Chapitre 6

Algorithme de Shor

Comme nous l'avons expliqué dans le chapitre précédent, on peut ramener la factorisation d'un entier N à la recherche de l'ordre d'un nombre a pris au hasard dans $\{2, 3, ..., N-1\}$. L'ordre $Ord_n(a)$ est le plus petit entier r tel que

$$a^r = 1 \, mod \, N.$$

En d'autres termes, nous cherchons la période de la fonction arithmétique

$$\begin{aligned} f_{a,N} : \mathbb{Z} &\to \mathbb{Z} \\ x &\to f_{a,N}(x) = a^x \ \ mod \, N. \end{aligned}$$

Cette période (ou l'ordre) est le plus petit entier r t.q.

$$f_{a,N}(x) = f_{a,N}(x + r), \qquad \forall x \in \mathbb{Z}.$$

Nous commençons donc par étudier un algorithme général de "recherche de la période d'une fonction arithmétique".

6.1 Recherche de la période d'une fonction arithmétique

Soit $f : \mathbb{Z} \to \mathbb{Z}$ de période inconnue

$$f(x) = f(x + r), \qquad \forall x \in \mathbb{Z}.$$

Comme nous serons obligés de travailler avec un nombre fini de bits, nous allons tronquer $\mathbb{Z}$ à $\frac{\mathbb{Z}}{M\mathbb{Z}} = \{0, 1, 2, ...M-1\}$ où M est choisi bien plus grand que $r : M >> r$. Ici, $\frac{\mathbb{Z}}{M\mathbb{Z}}$ est le groupe additif des entiers pris $mod \, M$. En fait

r est inconnu, mais nous supposons que l'on connait une borne supérieure, et qu'il est donc possible de choisir $M >> r$. Par exemple, pour la recherche de l'ordre, nous savons que $r < N$. Nous verrons dans ce cas que $M = O(N^2)$ est suffisant.

Soit $H = \{$ensemble des multiples de r plus petits que $M\}$. Si M est un multiple de r alors H est un sous groupe de $\frac{\mathbb{Z}}{M\mathbb{Z}}$ et nous pourions appliquer un algorithme du même type que celui de Simon. Mais puisque r est inconnu, nous ne pouvons pas espérer choisir M multiple de r, si bien qu'en général H n'est pas un sous groupe de $\frac{\mathbb{Z}}{M\mathbb{Z}}$. Néanmoins, puisque $M >> r$ on peut considérer que "l'effet de bord" ne sera pas visible pour la plupart des entiers et que "H est presque un sous groupe" de $\frac{\mathbb{Z}}{M\mathbb{Z}}$. A quelques ennuis techniques près, l'algorithme sera essentiellement une généralisation de celui de Simon.

Tout d'abord il nous faut représenter les entiers $x \in \{0, ..., M-1\}$ par des états quantiques. Nous prenons (sans perte de généralité) $M = 2^m$ et notons que x peut être représenté grâce à son expansion binaire

$$x = 2^{m-1}x_{m-1} + 2^{m-2}x_{m-2} + ... + 2^2x_2 + 2x_1 + x_0,$$

avec m bits

$$x = \underbrace{(x_{m-1}.....x_0)}_{\text{dev binaire de x}}.$$

En particulier $(0, ..., 0) = 0$ et $(1, ..., 1) = 2^m - 1$. Il est donc naturel de prendre comme espace de Hilbert

$$\mathcal{H} = \underbrace{C^2 \otimes C^2 \otimes ... \otimes C^2}_{\text{m fois}},$$

et de stocker l'entier x dans un état quantique $|x\rangle \in \mathcal{H}$ construit à partir de m qubits (m systèmes à 2 niveaux : spins nucléaire, polarization des photons...)

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

La fonction f est comme d'habitude représentée par l'opération unitaire

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

où $|0\rangle$ et $|f(x)\rangle$ dont des états à m qubits (dans l'algorithme de shor on calcule $f(x)$ mod N et donc m bits suffisent certainement). Nous aurons aussi besoin de la "Transformée de Fourrier Quantique" définie par :

$$QFT|x\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{xy}{M}} |y\rangle \quad = \frac{1}{2^{m/2}} \sum_{y_0....y_{m-1} \in \{0,1\}^m} e^{2\pi i \frac{xy}{M}} |y_0....y_{m-1}\rangle$$

