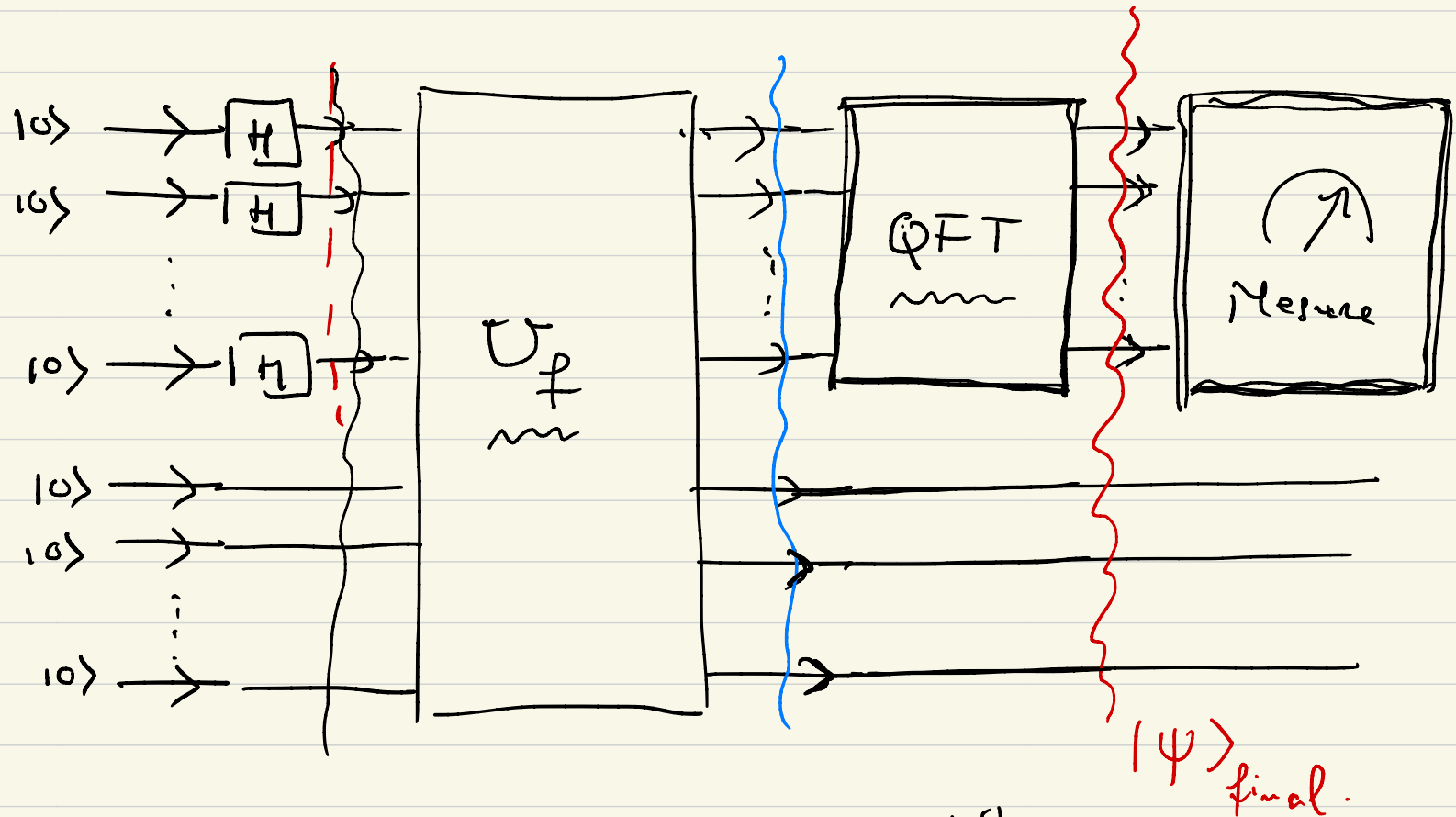



Suite de l'analyse du circuit de l'algorithme :



- $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ pour 1 qubit.

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

- $$U_f \left(\underbrace{|x\rangle}_{|x_{m-1}\rangle \otimes \dots \otimes |x_0\rangle} \otimes \underbrace{|0\rangle}_{|0\rangle \otimes \dots \otimes |0\rangle} \right) = |x\rangle \otimes \underbrace{|f(x)\rangle}_{\text{produit tensoriel des qubits élémentaires du dev binaire de } f(x)}$$

- $$\underbrace{QFT}_{2^m \times 2^m} |x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{\frac{2\pi i}{M} x y} \underbrace{|y\rangle}_{|y_{m-1}\rangle \otimes \dots \otimes |y_0\rangle}$$

$$\underbrace{10\rangle}_{m \text{ qubits}} \otimes \underbrace{10\rangle}_{m \text{ qubits}}$$

• état initial : $\underbrace{10\rangle \otimes \dots \otimes 10\rangle}_{m \text{ qubits}} \otimes \underbrace{10\rangle \otimes \dots \otimes 10\rangle}_{m \text{ qubits}}$

• après la 1^{ère} série de portes H :

m qubits.

$$\underbrace{H|0\rangle \otimes \dots \otimes H|0\rangle}_{m \text{ qubits}} \otimes \underbrace{10\rangle \otimes \dots \otimes 10\rangle}_{m \text{ qubits}}$$

$$= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes 10\rangle \otimes \dots \otimes 10\rangle$$

