Chap 4. L'algorithme de Shor.

Comme nous l'avons déjà expliqué dans le chapitre précédent on peut baser la factorisation d'un entier N sur la recherche de l'ordre d'un nombre a pris au hazard dans $\{2, 3, \dots N-1\}$.

L'ordre $Ord_N(a)$ est le plus entier r tel que

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

En d'autre terme il s'agit de la période de la fonction arithmétique

$$f_{a,N} : \mathbb{Z} \to \mathbb{Z}$$

$$x \longmapsto a^x = f_{a,N}(x) \mod N.$$

L'ordre est le plus petit entier $t.q$

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

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

4.1. Recherche de la période d'une fonction arithmétique.

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

$$f(x) = f(x + r) \qquad \forall x$$

Comme nous serons obligés de travailler avec un nombre fini de bits nous allons tronquer $\mathbb{Z}$ à $\mathbb{Z}_M = \{0, 1, 2, \dots M-1\}$

où M est choisi bien plus grand que r : $M \gg r$.

En fait r est inconnu mais nous supposons que l'on a quand même une vague idée de son ordre de grandeur et qu'il est possible de prendre $M \gg r$. $\mathbb{Z}_M$ est le groupe des entiers pris mod M ; donc dans ce paragraphe nos opérations sont mod M.

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 $\mathbb{Z}_M$ et nous pouvons espérer appliquer un algorithme ressemblant à celui de Simon. Par contre si M n'est pas un multiple de r alors H n'est pas exactement un sous groupe de $\mathbb{Z}_M$. Néanmoins comme $M \gg r$ 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 $\mathbb{Z}_M$.

Puisque r est inconnu, il n'est pas possible de choisir

$M \gg r$ multiple de r (à moins d'avoir beaucoup beaucoup de chance !) et nous serons toujours dans le cas où H est presque un sous groupe de $\mathbb{Z}_M$. Cela va créer quelques ennuis techniques ; mais essentiellement l'algorithme sera une généralisation de celui de Simon.

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

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

par m bits $\quad x = \underbrace{(x_{m-1} \dots x_0)}_{\text{développement binaire de } x}$.

Il est alors naturel de prendre comme espace de Hilbert

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

et de stocker x dans un état $|x\rangle \in \mathcal{H}$ construit à partir de m bits quantiques (systèmes à 2 niveaux, spins, photons...)

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

La fonction f est connue d'habitude représentée par l'opérateur unitaire

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

où $|0\rangle$ et $|f(x)\rangle$ sont des états à m qubits, puisque $f(x)$ prend ses valeurs dans $\mathbb{Z}_M$ et $M = 2^m$.

Nous aurons aussi besoin de la "Transformée de Fourier Quantique" définie par :

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

$$= \frac{1}{\sqrt{M}} \sum_{y_0 \cdots y_{m-1}} e^{2\pi i \frac{xy}{M}} |y_0 \cdots y_{m-1}\rangle .$$

