Algorithme quantique de Shor

. pour rechercher la période d'une fct

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$x \longmapsto f(x).$$

promesse $f(x) = f(x+r)$.

$r \neq 0$ période.

\#

1. Alg général avec circuit vidéos 1 et 2
2. Processus de Mesure analyses vidéos 3 et 4
3. Détailler encore certains pts vidéos 5 et 6.

\#.

- Application phare : Factorisation

d'un entier $N = p \cdot q$

(p, q deux nbs premiers impairs. et $p \neq q$).

Grâce Alg de Rabin et Miller qui ramène fact $\rightarrow$ période

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

et $a \in \{2, \dots, N-1\}$.

avec $PGCD(a, N) = 1$.

"G" et H serait s-groupe des multiples de r

$f : \underline{\underline{\mathbb{Z}}} \to \mathbb{Z}$. périodique

$$f(x) = f(x+r) \quad (*).$$

r = le plus petit entier possible $r \neq 0$

inconnue.

Tronqué $\mathbb{Z}$ sur $\frac{\mathbb{Z}}{M\mathbb{Z}} = \{0, 1, \ldots, M-1\}$

entiers modulo M

avec M "grand".

$$M \gg r.$$

Application à la $\underline{\underline{\text{facto}}}$ $f(x) = a^x \bmod N$.

et r satisfait $a^r = 1 \; \underline{\bmod N}$ ← Nb à factoriser

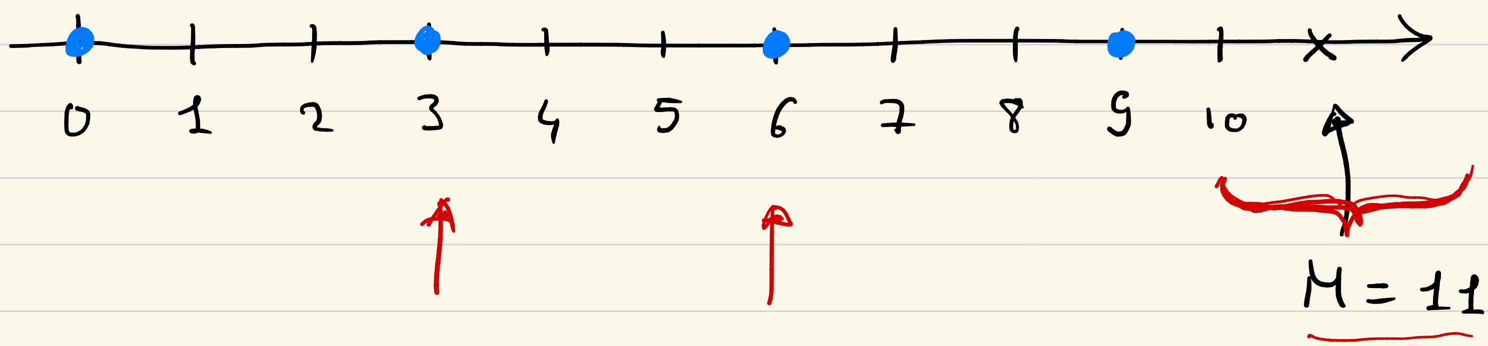
certainement $r < N$ et donc on

prendre $\underline{M \gg N}$. Nous verrons que en pratique

$$\underline{M = N^2}.$$

$\{0, 1, 2, \dots M-1\}$. $\qquad \dfrac{\mathbb{Z}}{M\mathbb{Z}}$

H



Pour fixer les idées $\underbrace{M = 11}_{\text{Notre choix.}}$ et $\underbrace{r = 3}_{\text{“inconnu”}}$.

$M \gg r$.

Rappelez vous du cadre de l'Alg de Simon.

$G = \dfrac{\mathbb{Z}}{M\mathbb{Z}}$. et $H \subset G$ $\quad H$ s-groupe caché.