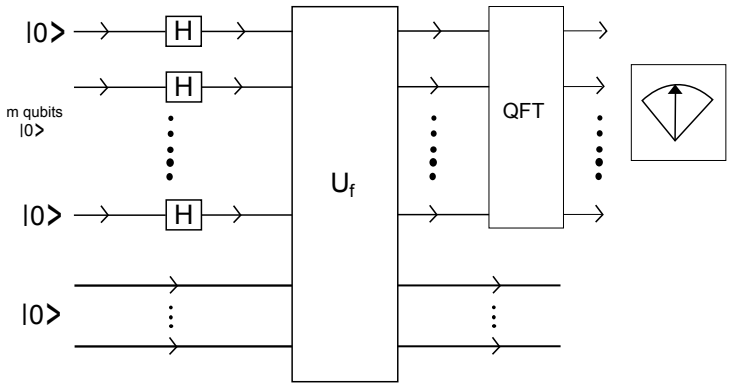

FIGURE 6.1 – Circuit quantique pour la recherche de la période d'une fonction arithmétique

Cette opération est linéaire c.a.d que si $|\Psi\rangle = \sum_{x=0}^{M-1} c_x|x\rangle$, alors

$$QFT|\Psi\rangle = \sum_{x=0}^{M-1} c_x QFT|x\rangle.$$

On peut aussi montrer que l'opération est unitaire : ceci est un prérequis important pour pouvoir la réaliser grâce à un circuit quantique.

6.2 Circuit pour la recherche de la période

Le circuit de l'algorithme de recherche de la période est représenté sur la figure 6.1.

Le circuit pour U_f dépend de la fonction spécifique. Pour la recherche de l'ordre nous prendrons la fonction $f(x) = a^x \, mod \, N$ et verrons comment réaliser son circuit au paragraphe 6.6. Le circuit pour QFT sera réalisé au paragraphe 6.5.

Calculons maintenant l'évolution de l'état initial :

$$|0\rangle \otimes |0\rangle = \underbrace{|0...0\rangle}_{\text{m fois}} \otimes \underbrace{|0...0\rangle}_{\text{m fois}}.$$

Juste après les portes de Hadamard :

$$H^{\otimes m} \underbrace{|0...0\rangle}_{\text{m fois}} \otimes |0\rangle ... = \left(\frac{1}{2^{\frac{m}{2}}} \sum_{x_0 ... x_{m-1} \in \{0,1\}^m} |x_{m-1} .... x_0\rangle \right) \otimes |0\rangle.$$

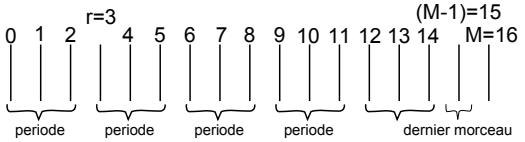

FIGURE 6.2 – Exemple de décomposition de $\{0, 1, ..., M-1\}$ pour $r+3$ et $M = 16$

C'est un état de superposition cohérente sur toutes les entrées classiques. Il peut aussi s'écrire de façon plus compacte :

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

Après U_f nous obtenons l'état

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

Exploitons le fait que f est périodique pour réorganiser cette somme. L'intervalle $[0, M-1]$ est décomposé en morceaux de longueur r, sauf pour le dernier qui sera plus court. Les entiers dans la premiere periode sont $x_0 \in \{0, 1, ..., r-1\}$. Si M était un multiple de r, on pourrait représenter chaque x comme

$$x = x_0 + jr \text{ avec } 0 \leq j \leq \frac{M}{r} - 1.$$

Dans le cas gén'eral (voir figure 6.2) on aura

$$x = x_0 + jr \text{ avec } 0 \leq j \leq A(x_0) - 1,$$

et $A(x_0)$ un entier dépendant de x_0 qui doit satisfaire

$$M - r \leq x_0 + (A(x_0) - 1)r \leq M - 1.$$

Nous avons :

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

Finalement nous agissons sur cet état avec QFT. L'état obtenu est :

$$\begin{aligned}|\Psi_{fin}\rangle =& \frac{1}{\sqrt{M}} \sum_{x_0}^{r-1} \sum_{j=0}^{A(x_0)-1} QFT|x_0 + jr\rangle \otimes |f(x_0)\rangle \\ =& \frac{1}{\sqrt{M}} \sum_{x_0}^{r-1} \sum_{j=0}^{A(x_0)-1} \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i \frac{(x_0+jr)y}{M}} |y\rangle \otimes |f(x_0)\rangle \\ =& \frac{1}{M} \sum_{x_0=0}^{r-1} \left(\sum_{y=0}^{M-1} \left(e^{2\pi i \frac{x_0 y}{M}} \sum_{j=0}^{A(x_0)-1} e^{2\pi i \frac{jy}{M/r}} \right) |y\rangle \right) \otimes |f(x_0)\rangle.\end{aligned}$$

Cette dernière expression est l'état final $|\Psi_{fin}\rangle$ juste avant la mesure.

