

Informatique quantique IFT6155

Transformé de Fourier

Transformé de Fourier

La transformé de Fourier quantique est une transformation introduite par Peter Shor. Cette opération unitaire est probablement la plus importante. Elle seras utiliser dans trois algorithme important.

Transformé de Fourier

Définition de la transformé de Fourier sur n qubits

$$F_n |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i xy/2^n} |y\rangle$$

F_n est unitaire

$$(F_n |a\rangle)^\dagger (F_n |b\rangle)$$

$$\begin{aligned} &= \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} e^{2\pi i ax/2^n} |x\rangle \right)^\dagger \left(\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i by/2^n} |y\rangle \right) \\ &= \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} e^{-2\pi i ax/2^n} \langle x| \right) \left(\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i by/2^n} |y\rangle \right) \\ &= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (e^{-2\pi i ax/2^n}) (e^{2\pi i bx/2^n}) \\ &= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (e^{2\pi i (b-a)x/2^n}) \end{aligned}$$

F_n est unitaire

$$(F_n |a\rangle)^\dagger (F_n |b\rangle) = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (e^{2\pi i(b-a)x/2^n})$$

si $a = b$ alors

$$(F_n |a\rangle)^\dagger (F_n |a\rangle) = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (e^{2\pi i 0 x/2^n}) = \frac{1}{2^n} \sum_{x=0}^{2^n-1} 1 = 1$$

si $a \neq b$ alors

$$\begin{aligned} (F_n |a\rangle)^\dagger (F_n |b\rangle) &= \frac{1}{2^n} \sum_{x=0}^{2^n-1} e^{2\pi i(b-a)x/2^n} \\ &= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (e^{2\pi i(b-a)/2^n})^x \\ &= \frac{1}{2^n} \left(\frac{1 - e^{2\pi i(b-a)}}{1 - e^{2\pi i(b-a)/2^n}} \right) \\ &= \frac{1}{2^n} \left(\frac{1 - 1}{1 - e^{2\pi i(b-a)/2^n}} \right) \\ &= 0 \end{aligned}$$

Transformé de Fourier

$$F_n |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i xy/2^n} |y\rangle$$

$$F_1 = H$$

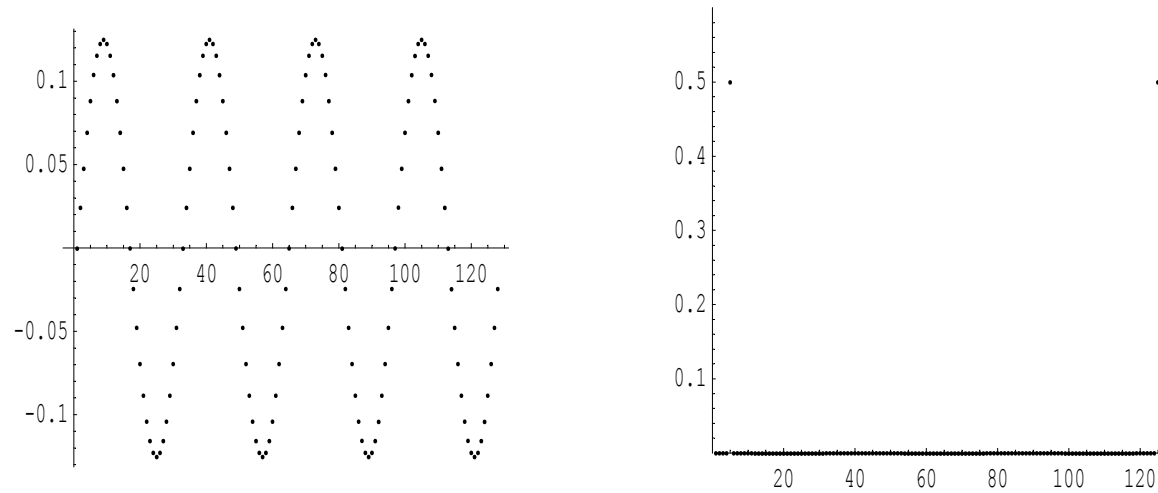
Si $w = e^{2\pi i/8}$ alors $w^8 = 1$ et