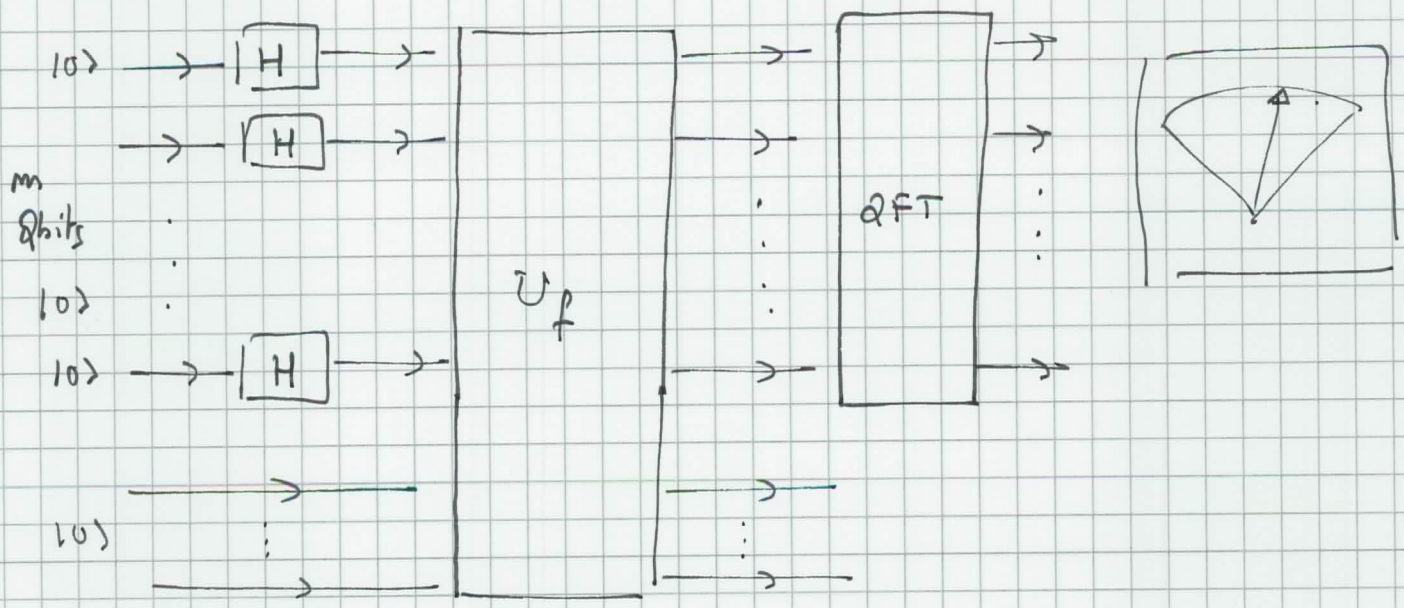
Cette opération est linéaire, c.à.d que si $|\psi\rangle = \sum_{x=0}^{M-1} c_x |x\rangle$ on a :

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

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

4.2 Circuit pour la Recherche de la Période.

Donnons maintenant le circuit de l'algorithme de recherche de la période :



Le circuit pour U_f dépend de la fonction spécifique. Plus tard nous prendrons la fonction $(f(x) = a^x \bmod N)$ et verrons comment réaliser son circuit. Le circuit pour QFT sera réalisé plus loin.

Calculons l'évolution de l'état initial

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

Juste après la porte de Hadamard :

$$H^{\otimes m} \underbrace{|0 \ldots 0\rangle}_{m \text{ fois}} \otimes |0\rangle \ldots$$

$$= \left\{ \frac{1}{2^{m/2}} \sum_{x_0 \ldots x_{m-1}} |x_{m-1} \ldots x_0\rangle \right\} \otimes |0\rangle$$

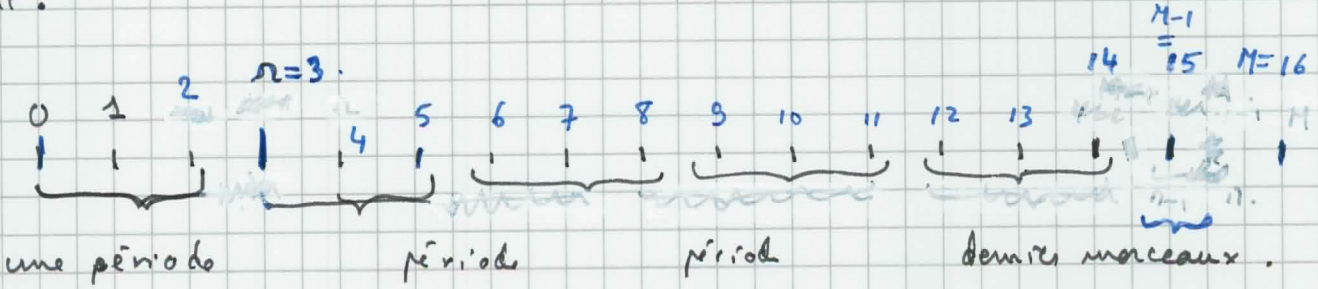
Nous avons, comme d'habitude, créé un état de superposition cohérente sur toutes les entrées classiques. Cet état peut aussi s'écrire de façon plus compacte :

$$\left\{ \frac{1}{2^{m/2}} \sum_{x=0}^{M-1} |x\rangle \right\} \otimes |0\rangle .$$

Après U_f nous obtenons l'état :

$$\frac{1}{2^{m/2}} \sum_{x=0}^{M-1} |x\rangle \otimes |f(x)\rangle .$$

Exploitons le fait que f est périodique pour organiser cette somme. L'intervalle $[0, M-1]$ est décomposé en morceaux de longueur r, sauf pour le dernier qui sera plus court :



Sur la figure $r = 3$ et $M = 5 \cdot 3 + 1 = 16 = 2^4$.