6.3 Le Processus de Mesure

Il reste maintenant à analyser l'opération de mesure. Tout d'abord il nous faut choisir une "base représentant l'appareil de mesure". Celle-ci est formée par l'ensemble des projecteurs.

$$P_y = |y\rangle\langle y| \otimes \mathbb{I}_{m\times m}, \qquad y \in \{0, 1, 2, \cdots M-1\}.$$

L'état quantique résultant juste après la mesure est

$$\frac{P_y|\Psi\rangle_{fin}}{\langle\Psi_{fin}|P_y|\Psi_{fin}\rangle},$$

avec la probabilité

$$\text{Prob}(y) = \langle\Psi_{fin}|P_y|\Psi_{fin}\rangle.$$

Le calcul détaillé sera fait aux exercices. D'abord, on calcule $P_y|\Psi_{fin}\rangle$, puis $\langle\Psi_{fin}|P_y|\Psi_{fin}\rangle = \langle\Psi_{fin}|P_yP_y|\Psi_{fin}\rangle$. Cela donne

$$\text{Prob}(y) = \frac{1}{M^2} \sum_{x_0=0}^{r-1} \left| \sum_{j=0}^{A(x_0)=1} e^{2\pi i \frac{jy}{M/r}} \right|^2.$$

Remarquons que les différents termes de la somme sur x_0 n'interfèrent pas car les kets $|f(x_0)\rangle$ sont orthogonaux entre eux.

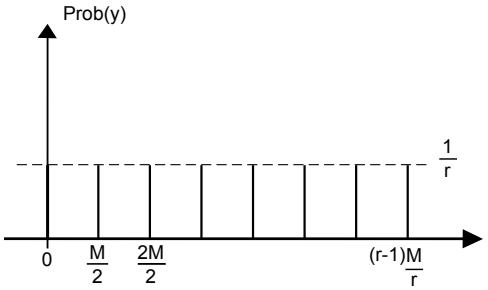

FIGURE 6.3 – Distribution de probabilité des résultats de mesures pour M multiple de r.

6.4 Analyse de la probabilité $\mathrm{Prob}(y)$

6.4.1 Traitons d'abord le cas (irréaliste) simple ou M serait multiple de r

Dans ce cas, $A(x_0) = \frac{M}{r}$ et donc

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

Si $y = k\frac{M}{r}$ avec $k = \{0, 1, ..., r-1\}$ on a

$$e^{2\pi i \frac{jy}{M/r}} = e^{2\pi i j k} = 1.$$

Si bien que $\mathrm{Prob}(y) = \frac{r}{M^2} \left|\frac{M}{r}\right|^2 = \frac{1}{r}$. Puisque cette probabilité doit se sommer à 1, nous en déduisons qu'elle est nulle pour toutes les autres valeurs de $y \neq k\frac{M}{r}$. Cette distribution est représentée sur la figure 6.3.

La mesure donne avec probabilité 1 une valeur de y de la forme

$$y = k\frac{M}{r} \;\; avec \;\; k \in \{0, 1, ..., r-1\}.$$

Puisque M est connu, grâce à la valeur de y donnée par la mesure, nous calculons $\frac{y}{M}$. Deux cas de figure se presentent à nous :

- $\frac{y}{M} = \frac{K}{r}$ et $PGCD(K, r) = 1$. Alors nous pouvons trouver k et r en simplifiant la fraction $\frac{y}{M}$ "au maximum" jusqu'à ce que les numérateurs et dénominateurs n'aient plus de facteurs communs. Nous trouvons ainsi r.

– $\frac{y}{M} = \frac{K}{r}$ et $PGCD(K, r) \neq 1$. Alors nous ne savons pas jusqu'où simplifier la fraction (et n'avons pas de facon systématique de trouver k et r).

En "pratique" nous ne savons pas à priori si k et r sont premiers entre eux ou non. Ainsi nous adoptons la procédure suivante : dans tous les cas simplifier la fraction $\frac{y}{M}$ au maximum, et tester si le r trouvé est bien une période de $f(x)$. La probabilité de succès est la probabilité d'avoir $PGCD(k, r) = 1$ quand k est tiré uniformément dans $\{0, 1, ..., r-1\}$. D'après ce que nous avons appris dans le chapitre précédent :

$$\text{Prob}(PGCD(k, r) = 1, k \in \{0, 1, ..., r-1\}) = \frac{\Phi(r)}{r} \geq \frac{1}{4(\ln \ln(r))}.$$

Puisque $r < M$, nous avons une probabilité de succès

$$\text{Prob}(succes) \geq \frac{1}{4 \ln \ln\, M} \qquad \left(= \frac{1}{4 \ln 2 \ln m}\right).$$

