Algorithme de Shor

Vidéo ■ partie 13.1. Arithmétique pour l'algorithme de Shor
Vidéo ■ partie 13.2. Début de l'algorithme de Shor
Vidéo ■ partie 13.3. Transformée de Fourier discrète (pour Shor)
Vidéo ■ partie 13.4. Fin de l'algorithme de Shor

Nous détaillons le circuit et les calculs qui permettent une factorisation rapide des entiers à l'aide d'un ordinateur quantique.

1. Arithmétique pour l'algorithme de Shor

1.1. Objectif : factoriser N

Soit N un entier. Nous aimerions décomposer N en produit de facteurs premiers : $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. Pour cela il suffit de trouver un algorithme qui fournit un facteur d de N, avec $1 < d < N$. Ensuite pour obtenir la factorisation complète, il suffit d'appliquer itérativement cet algorithme à d et à $\frac{N}{d}$. Par exemple dans le cas $N = pq$ de la cryptographie RSA, il n'y a qu'une seule étape.
Au début de l'algorithme, on commence par choisir au hasard un entier a avec $1 < a < N$. On calcule le pgcd de a et de N par l'algorithme d'Euclide (c'est une étape très rapide).

- Si $\text{pgcd}(a,N) \neq 1$ alors $d = \text{pgcd}(a,N)$ est un facteur non-trivial de N et l'algorithme est terminé ! (Par exemple dans le cas $N = pq$, cette situation est rare, car il faudrait choisir a un multiple de p ou de q.)
- Si $\text{pgcd}(a,N) = 1$, alors $a \in (\mathbb{Z}/N\mathbb{Z})^*$, c'est-à-dire a est inversible modulo N. En particulier il existe un entier $k > 0$, tel que $a^k \equiv 1 \pmod N$.

1.2. Ordre

Définition.
On appelle ***ordre*** d'un entier a modulo N, le plus petit entier r strictement positif tel que $a^r \equiv 1 \pmod N$:

$$r = \min\left\{k > 0 \mid a^k \equiv 1 \pmod N\right\}.$$

Le théorème de Lagrange pour le groupe $(\mathbb{Z}/N\mathbb{Z})^*$ de cardinal $\varphi(N)$ donne une borne sur r.

Proposition 1.
Si $\varphi(N)$ est l'indicatrice d'Euler et a est un nombre premier avec N, alors

$$a^{\varphi(N)} \equiv 1 \pmod N$$

et l'ordre de a modulo n divise $\varphi(N)$.

Mais attention, ni l'ordre r, ni l'indicatrice $\varphi(N)$ ne sont faciles à calculer. Par exemple dans le cas $N = pq$, alors $\varphi(N) = (p-1)(q-1)$ et on ne peut pas calculer $\varphi(N)$ sans connaître les facteurs p et q (que l'on ne connaît pas car c'est ce que l'on veut calculer).

1.3. Période

Proposition 2.
L'ordre r de l'entier a modulo N est la plus petite période de la fonction $k \overset{f}{\longmapsto} a^k \pmod N$.

Démonstration.
- Par définition de l'ordre r, on sait $a^r \equiv 1 \pmod N$ et $a^k \not\equiv 1 \pmod N$ pour $0 < k < r$.
- r est une période :
$$a^{k+\ell r} = a^k \cdot a^{\ell r} = a^k \cdot (a^r)^\ell \equiv a^k \cdot 1^\ell \equiv a^k \pmod N,$$
donc $f(k+\ell r) = f(k)$.
- r est la plus petite période : par l'absurde si $s < r$ était une période plus petite, alors $f(s) = f(0)$ donc $a^s \equiv a^0 \equiv 1 \pmod N$. Mais par définition, r est le plus petit entier tel que $a^r \equiv 1 \pmod N$, donc $s \geqslant r$ et nous avons une contradiction.

□

1.4. Facteurs de N

Nous allons faire plusieurs hypothèses au cours de ce chapitre. Nous discuterons plus tard de leur pertinence.

Hypothèse 1. L'ordre r de a modulo N est pair.

