Algo de Shor pour la factorisation des entiers. N

plus généralement il s'agit de rechercher la période de fcts arithmétiques.

1) Circuit de la QFT.

2) Circuit pour la fct $f : x \mapsto a^x \bmod N$

avec $\mathrm{PGCD}(a, N) = 1$

(fct utilisée pour la factorisation).

3) Résumé la vue d'ensemble de l'algorithme et discuter sa <u>complexité totale</u>

#

<u>Entier</u> $\mathbb{Z}/M\mathbb{Z}$ $\bmod M = \bmod 2^m$ avec $M \gg N^2$

$$x = 2^{m-1} x_{m-1} + \dots + 2x_1 + x_0 \ ; \ x_i \in \{0, 1\}$$

$$|x\rangle = |x_{m-1}\rangle \otimes \dots \otimes |x_1\rangle \otimes |x_0\rangle$$

avec $|x_i\rangle \in \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \ ; \ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

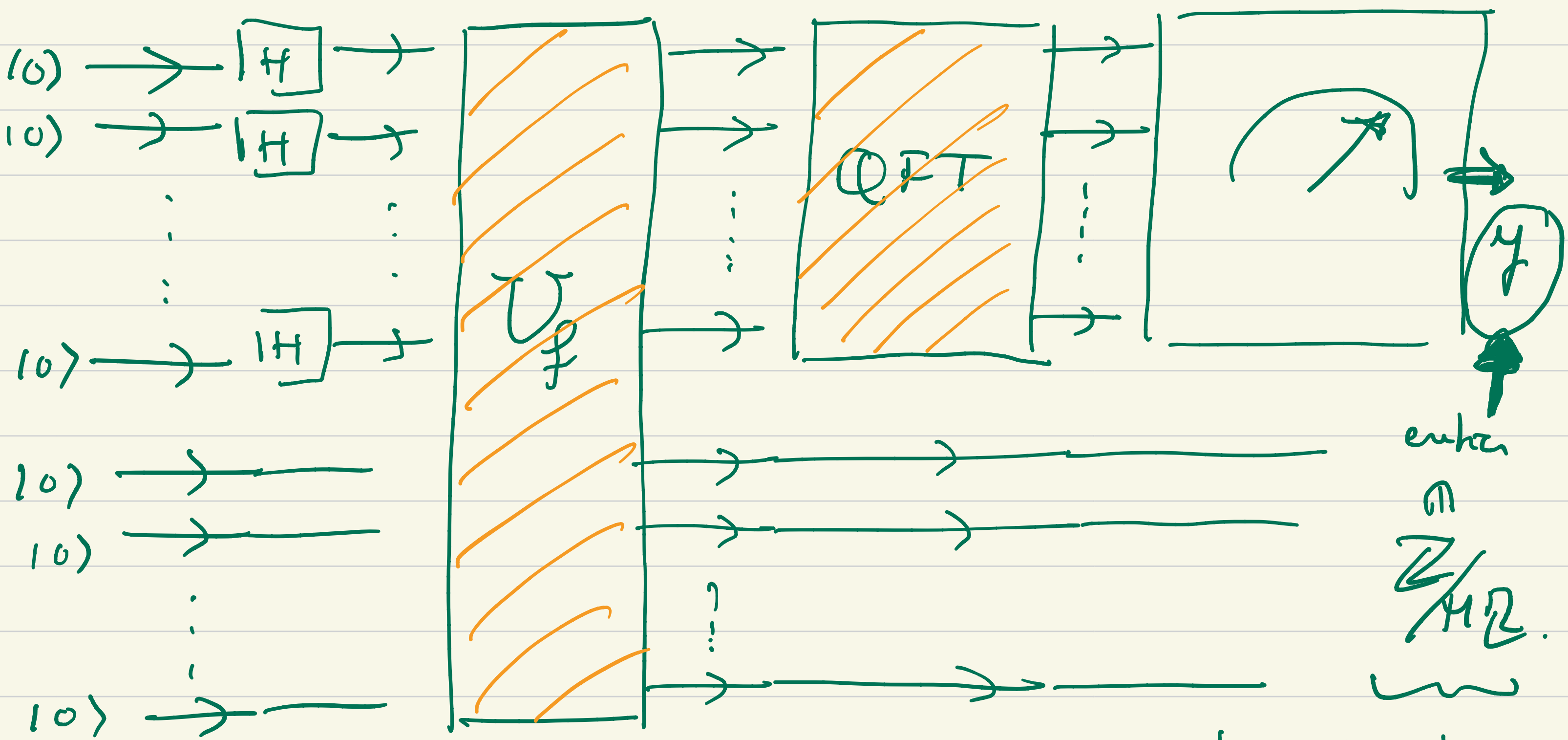
Ket vivent dans $(\mathbb{C}^2)^{\otimes m}$.

m̂ chose pour $f(x)$ mod M. & on ajoute

encore m bits pour stocker les résultats de $f(x)$.

Hilbert Total : $(\mathbb{C}^2)^{\otimes m} \otimes (\mathbb{C}^2)^{\otimes m}$.