Les entiers de la première période sont $x_0 \in \{0, 1, \ldots, r-1\}$.

Si M était un multiple de r on pourrait représenter chaque entier x comme

$$x = x_0 + j r \qquad \text{avec} \qquad 0 \le j \le \frac{M}{r} - 1$$

(car il y a $\frac{M}{r}$ périodes).

En général on aura la représentation

$$x = x_0 + j r \qquad \text{avec} \qquad 0 \le j \le A(x_0) - 1 .$$

où $A(x_0)$ est un entier qui doit satisfaire

$$M - r \le \underbrace{x_0 + A(x_0) r}_{\text{doit être dans la dernière période}} \le M - 1$$

Nous avons :

$$\frac{1}{2^{n/2}} \sum_{x=0}^{M-1} |x\rangle \otimes |f(x_1)\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{A(x_0)-1} |x_0 + j r\rangle \otimes |f(x_0 + j r)\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{A(x_0)-1} |x_0 + j r\rangle \otimes |f(x_0)\rangle .$$

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

$$\frac{1}{2^{m/2}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{A(x_0)-1} \mathrm{QFT}\,|x_0 + jr\rangle \otimes |f(x_0)\rangle .$$

$$= \frac{1}{2^{m/2}} \sum_{x_0=0}^{r-1} \sum_{j=0}^{A(x_0)-1} \frac{1}{2^{m/2}} \sum_{y=0}^{M-1} e^{2\pi i \frac{(x_0+jr)y}{M}} |y\rangle \otimes |f(x_0)\rangle$$

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

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

4.3 Le Processus de Mesure.

Il reste maintenant à prendre une base représentant l'appareil de mesure. Celle-ci est formée par les projecteurs

$$P_y = |y\rangle\langle y| \otimes \mathbb{1}_{M\times M} \quad ; \quad y \in \{0, 1, 2, \ldots M-1\}$$

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

$$\Pr(y) = \langle \psi_{fin} | P_y | \psi_{fin} \rangle .$$

Le calcul détaillé sera fait en exercices. D'abord on calcule $P_y |\psi_{fin}\rangle$ puis on fait le produit scalaire $\langle \psi_{fin} | (P_y |\psi_{fin}\rangle)$.

Cela donne

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

on nous rappellons que $A(x_0)$ est un entier (unique) t.q

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

4.4 Analyse de cette Probabilité :

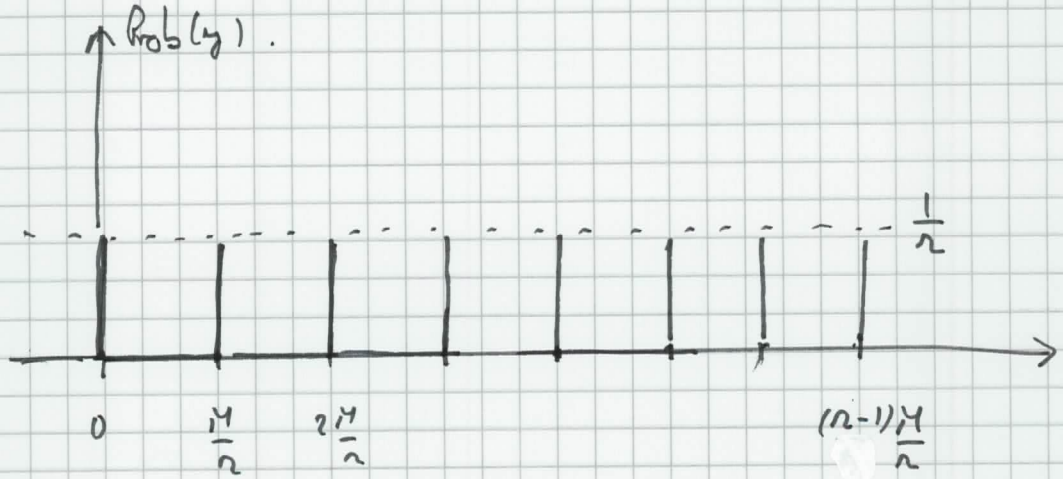
A. Traitons d'abord le cas (irréaliste) simple où M serait un multiple de r. Dans ce cas $A(x_0) = \frac{M}{r}$ et donc

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

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

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

si bien que $P_r(y) = \frac{r}{M^2} \cdot \left|\frac{M}{r}\right|^2 = \frac{1}{r}$. Puisque cette probabilité doit se sommer à 1, nous en déduisons qu'elle est nulle pour toutes les autres valeurs de $y \neq k\frac{M}{r}$.