$$F_3 = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & w & w^2 & w^3 & w^4 & w^5 & w^6 & w^7 \\ 1 & w^2 & w^4 & w^6 & 1 & w^2 & w^4 & w^6 \\ 1 & w^3 & w^6 & w & w^4 & w^7 & w^2 & w^5 \\ 1 & w^4 & 1 & w^4 & 1 & w^4 & 1 & w^4 \\ 1 & w^5 & w^2 & w^7 & w^4 & w & w^6 & w^3 \\ 1 & w^6 & w^4 & w^2 & 1 & w^6 & w^4 & w^2 \\ 1 & w^7 & w^6 & w^5 & w^4 & w^3 & w^2 & w^1 \end{pmatrix}$$

$$F_n^\dagger |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{-2\pi i xy/2^n} |y\rangle$$

Examples

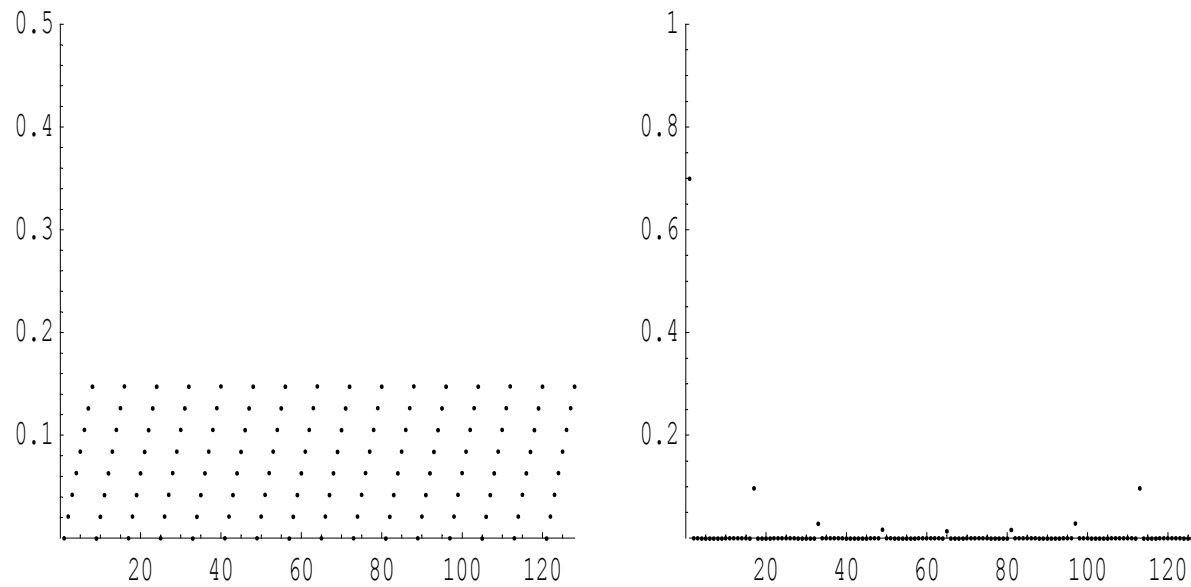
Soit $|\psi\rangle = \alpha \sum_{i=0}^{127} \sin(2\pi i/32) |i\rangle$ et $|\alpha_i|$ pour $F_7 |\psi\rangle = \sum_i \alpha_i |i\rangle$.



Il y a quatre périodes et la probabilité d'observer 4 ou 128-4 est 1.

Examples

Soit $|\psi\rangle$ avec des amplitudes réelles et $|\alpha_i|^2$ pour $F_7 |\psi\rangle = \sum_i \alpha_i |i\rangle$