Ici si $H = \{$ens des multiples de r qui sont dans $G = \dfrac{\mathbb{Z}}{M\mathbb{Z}}\}$ en général H n'est pas un sous-groupe.

$3 + 6 \mod 11 = 9 \in H$

$\boxed{\underbrace{9 + 3}_{12} \mod 11 = 1 \notin H}$.

H serait un vrai s-groupe de $\dfrac{\mathbb{Z}}{M\mathbb{Z}}$ ssi r Div M.

Mais r est inconnu et donc on ne peut pas choisir M t.q r Div M.

• Tout entier $x \in \dfrac{\mathbb{Z}}{M\mathbb{Z}}$ peut être représenté

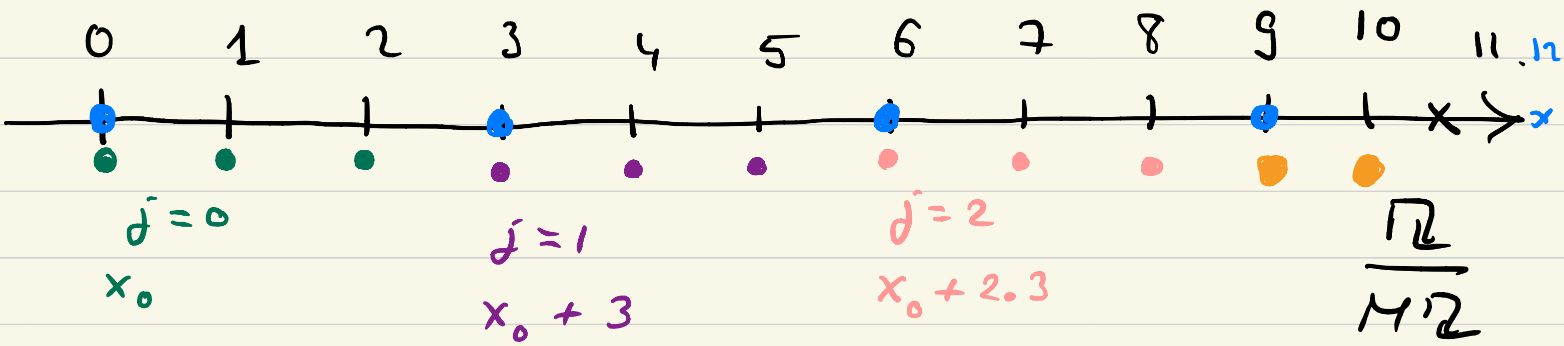
$$x = x_0 + j\, r$$

$x_0 \in \{0, 1, 2, \dots, r-1\}$. dans la première période.

$$0 \leq j \leq \underbrace{A(x_0) - 1}_{j_{max}} .$$

$x_0 + 3.3$

$j_{max} = 3$.



$\dfrac{\mathbb{Z}}{M\mathbb{Z}}$

$M = 11$

$r = 3$

• Pour élaborer l'alg quant il faut repr

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

et $\underbrace{f(x)}_{\in \{0, \dots, M-1\}}$ par des qu bits.

$$\begin{cases} f(x) = a^x \mod N. \\ M = N^2. \end{cases}$$

certainement on pourra représenter $f(x)$ avec les cubits dans $\{0, \dots, M-1\}$
Ψ
$f(x)$.

Aussi choix de $M \to$ Notre choix est plus facile $M = 2^m$ puissance de 2.