Bien que cette probabilité soit faible, nous pouvons l'amplifier en faisant tourner le circuit plusieurs fois. Au bout de T rounds :

$$\text{Prob(au moins 1 succes au bout de T rounds)} \geq 1 - \left(1 - \frac{1}{4 \ln \ln\, M}\right)^T,$$

ce qui peut être rendu proche de $1 - \epsilon$ si on prend

$$T = O(|ln\, \epsilon| \ln \ln\, M) = O(|\ln\, m||ln\, \epsilon|).$$

En effet :

$$\begin{aligned}
&1 - \left(1 - \frac{1}{4 \ln\, M}\right)^T \geq 1 - \epsilon \\
&\leftrightarrow \epsilon \geq \left(1 - \frac{1}{4 \ln\, M}\right)^T \leftrightarrow \ln\, \epsilon \geq T \ln \left(1 - \frac{1}{4 \ln\, M}\right) \\
&\leftrightarrow \ln\, \epsilon \geq -T \frac{1}{4 \ln\, M} \ (M \text{ grand}) \\
&\leftrightarrow T \geq 4 \ln \ln\, M |\ln\, \epsilon|
\end{aligned}$$

6.4.2 Passons maintenant au cas général ou M n'est pas un multiple de r.

Nous prouverons le lemme suivant. Une illustration graphique de son contenu est fournie par la figure 6.4.

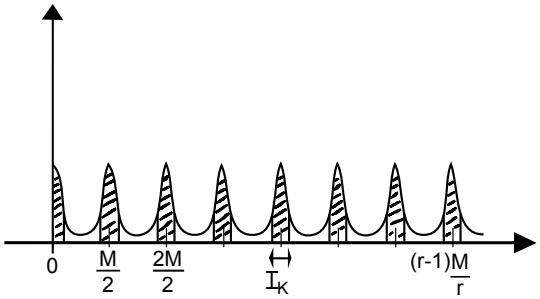

FIGURE 6.4 – Distribution de probabilité fournie par les mesures. L'aire hachurée est superieure a $\frac{2}{5}$. Notez que les intervalles I_k ont une longueur 1 et sont distant d'environ $M/r >> 1$.

Lemme. Soit $I = \cup_{k=0}^{r-1}\left[k\frac{M}{r} - \frac{1}{2}, k\frac{M}{r} + \frac{1}{2}\right] = \cup_{k=0}^{r-1} I_k$ une union d'intervalles disjoints I_k. Alors,

$$\text{Prob}(y \in I) \geq \frac{2}{5}.$$

En fait pour M de plus en plus grand, on peut remplacer $\frac{2}{5}$ par un nombre aussi proche que l'on veut de $\frac{4}{\pi^2}$.

Ainsi, avec probabilité au moins $\frac{2}{5}$ les mesures fournissent des entiers y proches de $k\frac{M}{r}$ avec $k \in \{0, 1, ..., r-1\}$. Lorsqu'une mesure donne $y \in I$ cela signifie qu'il existe k entier tel que

$$k\frac{M}{r} - \frac{1}{2} \leq y \leq k\frac{M}{r} + \frac{1}{2},$$

ce qui est équivalent à

$$\left|\frac{y}{M} - \frac{k}{r}\right| \leq \frac{1}{2M}. \tag{6.1}$$

Maintenant supposons que nous prenions $M > r^2$. Alors cette inégalité entraine,

$$\left|\frac{y}{M} - \frac{k}{r}\right| \leq \frac{1}{2r^2} \ \textit{pour} \ k \in \{0, 1, ..., r-1\}.$$

Comment pouvons nous determiner k et r à partir de y et M ? D'après ce que nous avons vu dans la théorie des fractions continuées, si le $PGCD(k, r) = 1$, alors $\frac{k}{r}$ est nécessairement un "convergent" du développement en fractions continuées de $\frac{y}{M}$. Il y a un nombre fini de "convergents" car $\frac{y}{M}$ est rationnel,

et ceux-ci peuvent être systématiquement calculés grâce à l'algorithme d'Euclide (en temps $O((\ln M)^3)$. Par contre si $PGCD(k,r) \neq 1$ on ne peut pas affirmer que $\frac{k}{r}$ est un convergent de $\frac{y}{M}$ et n'avons, dans ce cas, pas de moyen systématique de calculer k et r.

Nous adoptons donc la procédure suivante. Nous calculons tous les convergents de $\frac{y}{M}$ (grâce à l'algorithme d'Euclide) et examinons leurs dénominateurs r. Pour chacun de ces dénominateurs nous testons si c'est une période de $f(x)$. Le succès est assuré si $PGCD(k,r) = 1$, ce qui a lieu avec probabilté $O(\frac{1}{4 \ln \ln r})$.

