Algorithme de Shor. Continuation.

Rappel :

- Un alg pour trouver période de

$$f : \frac{\mathbb{Z}}{M\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{M\mathbb{Z}}.$$

r plus petit entier t.q et $r \neq 0$.
$$\begin{cases} f(x+r) = f(x). \\ \forall x \in \frac{\mathbb{Z}}{M\mathbb{Z}}. \end{cases}$$

- La fct de choix pour factoriser un entier N $\quad (M \approx N^2)$

$$f(x) = a^x \mod N.$$

avec $\quad \text{pgcd}(a, N) = 1.$

|| Période satisfait $\quad a^r = 1 \mod N.$
|| ici $\quad r = \text{Ord}_N(a).$

- Circuit Quantique manipule des qubits.

$x \in \frac{\mathbb{Z}}{M\mathbb{Z}}$: $x = x_{m-1} 2^{m-1} + \cdots + 2x_1 + x_0$

$M = 2^m$. $x_i \in \{0, 1\}$.

Notre choix !

entrées. Ket : $|x\rangle = \underbrace{|x_{m-1}\rangle \otimes \cdots \otimes |x_1\rangle \otimes |x_0\rangle}$

pr tensoriel forme une base de $(\mathbb{C}^2)^{\otimes m}$

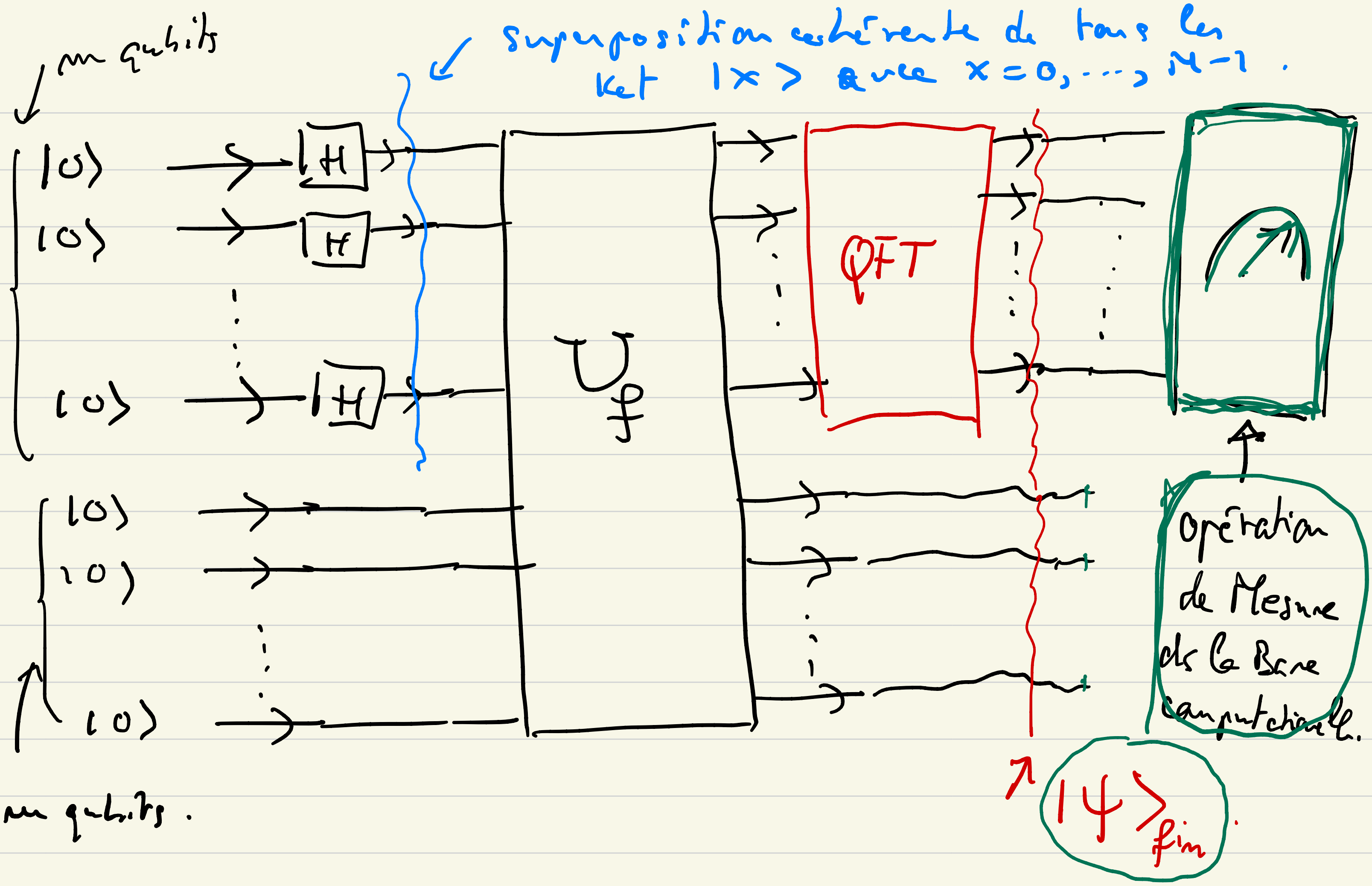
$|x_i\rangle \in \{|0\rangle, |1\rangle\}$.