$x \in \{0 \dots M-1\}$ $f(x) \in \{0 \dots M-1\}$ on a besoin de m bits.

$$\begin{cases} X = x_0 + 2 . x_1 + 2^2 x_2 + \dots + 2^{m-1} x_{m-1}. \\ x = [x_{m-1} \, x_{m-2} \dots x_1 \, x_0] \text{ dév binaire de } X. \end{cases}$$

- Naturel de coder $x \in \frac{\mathbb{Z}}{M\mathbb{Z}}$ dans un ensemble de m qubits.

$$x \mapsto |x_0\rangle \otimes |x_1\rangle \otimes \cdots \otimes |x_{m-1}\rangle \in (\mathbb{C}^2)^{\otimes m}$$

avec $|x_i\rangle \in \{ \underbrace{|0\rangle , |1\rangle}_{\text{base computationnelle de } \mathbb{C}^2} \}$.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ et } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Notation :

$$\underbrace{|x_0\rangle \otimes \cdots \otimes |x_{m-1}\rangle}_{\text{pr tensoriel des qubits élémentaire dans les états } |0\rangle,\ |1\rangle.} = |\overbrace{x_0 x_1 \cdots x_{m-1}}^{\text{dev binaire de l'entier } x.}\rangle$$

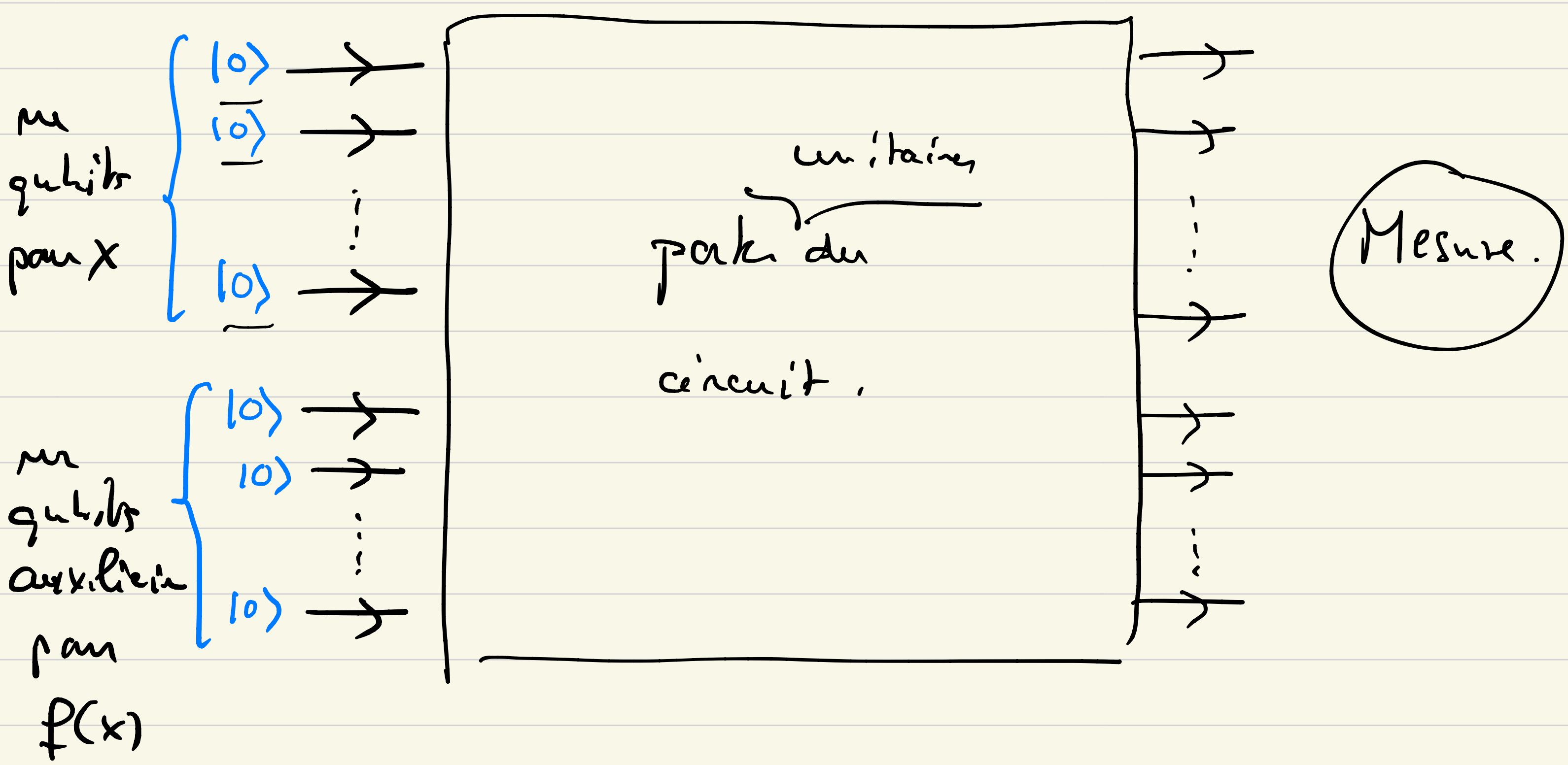
$$= |x\rangle$$

↑ l'entier $x \in \{0 \ldots M-1\}$

- Pour $f(x) \in \{0 \ldots M-1\} \mapsto |\underline{f(x)}\rangle$.
(comme pour x dév binaire etc...).

Espace de Hilbert du circuit quantique.

$$\underbrace{(\mathbb{C}^2)^{\otimes m}}_{\text{entrée}} \otimes \underbrace{(\mathbb{C}^2)^{\otimes m}}_{\text{sortie}} \qquad \text{avec } M = 2^m.$$



Etat initial : $\underbrace{|0\rangle^{\otimes m}}_{\underbrace{|00\ldots0\rangle}_{m \text{ fois}}} \otimes \underbrace{|0\rangle^{\otimes m}}_{\text{idem.}}$

son dév binaire → $|0\rangle.$

entier $0 \in \{0 \ldots M-1\}$ → $|0\rangle$

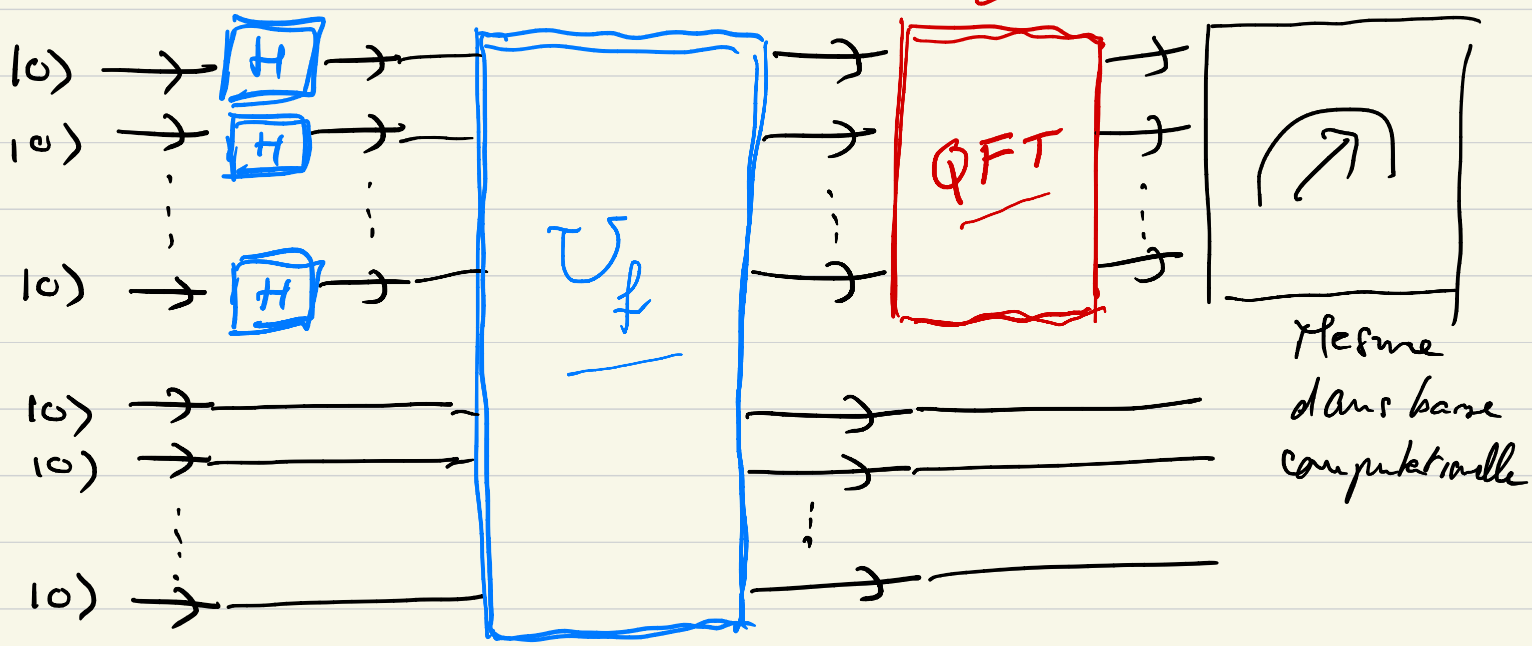
Etat initial du circuit :