Récapitulons. Quel est la probabilité de succès lors d'une expérience avec le circuit quantique ? Le circuit quantique est initialisé dans l'état $|0\rangle \otimes |0\rangle$. L'evolution unitaire conduit à l'état $|\Psi_{final}\rangle$, après quoi on effectue une mesure. Cette mesure donne l'entier y. Pour en déduire r avec succès, il faut remplir deux conditions :

- $y \in I$ pour un certain $k \in \{0, 1, ..., r-1\}$.
- Etant donné $y \in I_k$ il faut $PGCD(K, r) = 1$.

Donc :

$$\text{Prob(succes)} \geq \frac{2}{5} \times \frac{1}{4 \ln \ln r}.$$

En itérant l'experience $T \approx O(|\ln \epsilon| \ln \ln r)$ fois on peut amplifier la probabilité de succès à $1 - \epsilon$.

Il nous reste à démontrer le lemme utilisé ci-dessus.

Démonstration du Lemme. Dans l'expression de Prob(y) nous reconnaissons une somme géométrique de raison $\exp(2\pi i \frac{y}{M/r})$:

$$\begin{aligned} \sum_{j=0}^{A(x_0)-1} \exp(2\pi i \frac{yj}{M/r}) &= \frac{1 - (\exp(2\pi i \frac{y}{M/r}))^{A(x_0)}}{1 - (\exp(2\pi i \frac{y}{M/r}))} \\ &= \frac{\sin \pi \frac{yA(x_0)}{M/r}}{\sin \pi \frac{y}{M/r}}. \end{aligned}$$

La probabilité d'obtenir l'entier y est donc :

$$\text{Prob}(y) = \frac{1}{M^2} \sum_{x_0=0}^{r-1} \left\{ \frac{\sin^2 \pi \frac{yA(x_0)}{M/r}}{\sin^2 \pi \frac{y}{M/r}} \right\}.$$

Maintenant nous allons maintenant estimer la probabilité Prob($y \in I_k$). Fixons $k\frac{M}{r} - \frac{1}{2} \leq y \leq k\frac{M}{r} + \frac{1}{2}$. On peut toujours écrire (periodicité du

sinus) :

$$\frac{\sin^2 \pi \frac{yA(x_0)}{M/r}}{\sin^2 \pi \frac{y}{M/r}} = \frac{\sin^2 \pi \frac{(y-k\frac{M}{r})A(x_0)}{M/r}}{\sin^2 \pi \frac{(y-k\frac{M}{r})}{M/r}}.$$

Considérons la fonction

$$G(z) = \frac{\sin^2 \pi \frac{zA}{M/r}}{\sin^2 \pi \frac{z}{M/r}} \qquad \text{pour} \qquad \frac{-1}{2} \leq z \leq \frac{1}{2}.$$

On peut vérifier qu'elle atteint son minimum au bord de l'intervalle, c.a.d en $z = \pm\frac{1}{2}$. Donc :

$$\frac{\sin^2 \pi \frac{yA(x_0)}{M/r}}{\sin^2 \pi \frac{y}{M/r}} \geq \frac{\sin^2 \frac{\pi}{2} \frac{A(x_0)}{M/r}}{\sin^2 \frac{\pi}{2} \frac{1}{M/r}}.$$

Puisque $M >> r$ on peut utiliser l'approximation $A(x_0) \approx \frac{M}{r}$(en fait $A(x_0)$ est un entier proche de $\frac{M}{r}$). Donc cette borne inférieure est

$$\approx \frac{\sin^2 \frac{\pi}{2}}{\sin^2 \frac{\pi r}{2M}} \approx \frac{1}{\frac{\pi^2}{4}\left(\frac{r}{M}\right)^2} = \frac{4M^2}{\pi^2 r^2},$$

et finalement (en utilisant que la longueur de I_k vaut 1)

$$\text{Prob}(y \in I_k) \geq \frac{1}{M^2} \sum_{x_0=0}^{r-1} \frac{4M^2}{\pi^2 r^2} = \frac{4}{\pi^2}\frac{1}{r},$$

et aussi

$$\text{Prob}(y \in I) = \sum_{k=0}^{r-1} P_r(y \in I_k) \geq \frac{4}{\pi^2}.$$

Car les intervalles sont disjoints.