La mesure donne avec probabilité 1 une valeur de y t.q

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

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

i) $\frac{y}{M} = \frac{k}{r}$ avec $PGCD(k, r) = 1$. 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 r.

ii) $\frac{y}{M} = \frac{k}{r}$ avec $PGCD(k, r) \neq 1$. Alors nous ne savons pas jusqu'où simplifier la fraction et nous ne trouvons pas r de façon certaine.

La probabilité de succès est la probabilité d'être dans le premier cas. D'après ce que nous avons appris au chap 3 :

$$\text{Prob}\left(\text{PGCD}(k, r) = 1 \;,\; k \in \{0, \dots, r-1\}\right) \geq \frac{\varphi(r)}{r} \geq \frac{1}{4 \log\log r}.$$

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

$$\Pr(\text{succès}) \geq \frac{1}{4 \log\log M} \qquad \left(= \frac{1}{4 \log\log n} \right).$$

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

$$\Pr(\text{au moins 1 succès au bout de } T \text{ rounds}) \geq 1 - \left(1 - \frac{1}{4 \log\log M}\right)^T$$

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

$$T = O\left(\ln(1/\epsilon) \log\log M\right) = O\left(\log n / |\ln \epsilon|\right).$$

(En effet : $1 - \left(1 - \frac{1}{4 \log\log n}\right)^T \geq 1 - \epsilon$

$$\Leftrightarrow \quad \epsilon \geq \left(1 - \frac{1}{4 \log\log n}\right)^T \quad \Leftrightarrow \quad \ln \epsilon \geq T \log\left(1 - \frac{1}{4 \log\log n}\right)$$

$$\Leftrightarrow \quad \ln \epsilon \geq -T \frac{1}{4 \log\log M} \qquad (\text{si } M \text{ large})$$

$$\Leftrightarrow \quad \boxed{T \geq 4 \log\log M / |\ln \epsilon|}. \quad)$$

B. Passons maintenant au cas général où M n'est pas un multiple de r.

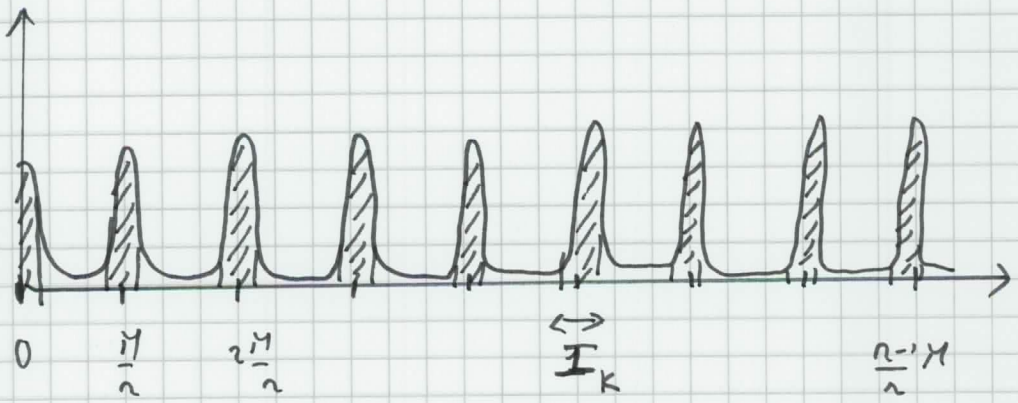
Lemme. Soit $I = \bigcup_{k=0}^{r-1} \left[k\frac{M}{r} - \frac{1}{2}, \; k\frac{M}{r} + \frac{1}{2} \right] = \bigcup_{k=0}^{r-1} I_k$

une union d'intervalles disjoints I_k (voir figure). 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 $\frac{4}{\pi^2}$.

Nous prouvons ce lemme plus tard. Sa signification est la suivante : avec probabilité au moins $\frac{2}{5}$ les valeurs obtenues de y sont proche des points $k\frac{M}{r}$ avec $k \in \{0, 1, \ldots, r-1\}$.



L'aire hachurée est supérieure à $2/5$.

Si $y \in I$ cela signifie qu'il existe k entier tel que

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

$$-\frac{1}{2} \leq y - \frac{kM}{r} \leq \frac{1}{2}$$

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

ce qui est équivalent à $\left| \frac{y}{M} - \frac{k}{r} \right| \leq \frac{1}{2M}$.