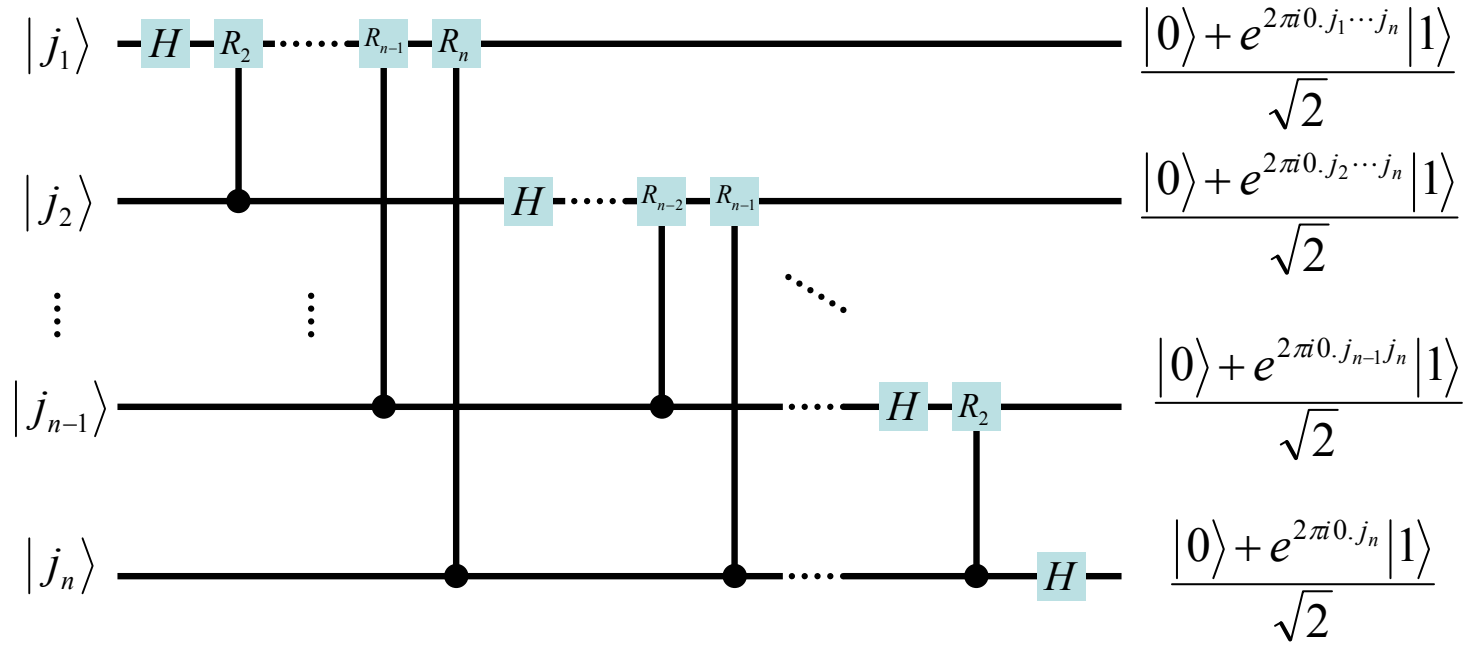
La probabilité d'observer 0 est proche de 0.7 et la probabilité d'observer 16 ou 128-16 est proche de 0.2.

Un peu d'algèbre

Si $|j\rangle = |j_1 j_2 \cdots j_n\rangle$,

$$\begin{aligned}
 F_n |j\rangle &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle \\
 &= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \cdots \sum_{k_n=0}^1 e^{2\pi i j \left(\sum_{l=1}^n k_l 2^{-l} \right)} |k_1 k_2 \cdots k_n\rangle \\
 &= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \cdots \sum_{k_n=0}^1 \prod_{l=1}^n e^{2\pi i j k_l 2^{-l}} |k_1 k_2 \cdots k_n\rangle \\
 &= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^1 \cdots \sum_{k_n=0}^1 \bigotimes_{l=1}^n e^{2\pi i j k_l 2^{-l}} |k_l\rangle \\
 &= \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^n \left(\sum_{k_l=0}^1 e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right) \\
 &= \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^n \left(|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right) \\
 &= \frac{(|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle)(|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle) \cdots (|0\rangle + e^{2\pi i 0 \cdot j_1 \cdots j_n} |1\rangle)}{\sqrt{2^n}}
 \end{aligned}$$

Circuit F_n



$$R_n = C-S_{2\pi/2^k}$$

$$F_n = \text{Ordre inverse} \prod_{i=1}^n \left(H_{[i]} \prod_{j=1}^{n-i} R_{j+1}[i+j,i] \right)$$