Nous verrons dans le chapitre suivant « Compléments d'arithmétique » que c'est le cas pour plus de la moitié des entiers a choisis au départ. Si r n'est pas pair, alors on arrête l'algorithme et on choisit une nouvelle valeur de a. À l'aide de l'identité $a^2 - b^2 = (a-b)(a+b)$ et sachant que $a^r - 1 \equiv 0 \pmod N$, on obtient alors

$$(a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \pmod N$$

Cette décomposition est la clé pour une factorisation de N.

Hypothèse 2. $a^{r/2} + 1$ n'est pas divisible par N.

Encore une fois nous verrons dans le chapitre suivant que c'est la cas pour une majorité des entiers a choisis au départ.

Proposition 3.
Avec les hypothèses 1 et 2, les entiers
$$d = \operatorname{pgcd}(a^{r/2} - 1, N) \qquad \text{et} \qquad d' = \operatorname{pgcd}(a^{r/2} + 1, N)$$
sont des facteurs non triviaux de N.

Lemme 1.
Si $ab \equiv 0 \pmod N$ avec $a \not\equiv 0 \pmod N$ et $b \not\equiv 0 \pmod N$ alors $\operatorname{pgcd}(a,N)$ et $\operatorname{pgcd}(b,N)$ sont des diviseurs non triviaux de N.

Remarque.
L'anneau des entiers $\mathbb{Z}$ est *intègre*, cela signifie qui si un produit ab est nul alors l'un des facteurs a ou b est nul. Ici ce n'est pas le cas, car si N n'est pas un nombre premier l'anneau $\mathbb{Z}/N\mathbb{Z}$ n'est pas intègre. Par exemple avec $N = 6$ on a $2 \times 3 \equiv 0 \pmod 6$.

Preuve du lemme. Supposons $ab \equiv 0 \pmod N$, c'est-à-dire N divise ab.
- Si on avait $\operatorname{pgcd}(a,N) = 1$, comme $N | ab$, par le lemme de Gauss on a $N | b$, donc $b \equiv 0 \pmod N$, ce qui donnerait une contradiction.

- Par un raisonnement similaire, on ne peut pas avoir $\text{pgcd}(b,N)=1$.

Ainsi $d=\text{pgcd}(a,N)$ est un diviseur de N avec $1<d<N$, de même pour $d'=\text{pgcd}(b,N)$. □

Preuve de la proposition.

- Tout d'abord $a^{r/2}-1\not\equiv 0 \pmod N$, car sinon $a^{r/2}\equiv 1 \pmod N$ ce qui contredirait que r est le plus petit entier tel que $a^r\equiv 1 \pmod N$.
- L'hypothèse 2 dit exactement que $a^{r/2}+1\not\equiv 0 \pmod N$.
- Par le lemme $d=\text{pgcd}(a^{r/2}-1,N)$ et $d'=\text{pgcd}(a^{r/2}+1,N)$ sont des facteurs non triviaux de N.

□

1.5. Exemple de $N=15$

Prenons $N=15$.

- Si l'entier a est choisi parmi $\{3,5,6,9,10,12\}$, alors a n'est pas premier avec N. Dans ce cas $d=\text{pgcd}(a,N)$ donne un diviseur strict de N et c'est terminé. Par exemple si $a=9$, alors $d=\text{pgcd}(9,15)=3$ est un facteur de $N=15$.
- Si l'entier $a\in\{2,4,7,8,11,13,14\}$ alors $\text{pgcd}(a,N)=1$. Il faut maintenant calculer l'ordre de a.
- Prenons l'exemple de $a=2$. Alors l'ordre de 2 modulo 15 est $r=4$, car $2^4=16\equiv 1 \pmod{15}$.
  - $a^{r/2}-1=2^2-1=3$ ainsi $d=3=\text{pgcd}(3,15)$ est un facteur de N.
  - $a^{r/2}+1=2^2+1=5$ ainsi $d'=5=\text{pgcd}(5,15)$ est aussi un facteur de N.
  - Dans ce cas nous avons factorisé $15=3\times 5$.
- Prenons l'exemple de $a=7$. Alors l'ordre de 7 modulo 15 est encore $r=4$, car $7^4=2401\equiv 1 \pmod{15}$.
  - $a^{r/2}-1=7^2-1=48$ ainsi $d=\text{pgcd}(48,15)=3$ est un facteur de N.
  - $a^{r/2}+1=7^2+1=50$ ainsi $d'=\text{pgcd}(50,15)=5$ est aussi un facteur de N.
  - Dans ce cas nous avons factorisé $15=3\times 5$.