Maintenant nous supposons que nous avons pris $M \gg r$ t.q $M > r^2$. Alors la mesure donne un y t.q

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

avec $\text{prob} \geq \frac{2}{5}$.

Comment pouvons nous déterminer k et r?

D'après ce que nous avons vu dans la théorie des fractions continues, si $\text{PGCD}(k, r) = 1$, alors $\frac{k}{r}$ est un "convergent" du développement en fractions continues de $\frac{y}{M}$. De plus il y a un nombre fini de "convergents" de $\frac{y}{M}$. (car $\frac{y}{M}$ est rationel). On calcule tous les convergents $\frac{k}{r}$ et on regarde leurs dénominateurs r. On teste si r est bien une période de f.

Quelle est la probabilité de succès de l'algorithme ?

Lors d'une expérience on obtient $|\psi_{final}\rangle$ et on effectue une mesure. Cette mesure donne l'entier y.

Pour avoir un succès il faut :

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

  (sinon $\frac{k}{r}$ ne peut pas être un convergent de $\frac{y}{M}$).

Donc :

$$P_r(\text{succès}) = \sum_{k=0}^{r-1} P_r(y \in I_k)\ P(PGCD(k, r) = 1 \mid y \in I_k)$$

$$\geq \left\{ \sum_{k=0}^{r-1} P_r(y \in I_k) \right\} \frac{1}{4 \log(\log r)} = \frac{2}{5} \cdot \frac{1}{4 \log(\log r)}.$$

La probabilité de succès est donc supérieure à $\frac{1}{10 \log(\log r)}$. En itérant l'expérience $T \simeq O(|\ln \epsilon| \log(\log r))$ fois on peut amplifier la proba de succès à $1 - \epsilon$.

Il nous reste à démontrer le lemme de la page 12.

Démonstration du Lemme.

Dans l'expression de $P_n(y)$ nous reconnaissons une somme géométrique de raison $\exp\left(2\pi i \frac{y}{M/n}\right)$:

$$\sum_{j=0}^{A(x_0)-1} \exp\left(2\pi i \frac{yj}{M/n}\right) = \frac{1 - \left(\exp 2\pi i \frac{y}{M/n}\right)^{A(x_0)}}{1 - \exp 2\pi i \frac{y}{M/n}}$$

$$= \frac{\sin \pi \frac{y A(x_0)}{M/n}}{\sin \pi \frac{y}{M/n}} .$$

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

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

Maintenant nous allons estimer cette probabilité pour $y \in I_k$.

Fixons $k\frac{M}{n} - \frac{1}{2} \leq y \leq k\frac{M}{n} + \frac{1}{2}$. On peut toujours écrire : (périodicité de sin).

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

Considérons la fonction

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

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

$$\frac{\sin^2 \pi \frac{y A(x_0)}{M/n}}{\sin^2 \frac{\pi y}{M/n}} \gg \frac{\sin^2 \frac{\pi}{2} \frac{A(x_0)}{M/n}}{\sin^2 \frac{\pi}{2} \frac{1}{M/n}}$$

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

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

Finalement

$$Pr(y \in I_k) \geq \frac{1}{M^2} \sum_{x_0=0}^{n-1} \frac{4}{\pi^2} \frac{M^2}{n^2} = \frac{4}{\pi^2} \frac{1}{n}.$$

et

$$Pr(y \in I) = \sum_{k=0}^{n-1} Pr(y \in I_k) \geq \frac{4}{\pi^2}$$ car les intervalles sont disjoints

■

4.5. Le circuit de la QFT.

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

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

et que pour $M=4$

$$QFT\,|x\rangle = \frac{1}{\sqrt{4}}\left(|0\rangle + e^{i\frac{\pi}{2}x}|1\rangle + e^{i\pi x}|2\rangle + e^{3i\frac{\pi}{2}x}|3\rangle\right).$$

$$= \frac{1}{\sqrt{4}}\left(|00\rangle + e^{i\frac{\pi}{2}x}|01\rangle + e^{i\pi x}|10\rangle + e^{3i\frac{\pi}{2}x}|11\rangle\right)$$