Analyse

L'état de départ

$$|j_1 j_2 \cdots j_n\rangle$$

après $H_{[1]}$

$$\begin{aligned} \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{j_1} |1\rangle) |j_2 \cdots j_n\rangle = \\ \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0 \cdot j_1} |1\rangle) |j_2 \cdots j_n\rangle \end{aligned}$$

après $R_{2[2,1]}$

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2} |1\rangle) |j_2 \cdots j_n\rangle$$

après $R_{3[3,1]} \cdots R_{n[n,1]}$

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0 \cdot j_1 \cdots j_n} |1\rangle) |j_2 \cdots j_n\rangle$$

Analyse

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.j_1 \cdots j_n} |1\rangle) |j_2 \cdots j_n\rangle$$

après $H_{[2]}$

$$\frac{1}{\sqrt{4}}(|0\rangle + e^{2\pi i 0.j_1 \cdots j_n} |1\rangle)(|0\rangle + e^{2\pi i 0.j_2} |1\rangle) |j_3 \cdots j_n\rangle$$

après $R_{2[3,2]} \cdots R_{n-1[n,2]}$

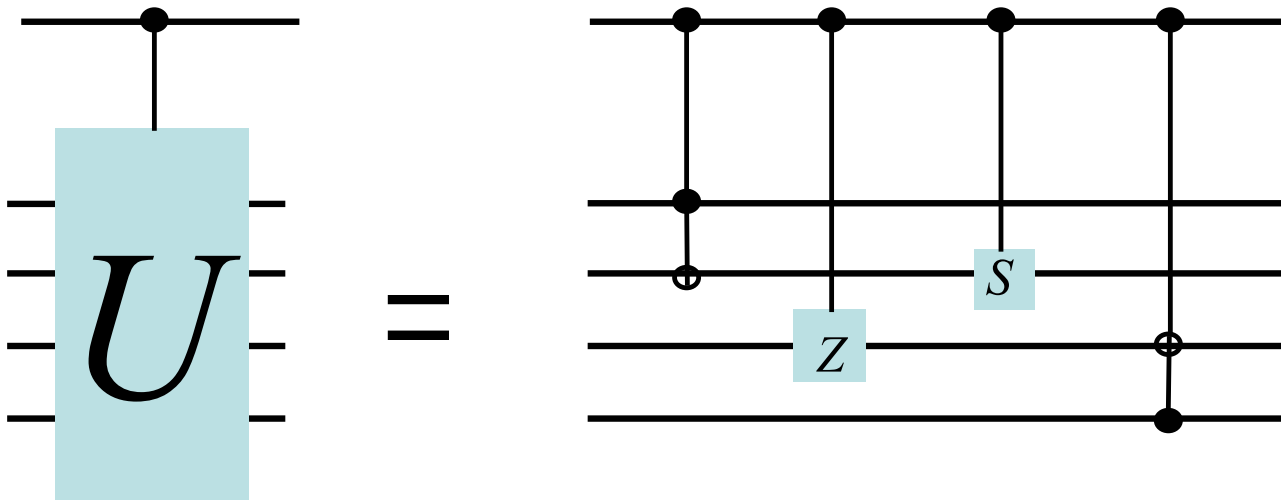
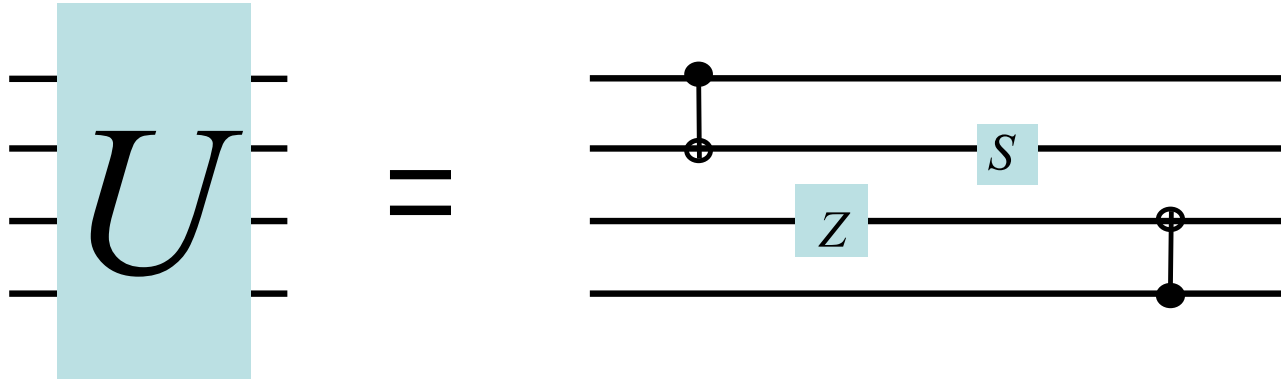
$$\frac{1}{\sqrt{4}}(|0\rangle + e^{2\pi i 0.j_1 \cdots j_n} |1\rangle)(|0\rangle + e^{2\pi i 0.j_2 \cdots j_n} |1\rangle) |j_3 \cdots j_n\rangle$$