qubit auxiliaire pour $|f(x)\rangle \in (\mathbb{C}^2)^{\otimes m}$

ici $f(x) \in \frac{\mathbb{Z}}{M\mathbb{Z}} \to m$ bits classiques pour repr $f(x)$.

et donc on va prendre m qubits pour $|f(x)\rangle$.

(prod tensoriel obtenu par déc binaire de $f(x)$).



par déf : $U_f \, |x\rangle \otimes \underbrace{|0\rangle}_{\substack{|0\rangle\otimes\cdots\otimes|0\rangle \\ m \text{ fois} \\ m \text{ qubits}}} = |x\rangle \otimes |f(x)\rangle$

Le circuit détaillé dépend de la fct f.
On verra cela la prochaine fois pour $f(x) = a^x \bmod N$

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

Le circuit détaillé de QFT ⟶ prochaine fois.

Plan :

0) Ecrire à nouveau l'expression de $|\psi\rangle_{fin}$ avant la mesure

1) Calculer la sortie de l'app de mesure et surtout sa probabilité.

2) Analyse de ce résultat pour retrouver la période de f c.a.d r.

ff.

0) Expression de $|\psi\rangle_{fin}$

$$|\psi\rangle_{fin} = \frac{1}{M} \sum_{x_0=0}^{r-1} \left\{ \underbrace{\sum_{y=0}^{M-1} e^{2\pi i \frac{x_0 y}{M}} \left(\sum_{j=0}^{j_{max}(x_0)} e^{2\pi i \frac{j y}{M/r}} \right) |y\rangle}_{\text{état qui vit dans l'esp d'Hilbert des } m \text{ premiers qubits du circuit}} \otimes \underbrace{|f(x_0)\rangle}_{\text{vit ds l'esp d'Hilbert des qubits auxiliaires ou de stockage}} \right\}$$

état qui vit dans l'esp d'Hilbert des m premiers qubits du circuit.

cet état est dév sur la base computationnelle

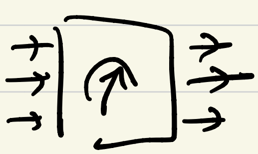
$$\left\{ |y\rangle = |y_{m-1}\rangle \otimes \cdots \otimes |y_1\rangle \otimes |y_0\rangle \right\}$$

avec $y = y_{m-1} 2^{m-1} + \cdots + 2y_1 + 2y_0$

$|y_i\rangle \in |0\rangle$ et $|0\rangle$.

vit ds l'esp d'Hilbert des qubits auxiliaires ou de stockage.