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

l'entier $x \in \{0,1,2,3\}$ peut être représenté en notation binaire

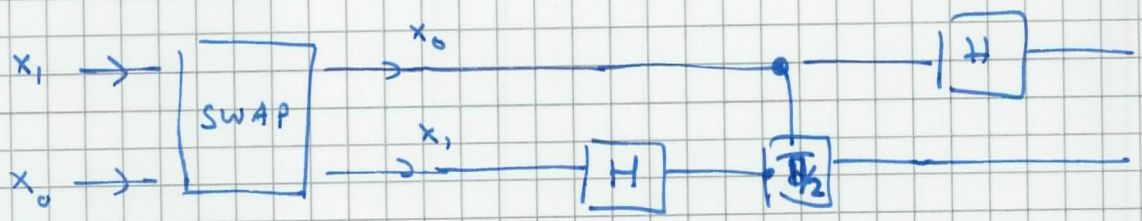
$$x = 2x_1 + x_0 \quad ; \quad x_0, x_1 \in \{0,1\}.$$

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

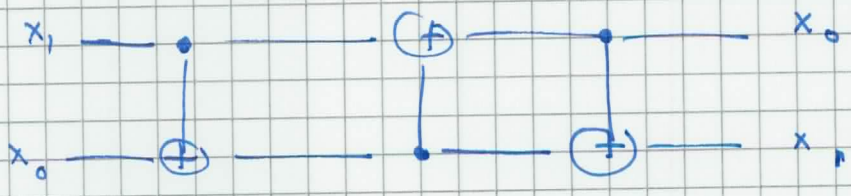
$e^{i\frac{\pi}{2}x} = e^{i\pi x_1} e^{i\frac{\pi}{2}x_0} = (-1)^{x_1} e^{i\frac{\pi}{2}x_0}$ on trouve :

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

Cette factorisation est à la base de la réalisation du circuit de la QFT. Pour $M=4$ la factorisation ci-dessus suggère le circuit suivant :



La première opération échange les deux qubits. Elle peut être réalisée par trois portes CNOT



La seconde opération 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" contrôlé 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'état $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)$.

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 une généralisation des remarques ci-dessus.

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

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

Preuve. Rappelons que

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

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

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

$$= 2y' + y_0$$

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

$$\mathrm{QFT}\,|x\rangle = \frac{1}{2^{m/2}} \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{x\,2y'}{2^m}} |y'\rangle \otimes |0\rangle$$

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

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

Cette factorisation peut maintenant être répétée sur la première parenthèse, la seule différence est que $m \to m-1$. On obtient

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

$$\otimes \frac{|0\rangle + e^{i\frac{\pi x}{2^{m-1}}}|1\rangle}{\sqrt{2}}.$$

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 $M=4$).

$$x = 2^{m-1} x_{m-1} + \cdots + 2^2 x_2 + 2 x_1 + x_0$$

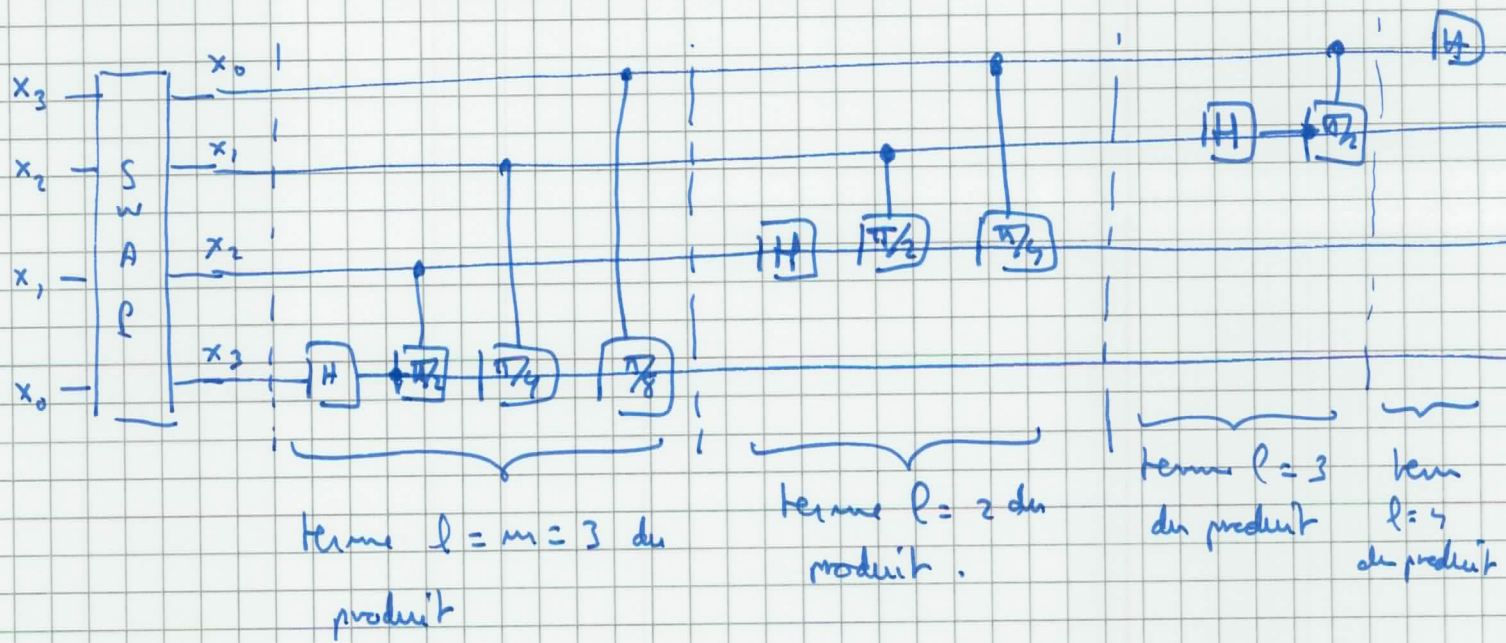
ce qui implique pour tout $1 \le \ell \le m$

