
A chaque base orthonormée correspond une mesure.

On change de base :

- en tournant l'appareil de mesure (!)
- en mesurant une quantité physique différente (énergie, position, . . .)

Bases Complementaires

Bases complémentaires : la mesure de tout vecteur d'une des bases dans l'autre donne un bit aléatoire uniforme.



Si on mesure un qubit dans une base puis dans une seconde complémentaire, la seconde mesure n'apporte aucune information sur l'état initial du système. (principe d'incertitude)

BB84

Classical One-Time Pad

Message $m \in \{0,1\}^n$
Shared private key $k \in \{0,1\}^n$

$k \in \{0,1\}^n$

Encoding : $w = m + k$
Alice sends w to Bob ——————————> Bob receives w
Decoding :
$w + k = m + k + k = m$

Unconditionally secure, but how to share a large private key ?

Quantum Key Distribution (BB84)

BB84

random bit	random basis	sent qubit
1		

BB84

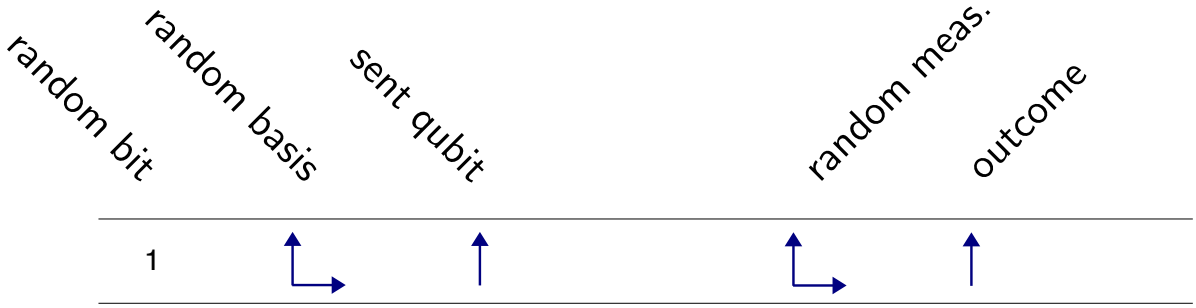
random bit	random basis	sent qubit
1		

BB84

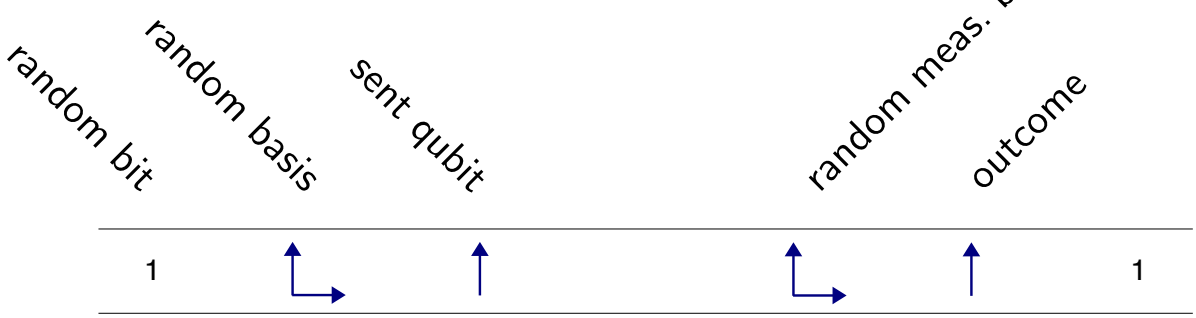
random bit | random basis | sent qubit | random meas. basis

1

BB84


random bit
random basis
sent qubit
random meas. basis
outcome
1

BB84


random bit
random basis
sent qubit
random meas. basis
outcome
1
1

BB84

random bit	random basis	sent qubit	random meas. basis	outcome	
1					1
1					

BB84

random bit	random basis	sent qubit	random meas. basis	outcome
1	↱	↑	↱	1
1	↱	↑	↗	0

BB84

random bit	random basis	sent qubit	random meas. basis	outcome
1					1
1					1

BB84

random bit	random basis	sent qubit	random meas. basis	outcome
1					1
1					1
1					0