6.5 Le circuit de la QFT

Dans ce paragraphe nous montrons comment réaliser le circuit de la QFT. En exercice nous avons vu que pour $M = 2$, on a $QFT = H$ (la porte de Hadamard) :

$$(QFT)_{M=2}|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle).$$

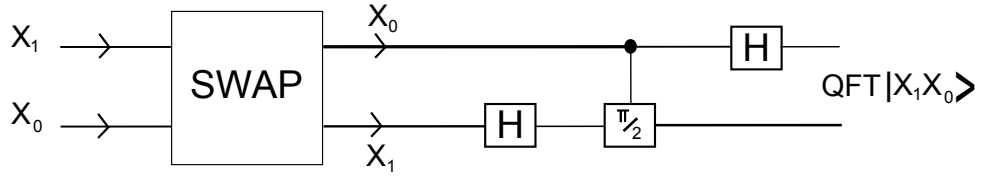

FIGURE 6.5 – Circuit de la $(QFT)_{M=4}$.

FIGURE 6.6 – Circuit pour un $SWAP$.

Pour $M = 4$,

$$\begin{aligned}(QFT)_{M=4}|x\rangle &= \frac{1}{\sqrt{4}}\left(|0\rangle + e^{i\frac{\pi}{2}x}|1\rangle + e^{i\pi x}|2\rangle + e^{3i\frac{\pi}{2}x}|3\rangle\right)\\ &= \frac{1}{\sqrt{4}}\left(|00\rangle + e^{i\frac{\pi}{2}x}|01\rangle + e^{i\pi x}|10\rangle + e^{3i\frac{\pi}{2}x}|11\rangle\right)\\ &= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi x}|1\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{\pi}{2}x}|1\rangle\right).\end{aligned}$$

En notation binaire $x \in \{0,1,2,3\}$ est représenté par

$$x = 2x_1 + x_0\,;\; x_0, x_1 \in \{0,1\}$$

si bien que $e^{i\pi x} = e^{2\pi i x_1}e^{i\pi x_0} = (-1)^{x_0}$ et $e^{i\frac{\pi}{2}x} = e^{i\pi x_1}e^{i\frac{\pi}{2}x_0} = (-1)^{x_1}e^{i\frac{\pi}{2}x_0}$. On trouve alors

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

Cette factorisation est à la base de la réalisation du circuit de la QFT. La factorisation suggère le circuit suivant de la figure 6.5. La première opération $SWAP$ échange les deux qubits. Elle peut être réalisée par trois portes $CNOT$ (figure 6.6). La seconde operation de la figure 6.5 est une porte de Hadamard agissant sur $|x_1\rangle$ pour produire $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)$. La troisième opération est un "phase shift" controlé par le premier bit x_0 : si $x_0 = 0$ il n'y a pas de phase shift et le second bit reste dans l'etat $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)$; par contre si $x_0 = 1$, il y a un phase shift et le second bit est transformé en $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}e^{i\frac{\pi}{2}}|1\rangle)$. Enfin, la dernière porte de Hadamard agit sur $|x_0\rangle$ pour produire $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_0}|1\rangle)$.

Le circuit général de la QFT est obtenu par une généralisation des remarques ci-dessus.

Lemme. Pour $x \in \{0, 1, ...M-1\}$ et $M = 2^m$

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

Démonstration. Rappelons que

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

Chaque $y \in \{0, 1, ..., 2^m - 1\}$ possède un developpement binaire

$$\begin{aligned} y &= 2^{m-1}y_{m-1} + 2^{m-2}y_{m-2} + ... + 2y_1 + y_0 \\ &= 2y' + y_0 \end{aligned}$$

où $y' = 2^{m-2}y_{m-1} + ... + y_1$. On décompose la somme sur y en une somme avec $y_0 = 0$ et une somme avec $y_0 = 1$ (cela revient a séparer les y pairs et impairs.)

$$\begin{aligned} QFT|x\rangle &= \frac{1}{2^{\frac{m}{2}}} \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{x2y'}{2^m}}|y'\rangle \otimes |0\rangle + \frac{1}{2^{\frac{m}{2}}} \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{x(2y'+1)}{2^m}}|y'\rangle \otimes |1\rangle \\ &= \left(\frac{1}{2^{\frac{m-1}{2}}} \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{xy'}{2^{m-1}}}|y'\rangle \right) \otimes \left(|0\rangle + e^{\frac{\pi i x}{2^{m-1}}}|1\rangle\right). \end{aligned}$$

Cette factorisation peut maintenant être répétée sur la premiere parenthèse. La seule difference est que $m \to m-1$. On obtient

$$QFT|x\rangle = \left(\frac{1}{2^{\frac{m-2}{2}}} \sum_{y''=0}^{2^{m-2}-1} e^{2\pi i \frac{xy''}{2^{m-2}-1}}|y''\rangle \right) \otimes \frac{|0\rangle + e^{\frac{i\pi x}{2^{m-2}}}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{\frac{i\pi x}{2^{m-1}}}|1\rangle}{\sqrt{2}}.$$

En itérant ce procédé, on obtient le résultat du lemme.