1) Mesure : À la sortie de l'app de mesure l'état est projeté sur un des états de la base comp.



$|y\rangle$ avec $y \in \{0, \ldots, M-1\}$.

Prob(y).

Calcul de Prob(y). pour $y \in \{0 \dots M-1\}$.

- L'app de mesure est décrit par un ensemble de projecteurs

$$P_y = \underbrace{|y\rangle\langle y|}_{2^m \times 2^m} \otimes \underbrace{I}_{\text{identité } 2^m \times 2^m}$$

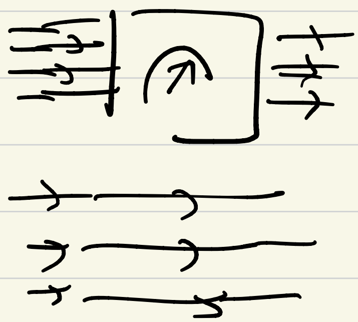
$2^m \times 2^m \longrightarrow$ matrice de projection sur le vecteur $|y\rangle \in (\mathbb{C}^2)^{\otimes m}$

identité $2^m \times 2^m$

Numérateur.

$$|y\rangle\langle y|\psi\rangle_{fin}$$

- $|\psi\rangle_{fin}$



$$\frac{P_y|\psi\rangle_{fin}}{\| P_y|\psi\rangle_{fin}\|}$$

avec y est choisit aléatoirement

$$\text{Prob}(y) = {}_{fin}\langle\psi|\underbrace{P_y|\psi\rangle_{fin}}$$

$$= \underbrace{{}_{fin}\langle\psi|y\rangle}\underbrace{\langle y|\psi\rangle_{fin}}_{\uparrow \text{ à calculer.}}$$

$$\langle y | \psi \rangle_{fin} = \langle y | \sum_{x_0=0}^{r-1} \sum_{y'=0}^{M-1} \dots \; |y'\rangle \otimes |f(x_0)\rangle .$$

$$\langle y | y' \rangle = \delta_{yy'}$$

$$\Rightarrow \langle y | \psi \rangle_{fin} = \frac{1}{M} \sum_{x_0=0}^{r-1} e^{2\pi i \frac{x_0 y'}{M}} \sum_{j=0}^{j_{max}(x_0)} e^{2\pi i \frac{j y'}{M/r}} \, \underbrace{|f(x_0)\rangle}$$

premier esp d'Hilbert $(\mathbb{C}^2)^{\otimes m}$

vit ds $(\mathbb{C}^2)^{\otimes m} \otimes \underbrace{(\mathbb{C}^2)^{\otimes m}}$.

vecteur. vit ds $\underbrace{(\mathbb{C}^2)^{\otimes m}}$

Finalement : $\langle \psi | y \rangle_{fin} \langle y | \psi \rangle_{fin} \quad = \text{Prob}(y)$.

$\#$ idem avec $\langle f(x_0)|$ et les phases complexe-conjuguée. $\bar{i} = -i$

$$\sum_{x_0'=0}^{r-1} \dots \underbrace{\langle f(x_0')|} \quad \sum_{x_0=0}^{r-1} \dots \underbrace{|f(x_0)\rangle} .$$

$$\langle f(x_0') | f(x_0) \rangle = \delta_{x_0 x_0'}$$

$$\begin{cases} 1 \text{ si } x_0 = x_0' \\ 0 \text{ si } x_0 \neq x_0' \end{cases}.$$

__Finalement :__

$$\underline{\mathrm{Prob}(y)} = \frac{1}{M^2} \sum_{x_0=0}^{r-1} \left| \sum_{j=0}^{j_{max}(x_0)} e^{2\pi i \frac{jy}{M/r}} \right|^2 . \qquad (*)$$

__Conseil :__ faire le calcul qui mène à (*) soi-même !

PAUSE

après nous allons analyser cette fct et voir que elle possède sa "masse" sur des entiers spéciaux "y" qui contiennent de l'information sur r.