etc...

$$\frac{1}{\sqrt{2^n}}(|0\rangle + e^{2\pi i 0.j_1 \cdots j_n} |1\rangle)(|0\rangle + e^{2\pi i 0.j_2 \cdots j_n} |1\rangle) \cdots (|0\rangle + e^{2\pi i 0.j_n} |1\rangle)$$

finalement on inverse l'ordre des qubits.

C-U



Estimation de phase

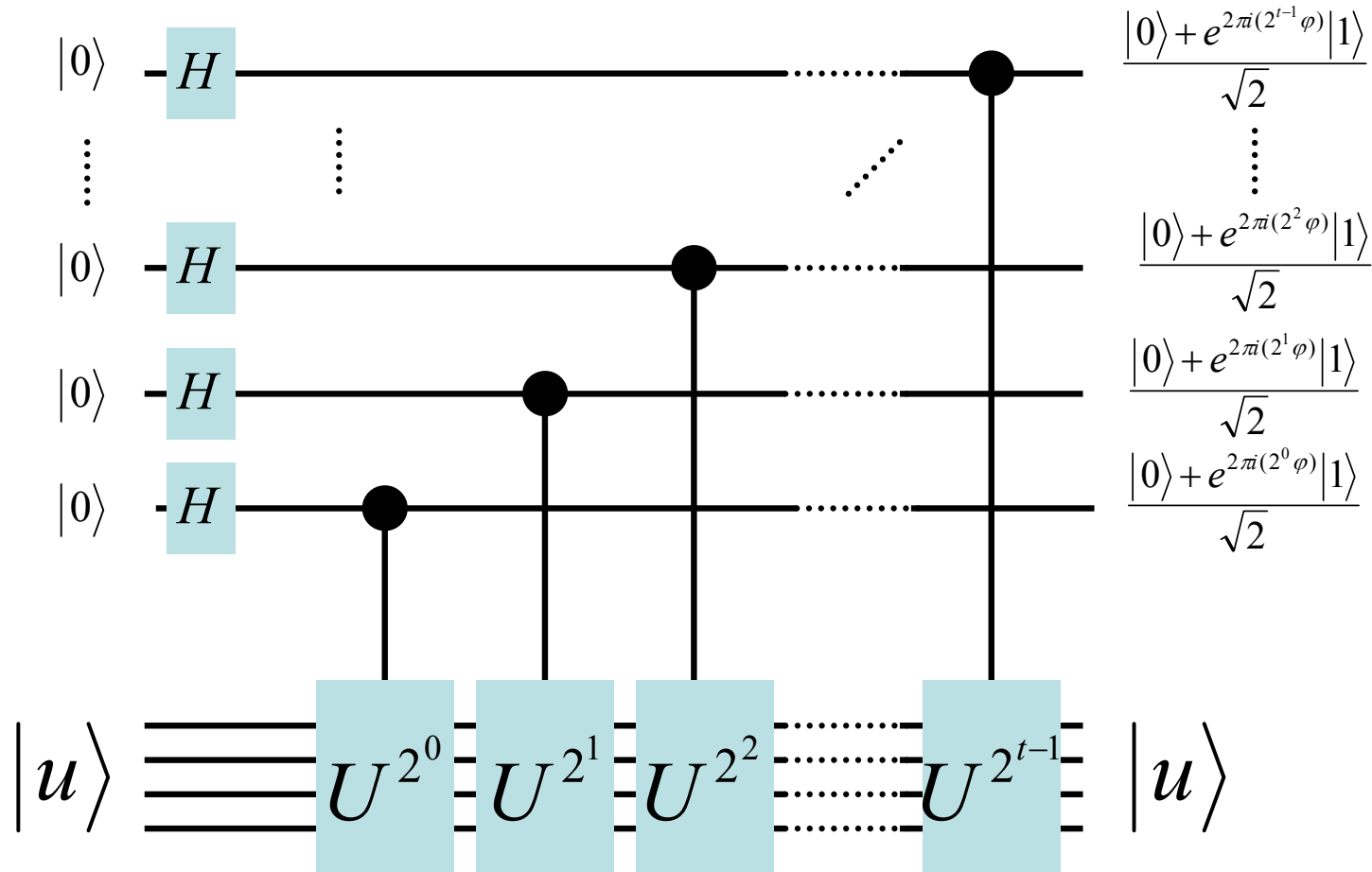
Supposons qu'un opérateur U a comme valeur propre $|u\rangle$ avec valeur propre $e^{2\pi i\varphi}$.