BB84

random bit	random basis	sent qubit	random meas. basis	outcome
1	↑→	↑	↑→	1
1	↑→	↑	↗↖	1
1	↗↖	↖	↑→	0
0	↗↖	↗	↗↖	0

BB84

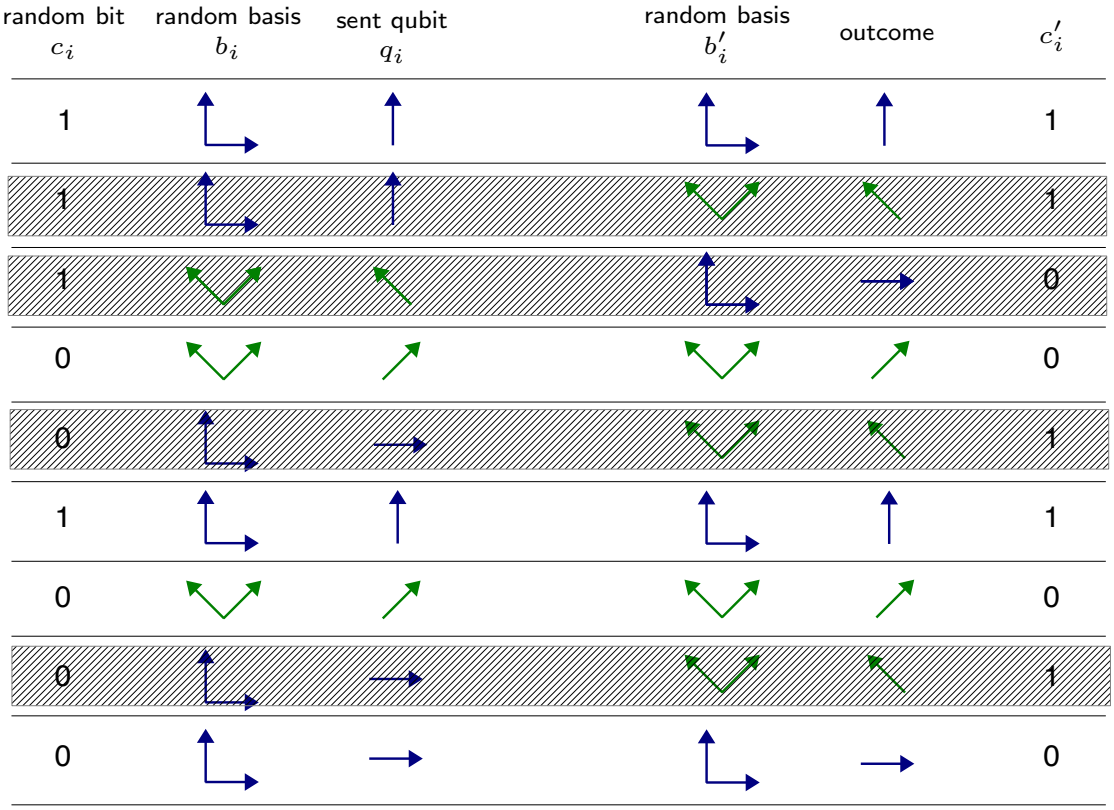
random bit c_i	random basis b_i	sent qubit q_i	random basis b'_i	outcome	c'_i
1					1
1					1
1					0
0					0
0					1
1					1
0					0
0					1
0					0

BB84

random bit c_i	random basis b_i	sent qubit q_i	random basis b'_i	outcome	c'_i
1					1
1					1
1					0
0					0
0					1
1					1
0					0
0					1
0					0

Alice and Bob announce their basis

BB84



Alice and Bob keep the common basis only

BB84

random bit c_i	random basis b_i	sent qubit q_i	random basis b'_i	outcome	c'_i
1					1
0					0
1					1
0					0
0					0

Alice and Bob keep the common basis only

BB84

random bit c_i	random basis b_i	sent qubit q_i	random basis b'_i	outcome	c'_i
1					1
0					0
1					1
0					0
0					0

Alice and Bob keep the common basis only

BB84

random bit c_i	random basis b_i	sent qubit q_i	random basis b'_i	outcome	c'_i
1					1
0					0
1					1
0					0
0					0

(If there is no spy,) Alice and Bob share random bits.