Voici une table qui résume les différents cas pour $N=15$:

a	a premier avec N ? (et ordre)	facteurs
2	oui $r=4$	$d=\text{pgcd}(2^{4/2}-1,15)=3$ et $d'=\text{pgcd}(2^{4/2}+1,15)=5$
3	non	$d=\text{pgcd}(3,15)=3$
4	oui $r=2$	$d=\text{pgcd}(4^{2/2}-1,15)=3$ et $d'=\text{pgcd}(4^{2/2}+1,15)=5$
5	non	$d=\text{pgcd}(5,15)=5$
6	non	$d=\text{pgcd}(6,15)=3$
7	oui $r=4$	$d=\text{pgcd}(7^{4/2}-1,15)=3$ et $d'=\text{pgcd}(7^{4/2}+1,15)=5$
8	oui $r=4$	$d=\text{pgcd}(8^{4/2}-1,15)=3$ et $d'=\text{pgcd}(8^{4/2}+1,15)=5$
9	non	$d=\text{pgcd}(9,15)=3$
10	non	$d=\text{pgcd}(10,15)=5$
11	oui $r=2$	$d=\text{pgcd}(11^{2/2}-1,15)=5$ et $d'=\text{pgcd}(11^{2/2}+1,15)=3$
12	non	$d=\text{pgcd}(12,15)=3$
13	oui $r=4$	$d=\text{pgcd}(13^{4/2}-1,15)=3$ et $d'=\text{pgcd}(13^{4/2}+1,15)=5$
14	oui $r=2$	l'hypothèse 2 n'est pas vérifiée, échec

1.6. Exemple de $N=21$

Fixons $N=21$.

- Les $a\in\{3,6,7,9,12,14,15,18\}$ ne sont pas premiers avec N. Dans ce cas $d=\text{pgcd}(a,N)$ donne un diviseur strict de N et c'est terminé.
- Les éléments a de $\{8,13\}$ sont d'ordre $r=2$; ceux de $\{2,10,11,19\}$ sont d'ordre $r=6$. Dans ces deux situations on obtient les facteurs d et d' égaux à 3 et 7.

- Les éléments $a = 4$ et $a = 16$ sont d'ordre $r = 3$ impair. L'hypothèse 1 n'est pas vérifiée et l'algorithme échoue.
- Pour $a = 5$, $a = 17$ ou $a = 20$, l'entier $N = 21$ divise $a^{r/2} + 1$. L'hypothèse 2 n'est pas vérifiée et l'algorithme échoue.

Exemple. Prenons $a = 2$. Son ordre est $r = 6$, car $2^6 = 64 \equiv 1 \pmod{21}$, l'ordre est pair ; $d = \text{pgcd}(2^{6/2} - 1, 21) = \text{pgcd}(7, 21) = 7$ et $d' = \text{pgcd}(2^{6/2} + 1, 21) = \text{pgcd}(9, 21) = 3$ sont les facteurs de $N = 21$.

Exercice. Faire un tableau qui détaille tous les cas pour $N = 21$ (comme ci-dessus pour $N = 15$).

1.7. Calcul de l'ordre sur un ordinateur classique

Comme mentionné précédemment, il n'y a pas de formule pour calculer directement r ou $\varphi(N)$ si on ne connaît pas déjà les facteurs de N. Ainsi un algorithme d'informatique classique pour calculer l'ordre d'un élément a modulo N nécessiterait de calculer successivement $a^1, a^2, a^3, \ldots$ modulo N, jusqu'à trouver l'ordre r caractérisé par $a^r \equiv 1 \pmod{N}$. Il y a donc au total environ $O(N)$ calculs du type $a^k \pmod{N}$.
C'est là qu'intervient la magie de l'informatique quantique qui permet d'évaluer tous les a^k en même temps.

2. Début de l'algorithme de Shor

Pour un entier a fixé, le but est de calculer tous les a^k modulo N pour k variant de 0 à $N-1$ afin de trouver l'ordre r pour lequel $a^r \equiv 1 \pmod{N}$. On rappelle que cet ordre r est aussi la plus petite période de la fonction $k \mapsto a^k \pmod{N}$.