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

Ici le point est que les bits x_i avec $i \ge \ell$ ne contribuent pas. Ainsi la décomposition finale est :

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

Donnons le circuit correspondant pour $m = 4$:



On peut voir que l'opération SWAP requiert $O(3m)$ portes CNOT. D'autre part le nombre de portes H et de déphasages contrôlés est

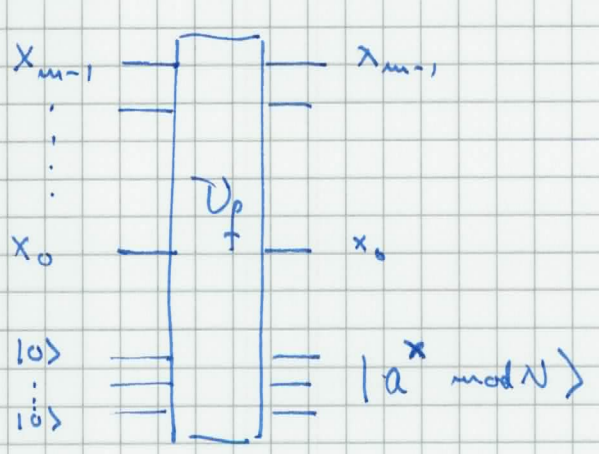
$$m + (m-1) + \cdots + 1 = \frac{m(m-1)}{2}$$

La profondeur du circuit est donc de l'ordre de $O(m^2)$. 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 est profondeur × largeur $= O(m^3)$.

4.6. Circuit pour U_f dans le problème de la factorisation.

Nous avons vu un algorithme aléatoire de factorisation d'entiers N basé sur la recherche de la période de l'exponentielle modulaire. Plus précisément pour a t.q $PGCD(a,N) = 1$ on cherche la période de la fonction $f(x) = a^x \bmod N$. Ceci est équivalent à la recherche de $Ord_N(a) = r$ c.à.d le plus petit entier r t.q $a^r = 1 \bmod N$.

Nous devons donc encore voir quel est le circuit qui réalise l'opérateur unitaire U_f.