BB84

random bit c_i	random basis b_i	sent qubit q_i	random basis b'_i	outcome	c'_i
1					1
0					0
1					1
0					0
0					0

The presence of a spy would introduce some noise.

BB84

random bit c_i	random basis b_i	sent qubit q_i	random basis b'_i	outcome	c'_i
1					1
0					0
1					1
0					0
0					0

The presence of a spy would introduce some noise.

$\Rightarrow$ Alice and Bob announce half of the bits to detect the presence of a spy.

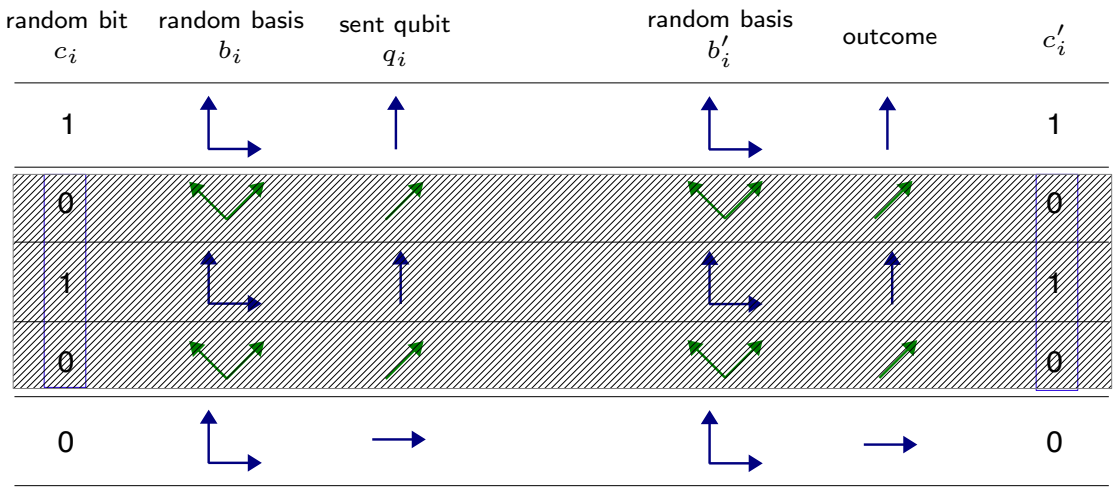
BB84

random bit c_i	random basis b_i	sent qubit q_i	random basis b'_i	outcome	c'_i
1					1
0					0
1					1
0					0
0					0

The presence of a spy would introduce some noise.

$\Rightarrow$ Alice and Bob announce half of the bits to detect the presence of a spy.

BB84



The presence of a spy would introduce some noise.

$\Rightarrow$ Alice and Bob announce half of the bits to detect the presence of a spy.

$\Rightarrow$ If no spy is detected, they keep the remaining bits as a shared private key.

BB84

- Alice chooses uniformly at random $4n$ bits c_i and $4n$ basis b_i. She encodes c_i in the basis b_i and sends the resulting state to Bob.
- Bob chooses uniformly at random $4n$ basis b'_i and measures the received qubit according to b'_i. Let c'_i be the outcomes of these measurements.
- Alice and Bob announce the basis b_i and b'_i and keep only the cases $b_i = b'_i$.
- Alice chooses at random half of the remaining bits as check bits. They announce the value of the check bits, if some check bits do not agree, they abort the protocol.

c_i	b_i	q_i	b'_i	outcome	c'_i
1					1
1					1
1					0
0					0

A Particular Attack

Eve's attack : Given $\epsilon \in [0, 1/4]$, for each qubit q_i

– with prob 4ϵ, Eve measures q_i in  Let c_i^* be its classical outcome.

– with prob $1-4\epsilon$, Eve does not measure q_i and picks c_i^* randomly in $\{0, 1\}$.