Circuit structure suivante :



$2m$ bits quantiques au total

entier $y \in \mathbb{Z}/M\mathbb{Z}$.

à partir de $\frac{y}{M}$ en calculant les convergents (Euclide) on en déduit la période de f.

Aujourd'hui

circuit de QFT

circuit de U_f

pour $f(x) = a^x \bmod N$

1) Circuit de QFT.

$x \in \{0 \dots M-1\}$

$= \mathbb{Z}/M\mathbb{Z}$.

$$QFT\,|x\rangle \equiv \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{xy}{M}} \, |y\rangle$$

$|x\rangle = |x_{m-1}\rangle \otimes \cdots \otimes |x_0\rangle$

$|y\rangle = |y_{m-1}\rangle \otimes \cdots \otimes |y_0\rangle$

Nous prendrons $M = 2^m$ pour des raisons de simplicité.

$\frac{\mathbb{Z}}{2\mathbb{Z}} = \{0, 1\} \bmod 2$

- **Tout d'abord pour $M = 2$ $m = 1$.** $x_0 \in \{0,1\}$

$$(QFT)_{M=2} \, |x_0\rangle = \frac{1}{\sqrt{2}} \left\{ |0\rangle + \underbrace{e^{\frac{2\pi i x_0}{2}}} \, |1\rangle \right\}$$

$e^{i\pi x_0} = (-1)^{x_0}$.

$$|x_0\rangle \; — \boxed{H} — \; \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_0} |1\rangle\right).$$

ici $QFT = H$.

Maintenant $M=4$. $\quad n=2 \quad x = 2x_1 + x_0$.

$$\frac{\mathbb{Z}}{4\mathbb{Z}} = \{0, 1, 2, 3\} \mod 4.$$

$x_0, x_1 \in \{0,1\}$.

$$(QFT)_{M=4} |x\rangle = \frac{1}{\sqrt{4}} \Big\{ \underbrace{|0\rangle}_{|00\rangle} + e^{\frac{2\pi i x \cdot 1}{4}} \underbrace{|1\rangle}_{|01\rangle} + e^{\frac{2\pi i x \cdot 2}{4}} \underbrace{|2\rangle}_{|10\rangle} + e^{\frac{2\pi i x \cdot 3}{4}} \underbrace{|3\rangle}_{|11\rangle} \Big\}$$

$e^{\frac{i\pi x}{2}}$ $\quad e^{i\pi x}$ $\quad e^{\frac{3\pi i}{2}}$

$$= \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\pi x} |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + e^{\frac{i\pi}{2} x} |1\rangle \right)$$

$$e^{i\pi x} = \underbrace{e^{2\pi i x_1}}_{1} \underbrace{e^{i\pi x_0}}_{(-1)^{x_0}} = (-1)^{x_0} \quad \checkmark \qquad e^{i\pi} = -1$$

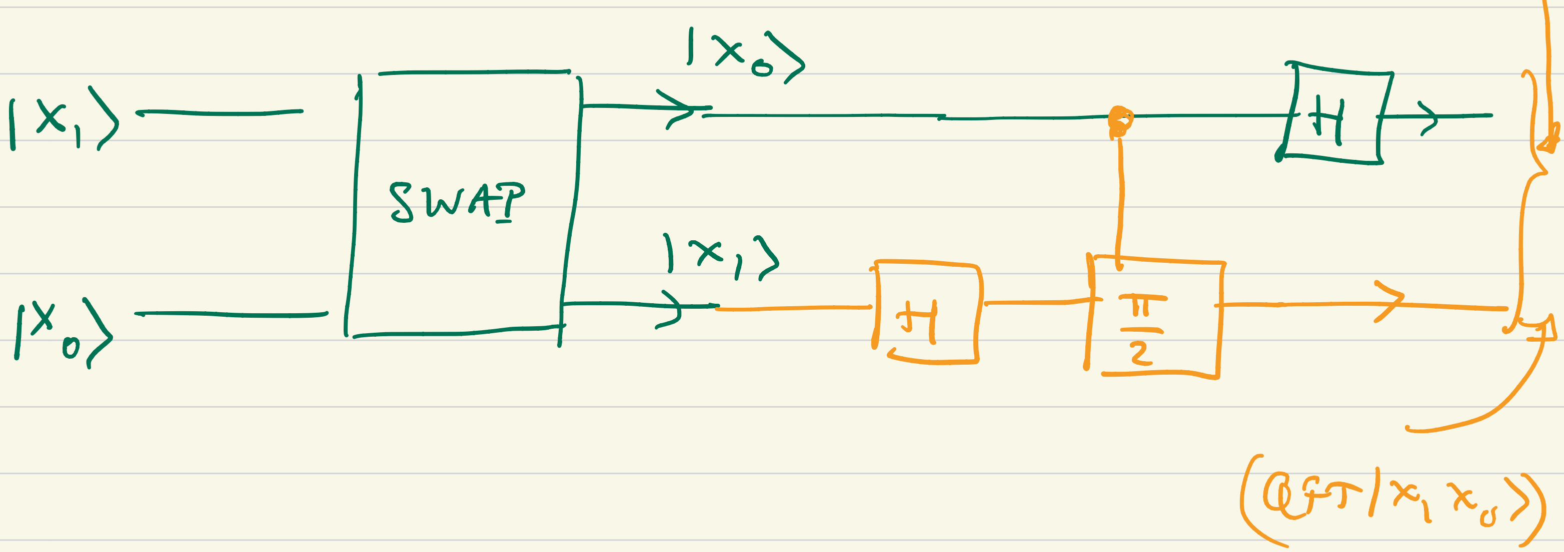
$$e^{i\frac{\pi}{2}x} = e^{\pi i x_1} e^{i\frac{\pi}{2}x_0} = (-1)^{x_1} e^{i\frac{\pi}{2}x_0}$$