$$U |u\rangle = e^{2\pi i\varphi} |u\rangle$$

Supposons que l'on connaisse $|u\rangle$ et que nous ayons à notre disposition $C-U^{2^t}$ pour tout t suffisamment grand.

Peux-t-on en déduire la phase φ ?

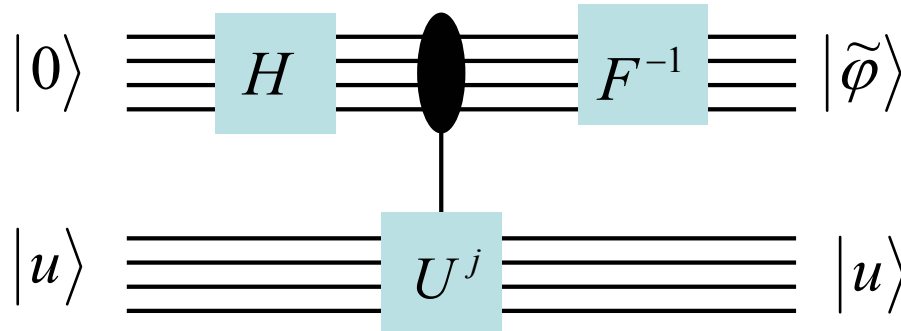
Estimation de phase



Estimation de phase

$$\begin{aligned}
 C-U(H \otimes I) |0\rangle |u\rangle &= \frac{1}{\sqrt{2^n}} (|0\rangle + e^{2\pi i(2^{t-1}\varphi)} |1\rangle) (|0\rangle + e^{2\pi i(2^{t-2}\varphi)} |1\rangle) \dots (|0\rangle + e^{2\pi i(2^0\varphi)} |1\rangle) \\
 &= \sum_{k=0}^{2^t-1} e^{2\pi i k \varphi} |k\rangle \\
 &\simeq \frac{1}{\sqrt{2^n}} (|0\rangle + e^{2\pi i 0.\varphi_t} |1\rangle) (|0\rangle + e^{2\pi i 0.\varphi_{t-1}\varphi_t}) \dots (|0\rangle + e^{2\pi i 0.\varphi_0 \dots \varphi_t} |1\rangle)
 \end{aligned}$$

Estimation de phase



Si le premier registre est formé de t qubits et $|\varphi\rangle$ s'exprime exactement avec t qubits alors $\tilde{\varphi} = \varphi$. Qu'arrive-t-il sinon. Il est plausible que $\tilde{\varphi}$ sera une bonne approximation de φ .

Théorème:

La probabilité que les $t - \lceil \log(2 + \frac{1}{2\epsilon}) \rceil$ premiers bits de $\tilde{\varphi}$ soient correctes est de $1 - \epsilon$. En particulier avec probabilité $3/4$ au moins $t - 2$ bits sont correctes.

Qualité de l'approximation

La taille du premier registre est t . Soit $b \in \{0, \dots, 2^t - 1\}$ tel que $b/2^t = 0.b_1 \dots b_t$ est égale au premier t bit de φ .