Probability of guessing $(Pr[c_i = c_i^*])$:

A Particular Attack

Eve's attack : Given $\epsilon \in [0, 1/4]$, for each qubit q_i

– with prob 4ϵ, Eve measures q_i in  Let c_i^* be its classical outcome.

– with prob $1-4\epsilon$, Eve does not measure q_i and picks c_i^* randomly in $\{0, 1\}$.

Probability of guessing $(Pr[c_i = c_i^*])$:

$Pr[c_i{=}c_i^*] = 4\epsilon\Big(\frac{1}{2}Pr[c_i{=}c_i^*|b_i{=}$ $] + \frac{1}{2}Pr[c_i{=}c_i^*|b_i{=}$ $]\Big) + (1-4\epsilon)\frac{1}{2}$

A Particular Attack

Eve's attack : Given $\epsilon \in [0, 1/4]$, for each qubit q_i

– with prob 4ϵ, Eve measures q_i in  Let c_i^* be its classical outcome.

– with prob $1-4\epsilon$, Eve does not measure q_i and picks c_i^* randomly in $\{0, 1\}$.

Probability of guessing $(Pr[c_i = c_i^*])$:

$$Pr[c_i{=}c_i^*] = 4\epsilon\Big(\tfrac{1}{2}\underbrace{Pr[c_i{=}c_i^*|b_i{=}\uparrow\rightarrow]}_{1} + \tfrac{1}{2}\underbrace{Pr[c_i{=}c_i^*|b_i{=}\nwarrow\nearrow]}_{1/2}\Big) + (1-4\epsilon)\tfrac{1}{2}$$

A Particular Attack

Eve's attack : Given $\epsilon \in [0, 1/4]$, for each qubit q_i

– with prob 4ϵ, Eve measures q_i in  Let c_i^* be its classical outcome.

– with prob $1-4\epsilon$, Eve does not measure q_i and picks c_i^* randomly in $\{0, 1\}$.

Probability of guessing $(Pr[c_i = c_i^*])$:

$$Pr[c_i{=}c_i^*] = 4\epsilon\Big(\tfrac{1}{2}\underbrace{Pr[c_i{=}c_i^*|b_i{=}\uparrow\rightarrow]}_{1} + \tfrac{1}{2}\underbrace{Pr[c_i{=}c_i^*|b_i{=}\nwarrow\nearrow]}_{1/2}\Big) + (1-4\epsilon)\tfrac{1}{2}$$

$$= \tfrac{1}{2} + \epsilon$$

A Particular Attack

Eve's attack : Given $\epsilon \in [0, 1/4]$, for each qubit q_i

– with prob 4ϵ, Eve measures q_i in  Let c_i^* be its classical outcome.

– with prob $1-4\epsilon$, Eve does not measure q_i and picks c_i^* randomly in $\{0, 1\}$.

Probability of guessing ($Pr[c_i = c_i^*]$) :

$$Pr[c_i{=}c_i^*] = 4\epsilon\Big(\tfrac{1}{2}\underbrace{Pr[c_i{=}c_i^*|b_i{=}\uparrow_{\rightarrow}]}_{1} + \tfrac{1}{2}\underbrace{Pr[c_i{=}c_i^*|b_i{=}\nwarrow\!\!\nearrow]}_{1/2}\Big) + (1{-}4\epsilon)\tfrac{1}{2}$$
$$= \tfrac{1}{2} + \epsilon$$

Probability of disturbing ($Pr[c_i \neq c_i' |\ b_i = b_i']$) :

$$Pr[c_i{\neq}c_i'|b_i{=}b_i'] = 4\epsilon\Big(\tfrac{1}{2}Pr[c_i{\neq}c_i'|b_i{=}b_i'{=}\uparrow_{\rightarrow}] + \tfrac{1}{2}Pr[c_i{\neq}c_i'|b_i{=}b_i'{=}\nwarrow\!\!\nearrow]\Big) + (1{-}4\epsilon).0$$

A Particular Attack

Eve's attack : Given $\epsilon \in [0, 1/4]$, for each qubit q_i

– with prob 4ϵ, Eve measures q_i in  Let c_i^* be its classical outcome.