=

$$\frac{1}{2^{m/2}} \sum_{x_0 \dots x_{m-1}} \underbrace{|x_{m-1}\rangle \otimes |x_{m-2}\rangle \otimes \dots \otimes |x_0\rangle}_{M-1} \otimes \underbrace{10\rangle \otimes \dots \otimes 10\rangle}_{m \text{ qubits}}$$

$$= \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |0\rangle$$

$$(M=2^m)$$

• Nous appliquons U_f ce qui donne

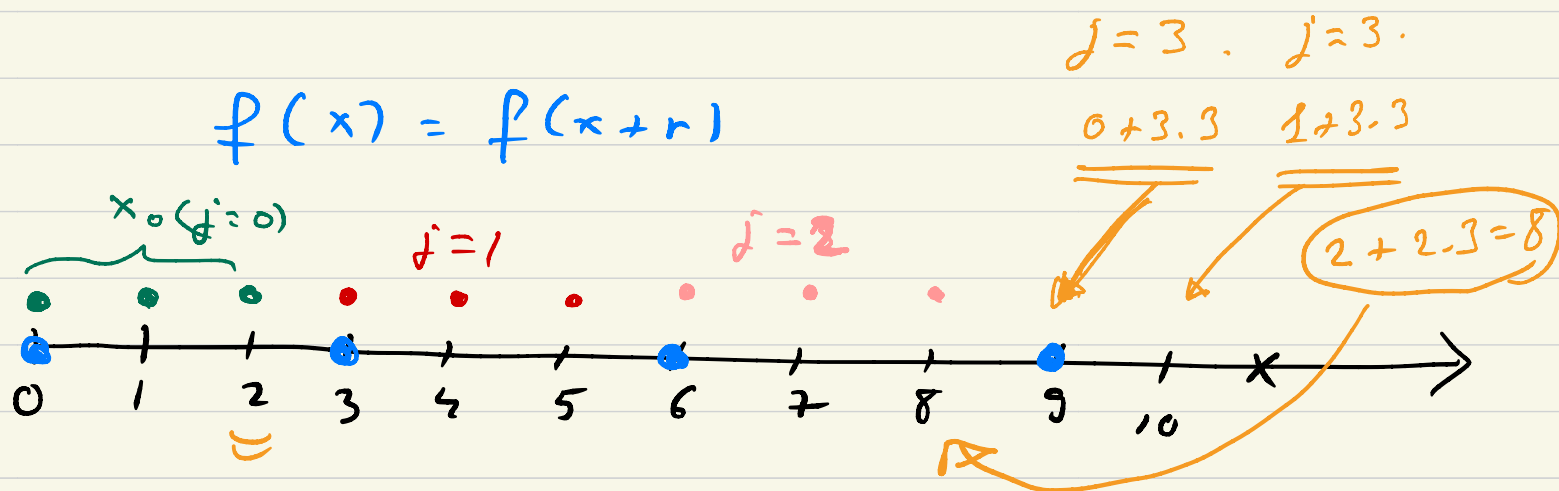
$$U_f \left(\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |0\rangle \right) = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} \underbrace{U_f(|x\rangle \otimes |0\rangle)}_{|x\rangle \otimes |f(x)\rangle}$$

état du circuit quantique après l'opération U_f :

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |f(x)\rangle. \quad (*)$$

maintenant utiliser la structure périodique de f .

(analogue à l'alg de Simon).



$$\begin{cases} M=11 \\ r=3. \end{cases}$$

$$(*) \quad x = x_0 + j \cdot r$$

$$\{0, 1, 2, \dots, r-1\}$$

$$\begin{cases} j_{\max}(x_0=0) = 3 \\ j_{\max}(x_0=1) = 3 \\ j_{\max}(x_0=2) = 2 \end{cases}$$

$$0 \leq j \leq j_{\max}(x_0)$$

le max possible de j dépend de x_0 .

Notation traditionnelle

$$j_{\max}(x_0) = A(x_0) - 1.$$

Avec cette représentation :

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |f(x)\rangle = \frac{1}{\sqrt{M}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{\overbrace{A(x_0)-1}^{j_{\max}(x_0)}} |x_0 + jr\rangle \otimes \underbrace{|f(x_0 + jr)\rangle}_{|f(x_0)\rangle}$$

Donc l'état juste après U_f (avant QFT) :

$$|\psi\rangle = \frac{1}{\sqrt{M}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{A(x_0)-1} |x_0 + jr\rangle \otimes |f(x_0)\rangle.$$

Il reste à appliquer QFT sur $|\psi\rangle$.

$$\underbrace{|\psi\rangle}_{\text{final}}$$

$$\text{QFT}|\psi\rangle = \frac{1}{\sqrt{M}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{A(x_0)-1} \left(\text{QFT} |x_0 + jr\rangle \right) \otimes \underbrace{|f(x_j)\rangle}$$

par definition

$$\text{QFT} |x_0 + jr\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{\frac{2\pi i}{M} (x_0 + jr)y} |y\rangle$$

$\Rightarrow$

$$|\psi\rangle_{\text{final}} = \frac{1}{\sqrt{M}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{A(x_0)-1} \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{\frac{2\pi i}{M} (x_0 + jr)y}$$

$$|\psi\rangle_{\text{final}} = \underbrace{\left[\frac{1}{M} \sum_{x_0=0}^{r-1} \left\{ \sum_{y=0}^{M-1} \left[\sum_{j=0}^{A(x_0)-1} e^{\frac{2\pi i}{M} (x_0 + jr)y} \right] |y\rangle \right\} \right]}_{|y\rangle \otimes |f(x_0)\rangle} \otimes |f(x_0)\rangle$$

• Expression finale de l'état juste avant la Mesure.

• la prochaine fois le processus de Mesure / Cette Mesure va donner un état $|y\rangle$ aléatoire / découvrir r dans cet ensemble