Soit $\delta = \varphi - b/2^t$ alors $0 \leq \delta \leq 2^{-t}$.

Avant $F_t^\dagger$ le premier registre est dans l'état

$$\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{2\pi i k \varphi} |k\rangle$$

après $F_t^\dagger$ l'état devien

$$\begin{aligned} & \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{2\pi i k \varphi} \left(\frac{1}{\sqrt{2^t}} \sum_{l=0}^{2^t-1} e^{-2\pi i k l / 2^t} |l\rangle \right) \\ &= \frac{1}{2^t} \sum_{k,l=0}^{2^t-1} e^{-2\pi i k l / 2^t} e^{2\pi i k \varphi} |l\rangle \\ &= \frac{1}{2^t} \sum_{k,l=0}^{2^t-1} \left(e^{2\pi i (\varphi - l/2^t)} \right)^k |l\rangle \end{aligned}$$

Qualité de l'approximation

Posons α_l l'amplitude de $|(b+l) \bmod 2^t\rangle$ alors

$$\begin{aligned}\alpha_l &= \sum_k^{2^t-1} \left(e^{2\pi i(\varphi-(b+l)/2^t)} \right)^k \\ &= \frac{1}{2^t} \left(\frac{1 - e^{2\pi i(\varphi-(b+l))}}{1 - e^{2\pi i(\varphi-(b+l)/2^t)}} \right) \\ &= \frac{1}{2^t} \left(\frac{1 - e^{2\pi i(2^t\delta-l)}}{1 - e^{2\pi i(\delta-l/2^t)}} \right)\end{aligned}$$

Pour tout θ , $|1 - e^{i\theta}| \leq 2$ et donc

$$|\alpha_l| \leq \frac{2}{2^t |1 - e^{2\pi i(\delta-l/2^t)}|}$$

Si $-\pi \leq \theta \leq \pi$ alors $2|\theta|/\pi \leq |1 - e^{i\theta}|$. Comme $-2^{t-1} \leq l \leq 2^{t-1}$ alors $-\pi \leq 2\pi i(\delta - l/2^t) \leq \pi$ et

$$|\alpha_l| \leq \frac{2}{2^t 4(\delta - l/2^t)} = \frac{1}{2(2^t\delta - l)}$$

Qualité de l'approximation

Soit m l'état observé et e l'erreur que nous sommes prêts à tolérer. On s'intéresse à la probabilité que $|m - b| > e$. Cette probabilité est donnée par

$$\begin{aligned}
 p(|m - b| > e) &= \sum_{l=-2^t+1}^{-(e+1)} |\alpha_l|^2 + \sum_{l=e+1}^{2^{t-1}} |\alpha_l|^2 \\
 &\leq \sum_{l=-2^t+1}^{-(e+1)} \frac{1}{4(2^t\delta - l)^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{4(2^t\delta - l)^2} \\
 &\leq \frac{1}{4} \left(\sum_{l=-2^t+1}^{-(e+1)} \frac{1}{(l - 2^t\delta)^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{(l - 2^t\delta)^2} \right) \\
 &\leq \frac{1}{4} \left(\sum_{l=-2^t+1}^{-(e+1)} \frac{1}{(l)^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{(l - 1)^2} \right) \\
 &\leq \frac{1}{2} \sum_{l=e}^{2^{t-1}-1} \frac{1}{l^2} \\
 &\leq \frac{1}{2} \int_{e-1}^{2^{t-1}-1} \frac{1}{l^2} dl \\
 &= \frac{1}{2(e-1)}
 \end{aligned}$$

Qualité de l'approximation

$$p(|m - b| > e) \leq \frac{1}{2(e - 1)}$$

Si $\epsilon = \frac{1}{2(e-1)}$ alors $e = \frac{1}{2\epsilon} + 1$.

Le nombre de bit possiblement en erreur est donné par $\log(e + 1) = \log(\frac{1}{2\epsilon} + 2)$.

Un utilisant un registre de t qubit, la probabilité que les $t - \lceil \log(2 + \frac{1}{2\epsilon}) \rceil$ premier bit de $\tilde{\varphi}$ soit corecte est de $1 - \epsilon$. En particulier avec probabilité $3/4$ au moins $t - 2$ bit sont corecte.