La dernière étape consiste à remplacer x par son développement binaire (comme nous l'avons fait pour $M = 4$)

$$x = 2^{m-1}x_{m-1} + ... + 2^2x_2 + 2x_1 + x_0,$$

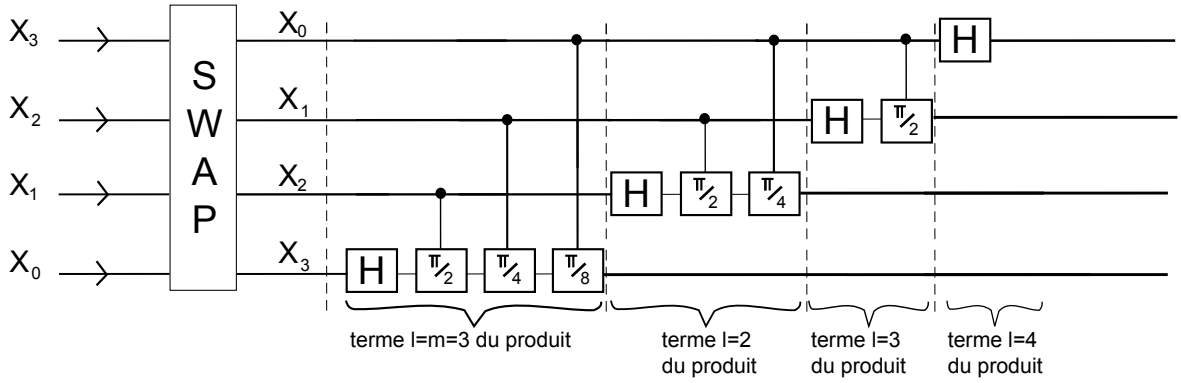

FIGURE 6.7 – Circuit de la QFT pour 4 qubits.

ce qui implique pour tout $1 \leq l \leq m$

$$e^{i\frac{\pi}{2^{l-1}}x} = e^{i\pi x_{l-1}} e^{i\frac{\pi}{2}x_{l-2}} ... e^{i\frac{\pi}{2^{l-1}}x_0}.$$

Ici le point est que les bits x_i avec $i \geq l$ ne contribuent pas. Remplacant cette expression dans la formule du lemme, on trouve la décomposition finale qui permet de construire un circuit :

$$QFT|x\rangle = \prod_{l=1}^{m} \left(\frac{|0\rangle + e^{i\pi x_{l-1}} e^{i\frac{\pi}{2}x_{l-2}} ... e^{i\frac{\pi}{2^{l-1}}x_0}|1\rangle}{\sqrt{2}} \right).$$

La figure 6.7 représente le circuit correspondant à cette dernière formule pour $m = 4$, c.a.d $M = 16$. On peut se convaincre que l'opération de $SWAP$ requiert $O(3m)$ portes $CNOT$. D'autre part, le nombre de portes H et déphasages controlés est

$$m + (m-1) + ... + 1 = \frac{m(m+1)}{2}.$$

La profondeur du circuit est donc de l'ordre de $\mathrm{O}(m^2)$. Cette profondeur indique comment le temps de calcul pour la QFT augmente avec la taille des entrées. D'autre part la largeur du circuit est m. Ainsi la taille totale est profondeur $\times$ largeur $= O(m^3)$.

6.6 Circuit pour $U_{f_{a,N}}$

Dans le chapitre précédent nous avons donné un algorithme aléatoire de factorisation d'entiers N basé sur la recherche de la période de l'exponentielle

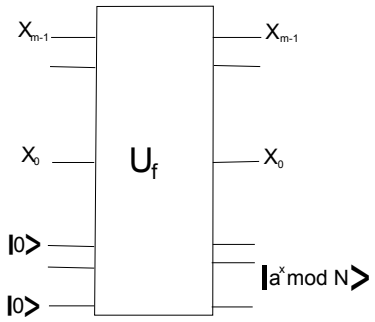

FIGURE 6.8 – Représentation unitaire de l'exponentielle modulaire

modulaire. Plus précisement, pour a t.q. $PGCD(a, N) = 1$, on cherche la période de la fonction $f_{a,N}(x) = a^x \, mod \, N$. Ceci est équivalent à la recherche de $Ord_N(a) = r$ c.à.d le plus petit entier r t.q $a^r = 1 \, mod \, N$.