$$|0\rangle \otimes |0\rangle.$$

schéma général

Le circuit de l'alg de Shor :

analyse de Fourier du signal sortant



- Créer de superposition de toutes les entrées possibles grâce aux portes de Hadamard H

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

- U_f "sous-circuit" (matrice unitaire) qui "calcule" f sur toutes les entrées classiques possibles.

$$U_f\, |x\rangle \otimes |0\rangle = |x\rangle \otimes |f(x)\rangle$$

|| Détail interne du sous-circuit dépend de f.
Nous verrons ceci ds le 3ème cours pour $f(x) = a^x \bmod N$

- QFT sous-circuit (mat unitaire) → Transf de Fourier Quantique

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

- Par définition : $x \in \{0 \cdots M-1\}$.

$$(QFT)|x\rangle \overset{\text{déf}}{=} \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{\frac{2\pi i}{M} x y} |y\rangle$$

(QFT) : matrice unitaire $2^m \times 2^m$

$|x\rangle \in (\mathbb{C}^2)^{\otimes m}$, $\dim = 2^m$

$M = 2^m$.

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

Par linéarité on a si $|\psi\rangle = \sum_{x=0}^{M-1} c_x |x\rangle$

$QFT|\psi\rangle = \sum_{x=0}^{M-1} c_x \, QFT|x\rangle$. Je connais l'action de QFT sur tout $|\psi\rangle \in (\mathbb{C}^2)^{\otimes m}$.

Plus explicitement dans le langage des qubits :

$$QFT(|x_{m-1}\rangle \otimes \cdots \otimes |x_0\rangle) \overset{\text{def}}{=} \frac{1}{2^{m/2}} \cdot \sum_{y_0 \cdots y_{m-1} \in \{0,1\}^m} \text{---}$$

$$\text{---} : e^{\frac{2\pi i}{M} (\text{déc bin } x)(\text{déc bin } y)} |y_{m-1}\rangle \otimes \cdots \otimes |y_0\rangle$$

- Nous avons vu que QFT peut être représentée par un circuit avec $O(n^2)$ portes à 1 et 2 qubits. [complexité pol].

- Nous avons vu que pour $f(x) = a^x \bmod N$.

U_f aussi avec circuit de complexité pol $O(n^2)$.

Finalement compl totale du circuit (en particulier sa profondeur) est $O(n^2)$ $\rightarrow$ $(\log_2 M)^2 \rightarrow (\log_2 N)^2$ ordre de grandeur.

PAUSE / prochaine vidéo on calcule les étapes du circuit et sa sortie juste avant la mesure.