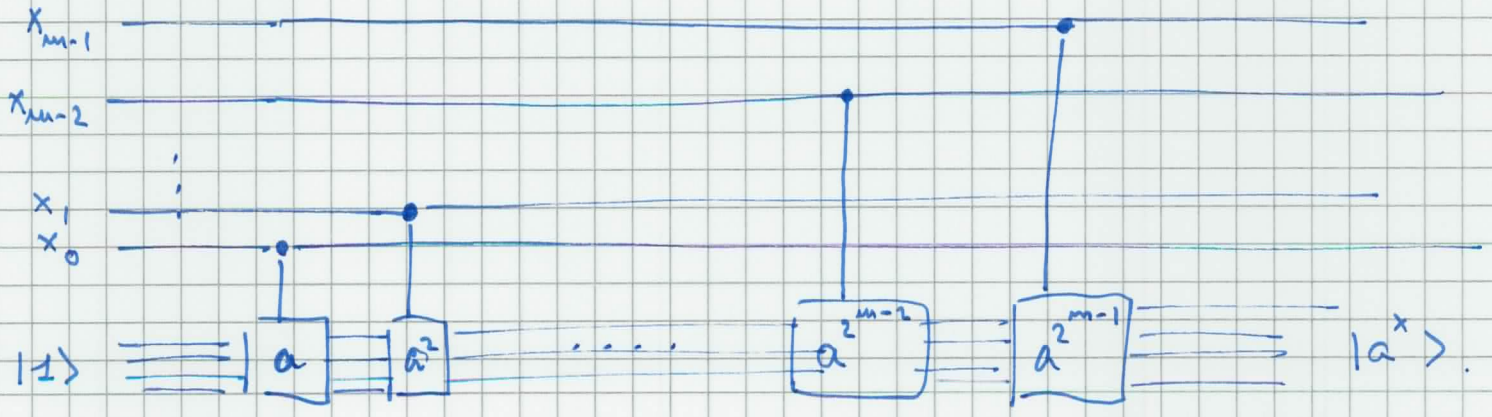


Notons d'abord que

$$a^x = a^{2^{m-1} x_{m-1}} \cdot a^{2^{m-2} x_{m-2}} \cdot \ldots a^{2 x_1} a^{x_0}$$

$$= \left(a^{2^{m-1}}\right)^{x_{m-1}} \left(a^{2^{m-2}}\right)^{x_{m-2}} \ldots (a^2)^{x_1} a^{x_0} .$$

Les puissances paires de a peuvent être pré-calculées en un nombre polynomial d'opérations. En effet en part de a qui possède m bits (au plus). Son carré a^2 se calcule en m^2 ops. 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 ops et ainsi de suite. En itérant ce procédé m fois on va jusqu'au calcul de $a^{2^{m-1}}$. Ainsi on peut calculer $\{a, a^2, a^4, a^8, \dots, a^{2^{m-1}}\}$ en $O(m \cdot m^2) = O(m^3)$ ops. Il existe des circuits classiques réversibles avec m^2 portes pour calculer chaque puissance. Ces circuits classiques réversibles peuvent aussi être rendus quantiques (car ils sont réversibles). Finalement pour calculer x, en vertu de l'identité ci-dessus il suffit de prendre le circuit :



La profondeur de ce circuit est $O(m^3)$ et sa largeur $O(m)$.

4.7. 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, $\neq p^e$ (avec au moins deux facteurs premiers distincts)

output : un facteur non trivial de N.

Temps de calcul : $O\left((\log_2 N)^3 \log_2(\log_2 N) \left|\ln \epsilon\right|\right)$ pour une proba(succès) $\geq 1-\epsilon$.

Taille du circuit : $O(\log_2 N)^3$.

Algorithme :

1. Choisir uniformément aléatoirement $a \in \{2 \dots N-1\}$.
2. Calculer $PGCD(a, N) = d$ par l'alg d'Euclide.
   Si $d > 1$ → succès ; on a un facteur.
   Sinon $d = 1$ → aller en 3.
3. Calculer $Ord_N(a)$ (i.e $a^r = 1 \bmod N$, r le plus petit ≥ 2).
   Pour cela utiliser le circuit quantique avec m qubits et $2^m = M \approx N^2$. Vérifiez que le résultat de la mesure y donne un r satisfaisant à $a^r = 1 \bmod N$.
   Si oui → aller en 4.
   Si non → ECHEC.

4. Vérifier si r est pair et $a^{r} \not\equiv -1 \bmod N$.
   Si oui → aller en 5.
   Si non → ECHEC

5. Calculer $PGCD(a^{r/2}+1, N)$ et $PGCD(a^{r/2}-1, N)$.
   Cela donne deux facteurs non triviaux de N (grâce à l'algorithme d'Euclide.).

La probabilité de succès d'un "round" est $O\left(\frac{1}{\log_2 \log_2 N}\right)$ 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 $O(\log_2 \log_2 N)$ rounds. Le temps de calcul total sera alors $O(|\ln \epsilon| (\log_2 \log_2 N)(\log_2 N)^3)$.

Remarque : Comme $M \approx N^2$ mettre N ou M dans le calcul du temps de calcul et de la probabilité de succès ne change rien aux ordres de grandeur.