2.1. Ordre

Fixons un entier a. Considérons la fonction f définie par

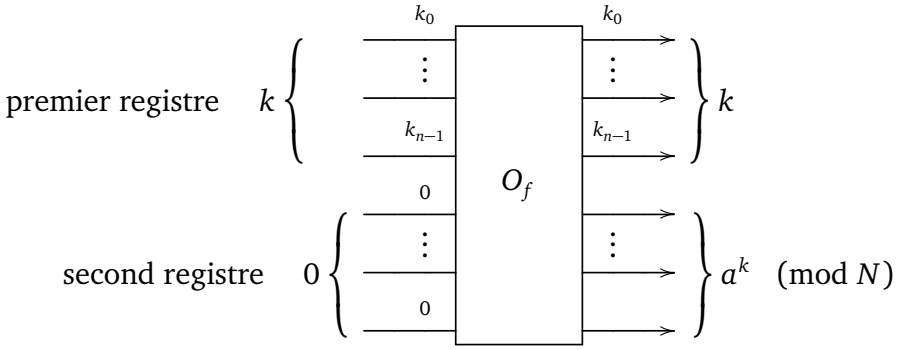
$$\begin{array}{rccc} f : & \mathbb{Z} & \longrightarrow & \mathbb{Z}/N\mathbb{Z} \\ & k & \longmapsto & a^k \pmod{N}. \end{array}$$

Ainsi $f(1) = a \pmod{N}$, $f(2) = a^2 \pmod{N}$, $f(3) = a^3 \pmod{N}$,...
On rappelle qu'à une fonction $f : x \mapsto y$ on associe l'oracle $F : (x, y) \mapsto (x, y \oplus f(x))$. Donc l'oracle associé à notre fonction $f : k \mapsto a^k \pmod{N}$ est $F : (k, y) \mapsto (k, y \oplus a^k \pmod{N})$, mais notre circuit sera toujours initialisé avec $y = 0$, donc dans notre situation nous considérerons $F : (k, 0) \mapsto (k, a^k \pmod{N})$.

> **Exemple.**
> Pour $N = 15$ et $a = 2$:
>
> $$\begin{array}{lcll} (0,0) & \overset{F}{\mapsto} & (0,1) & \\ (1,0) & \overset{F}{\mapsto} & (1,2) & \\ (2,0) & \overset{F}{\mapsto} & (2,4) & \\ (3,0) & \overset{F}{\mapsto} & (3,8) & \\ (4,0) & \overset{F}{\mapsto} & (4,1) & \text{car } 16 \equiv 1 \pmod{15} \\ (5,0) & \overset{F}{\mapsto} & (5,2) & \text{car } 32 \equiv 2 \pmod{15} \\ (6,0) & \overset{F}{\mapsto} & (6,4) & \text{car } 64 \equiv 4 \pmod{15} \\ & \vdots & & \end{array}$$

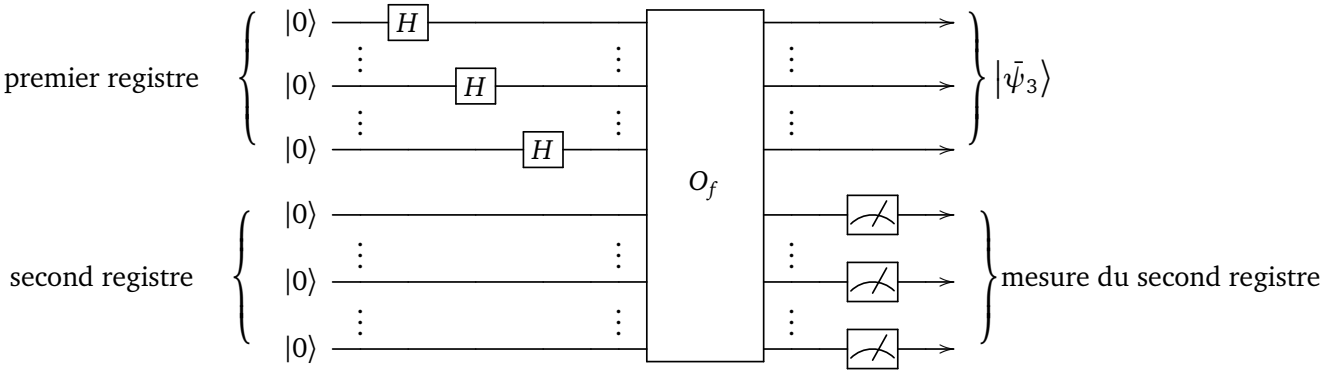
Choisissons un entier n tel que $2^n \geqslant N$. (Ce sera suffisant pour le cas étudié dans ce chapitre, mais dans le cas général il faut en fait avoir $2^n \geqslant N^2$, voir le chapitre « Compléments d'arithmétique ».)