– with prob $1-4\epsilon$, Eve does not measure q_i and picks c_i^* randomly in $\{0, 1\}$.

Probability of guessing ($Pr[c_i = c_i^*]$) :

$$Pr[c_i{=}c_i^*] = 4\epsilon\Big(\tfrac{1}{2}\underbrace{Pr[c_i{=}c_i^*|b_i{=}\uparrow_{\rightarrow}]}_{1} + \tfrac{1}{2}\underbrace{Pr[c_i{=}c_i^*|b_i{=}\nwarrow\!\!\nearrow]}_{1/2}\Big) + (1{-}4\epsilon)\tfrac{1}{2}$$
$$= \tfrac{1}{2} + \epsilon$$

Probability of disturbing ($Pr[c_i \neq c_i'|\ b_i = b_i']$) :

$$Pr[c_i{\neq}c_i'|b_i{=}b_i'] = 4\epsilon\Big(\tfrac{1}{2}\underbrace{Pr[c_i{\neq}c_i'|b_i{=}b_i'{=}\uparrow_{\rightarrow}]}_{0} + \tfrac{1}{2}\underbrace{Pr[c_i{\neq}c_i'|b_i{=}b_i'{=}\nwarrow\!\!\nearrow]}_{1/2}\Big) + (1{-}4\epsilon).0$$

A Particular Attack

Eve's attack : Given $\epsilon \in [0, 1/4]$, for each qubit q_i

– with prob 4ϵ, Eve measures q_i in  Let c_i^* be its classical outcome.

– with prob $1-4\epsilon$, Eve does not measure q_i and picks c_i^* randomly in $\{0, 1\}$.

Probability of guessing ($Pr[c_i = c_i^*]$) :

$$Pr[c_i{=}c_i^*] = 4\epsilon\Big(\tfrac{1}{2}\underbrace{Pr[c_i{=}c_i^*|b_i{=}\uparrow_\rightarrow]}_{1} + \tfrac{1}{2}\underbrace{Pr[c_i{=}c_i^*|b_i{=}\nwarrow\!\nearrow]}_{1/2}\Big) + (1{-}4\epsilon)\tfrac{1}{2}$$
$$= \tfrac{1}{2} + \epsilon$$

Probability of disturbing ($Pr[c_i \neq c_i' |\ b_i = b_i']$) :

$$Pr[c_i{\neq}c_i'|b_i{=}b_i'] = 4\epsilon\Big(\tfrac{1}{2}\underbrace{Pr[c_i{\neq}c_i'|b_i{=}b_i'{=}\uparrow_\rightarrow]}_{0} + \tfrac{1}{2}\underbrace{Pr[c_i{\neq}c_i'|b_i{=}b_i'{=}\nwarrow\!\nearrow]}_{1/2}\Big) + (1{-}4\epsilon).0$$
$$= \epsilon$$

A Particular Attack

Eve's attack : Given $\epsilon \in [0, 1/4]$, for each qubit q_i

– with prob 4ϵ, Eve measures q_i in  Let c_i^* be its classical outcome.

– with prob $1-4\epsilon$, Eve does not measure q_i and picks c_i^* randomly in $\{0, 1\}$.

- Eve guesses with probability $\frac{1}{2} + \epsilon$.
- Eve introduces an error with probability ϵ.

random bit c_i	random basis b_i	sent qubit q_i	random basis b_i	outcome	c_i'
1					0
0					0
1					1
0					1
0					0

Noisy Channel

The protocol admits up to 11% of errors when Alice and Bob announce their check bits, which implies that

- Alice and Bob do not share the same key
- Eve has some information about the key

Noisy Channel

The protocol admits up to 11% of errors when Alice and Bob announce their check bits, which implies that

- Alice and Bob do not share the same key
  $\rightarrow$ Information reconciliation
- Eve has some information about the key
  $\rightarrow$ Privacy amplification

General proof of security

- Protocol introduced in 1984, proof of security 15 years later.
- Using the error rates, Alice and Bob can upper bound the knowledge of Eve (with no assumption on the attack)
- Proof is based on Quantum Correcting Codes.