Nous devons trouver un circuit qui réalise l'opérateur unitaire correspondant $U_{f_{a,N}}$. Notons d'abord que

$$\begin{aligned} a^x &= a^{2^{m-1}x_{m-1}} a^{2^{m-2}x_{m-2}} .... a^{2x_1} a^{x_0} \\ &= \left(a^{2^{m-1}}\right)^{x_{m-1}} \left(a^{2^{m-2}}\right)^{x_{m-2}} ... \left(a^2\right)^{x_1} a^{x_0}. \end{aligned}$$

Il est possible de pré-calculer les puissances $\{a, a^2, a^4, a^8, ..., a^{2^{m-1}}\}$ en un nombre polynomial d'opérations. En effet on part de a qui posséde m bits (au plus). Son carré a^2 se calcule en m^2 opérations. Puisque a^2 est pris $mod \, M$, a^2 possède aussi m bits au plus. Le carré de ce dernier $a^4 = (a^2)^2$ se calcule en m^2 opérations, et ainsi de suite. En itérant ce procédé m fois, on va jusqu'au calcul de $a^{2^{m-1}}$. Ainsi on peut pré-calculer toutes ces puissances en $O(m^3)$ opérations. Il existe des circuits classiques réversibles pour faire ce calcul, et puisqu'ils sont réversibles, ils peuvent aussi être rendus quantiques (c.à.d unitaires). Finalement pour calculer a^x, en vertu de l'identité ci-dessus il suffit de prendre le circuit (figure 6.9) : La profondeur de ce circuit est $O(m^3)$, sa largeur $O(m)$ et sa taille $O(m^4)$.

6.7 Résumé de l'algorithme de Shor

Nous sommes maintenant en mesure de résumer la totalité de l'algorithme quantique de Shor pour la factorisation d'un entier N.

input : N impair et avec au moins deux facteurs premiers distincts.

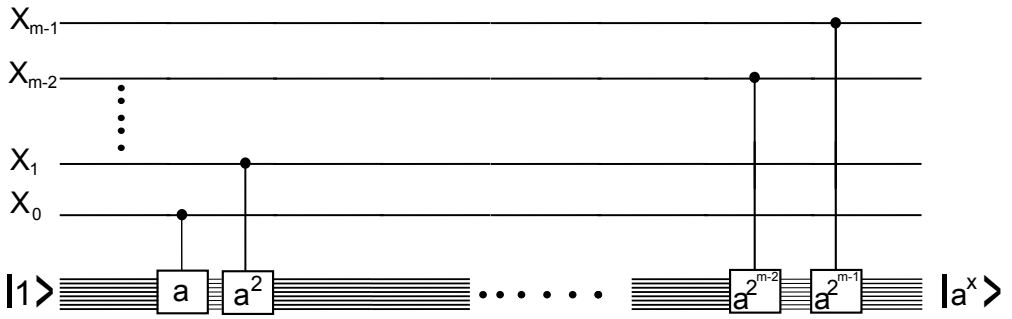

FIGURE 6.9 – Circuit pour l'exponentielle modulaire.

output : facteur non trivial de N.

temps de calcul : $O((\ln N)^3 \ln\ln N |\ln \epsilon|)$ pour une probabilité de succès supérieure à $1-\epsilon$.

taille du circuit : $O((\ln N)^3)$.

Algorithme :

1. Choisir uniformément aléatoirement $a \in \{2....N-1\}$.
2. Calculer PGCD(a,N)=d par l'algorithme d'Euclide :
   - si $d > 1 \rightarrow$ SUCCES ; on a un facteur,
   - sinon $d = 1 \rightarrow$ aller en 3.
3. Calculer $Ord_N(a)$ (i.e $a^r = 1\, mod\, N$, trouver le plus petit r). Pour cela utiliser le circuit quantique avec m qubits et $2^m = M \approx N^2$. Faire une mesure quantique et considérer le résultat y. Calculer les convergents de $\frac{y}{M}$ (grâce à l'algorithme d'Euclide). Trouver si r se trouve parmi les dénominateurs de ces convergents en testant $a^r = 1\, mod\, N$.
   - si oui (la théorie assure que c'est le plus petit possible) $\rightarrow$ aller en 4,
   - sinon $\rightarrow$ ECHEC.
4. Verifier si r est pair et $a^r \neq -1\, mod\, N$
   - si oui $\rightarrow$ aller en 5,
   - sinon $\rightarrow$ ECHEC.
5. Calculer PGCD$(a^{\frac{r}{2}}+1, N)$ et PGCD$(a^{\frac{r}{2}}-1, N$. Cela donne deux facteurs non triviaux de N (grâce à l'algorithme d'Euclide).

La probabilité de succès d'un tel "round" est $O\left(\frac{1}{\ln\ln N}\right)$ et sa complexité (temps de calcul) $O((\ln N)^3)$. On peut amplifier (comme d'habitude) la

probabilité de succès à $1-\epsilon$ en faisant $O(\ln \ln N)$ rounds. Le temps de calcul total sera alors $O(|\ln \epsilon|(\ln \ln N)(\ln N)^3)$.