$$\Rightarrow \boxed{(QFT)_{M=4} |x\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{x_0} \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{x_1} e^{\frac{i\pi}{2}x_0} |1\rangle \right)}$$

À Nouveau : $\boxed{X = 2x_1 + x_0}$

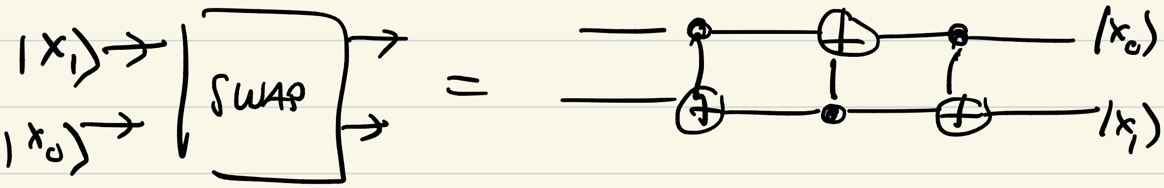
$$(QFT)_{M=4}\, \underbrace{|x_1\, x_0\rangle}_{\mathbb{C}^2 \otimes \mathbb{C}^2} = \underbrace{\boxed{\frac{|0\rangle + (-1)^{x_0}|1\rangle}{\sqrt{2}}}}_{\mathbb{C}^2} \otimes \underbrace{\boxed{\frac{|0\rangle + (-1)^{x_1} e^{i\frac{\pi}{2}x_0}|1\rangle}{\sqrt{2}}}}_{\mathbb{C}^2}.$$

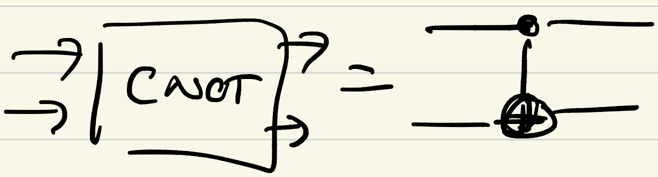
<u>Un circuit</u> :



Si on comprend cet exemple on comprend le reste.

<u>Remarque</u> :





XOR contrôlé.

Cas général :

Lemme : la formule de factorisation générale.

$x \in \{0, \dots, M-1\}$ $\qquad M = 2^m \qquad$ m qubits

$$QFT|x\rangle = \prod_{l=1}^{m} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{\pi x}{2^{l-1}}}|1\rangle\right).$$

Vérifier que l'on retrouve formule précédente si

$M = 2$, $M = 4$ ...

Démonstration du lemme :

$$QFT|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{xy}{2^m}} |y\rangle$$

$\frac{1}{2^{m/2}}$

$$y = 2^{m-1} y_{m-1} + \dots + 2y_1 + y_0.$$

$$= 2y' + y_0 \qquad y_0 = 0, 1.$$

avec $y' = 2^{m-2} y_{m-1} + \dots + 2y_2 + y_1.$

$$|y\rangle = |y'\rangle \otimes |y_0\rangle \quad y_0 = 0, 1.$$

$$QFT|x\rangle = \frac{1}{2^{m/2}} \sum_{y'=0}^{2^{m-1}-1} e^{\frac{2\pi i x (2y')}{2^{m-1}}} |y'\rangle \otimes |0\rangle \quad (y \text{ pairs}) \; = 2y'$$

$$+ \frac{1}{2^{m/2}} \sum_{y'=0}^{2^{m-1}-1} e^{\frac{2\pi i x (2y'+1)}{2^{m-1}}} \otimes |1\rangle \quad (y \text{ impairs}) \; = 2y'+1.$$

$$= \underbrace{\frac{1}{2^{\frac{m-1}{2}}} \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{x y'}{2^{m-1}}} |y'\rangle}_{\text{on itère encore une fois, puis encore et encore avec ici } m \to m-1 \,//\, y' = 2y'' + y_1 \to \text{pairs} \to \text{impairs}} \otimes \left(|0\rangle + e^{\frac{i\pi x}{2^{m-1}}} |1\rangle \right)$$

$$\underbrace{y_1}_{0,\,1.}$$

$\Rightarrow$ On obtient le résultat du lemme

$\blacksquare$