On peut alors coder n'importe quel entier plus petit que 2^n à l'aide d'un n-bit : pour $0 \leqslant x < 2^n$, on note $\underline{x} = x_0.x_1 \dots x_{n-1}$ son écriture binaire sur n bits.



Le circuit de l'oracle est composé de deux ***registres***, en entrée le premier registre reçoit l'entier k, codé sur n bits, donc à l'aide de n lignes quantiques, même chose pour le second registre qui correspond à 0. Nous avons également deux registres en sortie, le premier renvoie k et le second $a^k \pmod N$. L'oracle a bien pour action $(k, 0) \mapsto (k, a^k \pmod N)$. En termes de qubits, si l'entrée de l'oracle est $\left|\underline{k}\right\rangle \otimes \left|\underline{0}\right\rangle$ alors la sortie $\left|\underline{k}\right\rangle \otimes \left|\underline{a^k \pmod N}\right\rangle$.

2.2. Début du circuit



- **Initialisation.** Le circuit est initialisé par des qubits tous égaux à $|0\rangle$.
$$|\psi_0\rangle = |0\dots0\rangle \otimes |0\dots0\rangle = |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} = \left|\underline{0}\right\rangle \otimes \left|\underline{0}\right\rangle.$$
- **Transformation de Hadamard.** On applique une transformation de Hadamard, mais seulement sur le premier registre (donc sur les n premières lignes).
$$|\psi_1\rangle = H^{\otimes n}\left(\left|\underline{0}\right\rangle\right) \otimes \left|\underline{0}\right\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left|\underline{k}\right\rangle\right) \otimes \left|\underline{0}\right\rangle = |\psi_H\rangle \otimes \left|\underline{0}\right\rangle.$$
- **Oracle.** On a vu que l'oracle envoie $\left|\underline{k}\right\rangle \otimes \left|\underline{0}\right\rangle$ sur $\left|\underline{k}\right\rangle \otimes \left|\underline{a^k}\right\rangle$, donc
$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left|\underline{k}\right\rangle \otimes \left|\underline{a^k}\right\rangle.$$

Remarque. Les calculs dans le second registre se font modulo N. On raccourcit l'écriture $\left|\underline{a^k \pmod N}\right\rangle$ en $\left|\underline{a^k}\right\rangle$.

Nous allons maintenant récrire $|\psi_2\rangle$ en utilisant le fait que la fonction $k \mapsto a^k \pmod N$ est périodique de période r.

Hypothèse 3. L'ordre r divise 2^n.

C'est une hypothèse qui sert à simplifier la suite des calculs. Contrairement aux hypothèses 1 et 2, ce n'est pas une hypothèse vraie en général. Quand cette hypothèse est fausse les calculs qui suivent doivent être adaptés et sont un petit peu plus compliqués, mais le principe reste le même (voir le chapitre suivant).
Sous l'hypothèse 3, pour $0 \leqslant k < 2^n$, écrivons la division euclidienne de k par r :

$$k = \alpha r + \beta \qquad \text{avec } 0 \leqslant \alpha < \frac{2^n}{r} \text{ et } 0 \leqslant \beta < r.$$

Ainsi le qubit $\left|\underline{k}\right\rangle \otimes \left|\underline{a^k}\right\rangle$ s'écrit aussi $\left|\underline{\alpha r + \beta}\right\rangle \otimes \left|\underline{a^\beta}\right\rangle$ car on rappelle que modulo N :

$$a^k = a^{\alpha r+\beta} = a^{\alpha r} \cdot a^\beta = (a^r)^\alpha \cdot a^\beta \equiv 1^\alpha \cdot a^\beta \equiv a^\beta \pmod N.$$

Ainsi :

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{\beta=0}^{r-1} \sum_{\alpha=0}^{2^n/r-1} \left|\underline{\alpha r + \beta}\right\rangle \otimes \left|\underline{a^{\alpha r+\beta}}\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{\beta=0}^{r-1} \left(\sum_{\alpha=0}^{2^n/r-1} \left|\underline{\alpha r + \beta}\right\rangle \right) \otimes \left|\underline{a^\beta}\right\rangle.$$

2.3. Mesure du second registre

Après l'oracle, on effectue une mesure du second registre, c'est-à-dire des n dernières lignes du circuit. On obtient pour ce second registre la mesure d'un $\left|\underline{a^{\beta_0}}\right\rangle$ pour un certain entier $0 \leqslant \beta_0 < r$. Après cette mesure le qubit du premier registre est :

$$\left|\bar{\psi}_3\right\rangle = \frac{\sqrt{r}}{\sqrt{2^n}} \sum_{\alpha=0}^{2^n/r-1} \left|\underline{\alpha r + \beta_0}\right\rangle.$$

Le qubit complet en sortie de circuit est donc

$$|\psi_3\rangle = \left|\bar{\psi}_3\right\rangle \otimes \left|\underline{a^{\beta_0}}\right\rangle$$

(en supposant ici que la mesure du second registre $\underline{a^{\beta_0}}$, fige le second registre en le n-qubit $\left|\underline{a^{\beta_0}}\right\rangle$).

2.4. Que donnerait la mesure du premier registre ?

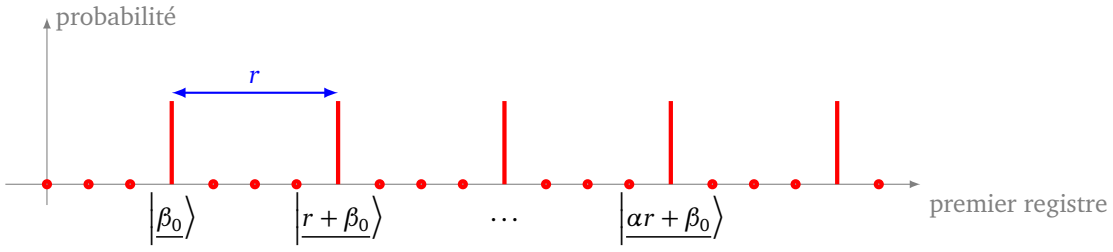
Le qubit $|\psi_3\rangle$ est une somme de $\left|\underline{\alpha r + \beta_0}\right\rangle$, $\alpha = 0, \ldots, \frac{2^n}{r} - 1$. Si on mesurait ensuite le premier registre, c'est-à-dire le qubit $\left|\bar{\psi}_3\right\rangle$ alors on obtiendrait l'un des états

$$\left|\underline{\alpha r + \beta_0}\right\rangle \qquad \text{pour un certain } 0 \leqslant \alpha < 2^n/r,$$

ou plus exactement, un n-bit $\underline{\alpha r + \beta_0}$, c'est-à-dire l'un des entiers

$$\alpha r + \beta_0 \qquad \text{pour un certain } 0 \leqslant \alpha < 2^n/r.$$

En plus, ces entiers $\alpha r + \beta_0$ sont tous équiprobables.
Voici schématiquement ce que donne la mesure du premier registre : parmi toutes les possibilités $\left|\underline{0}\right\rangle$ à $\left|\underline{2^n - 1}\right\rangle$, la mesure donne l'un des $\alpha r + \beta_0$ où β_0 est un entier fixé (donné par la mesure du second registre) et r est la période.



Le but est de trouver r, mais on ne connaît ni α, ni β_0, donc connaître l'un des $\alpha r + \beta_0$, ne permet pas de retrouver r.
Par exemple, pour $N = 15$, $\beta_0 = 1$, la mesure donne l'un des entiers 1, 5, 9 ou 13. L'écart entre ces entiers donne la période cherchée $r = 4$, mais la connaissance d'un seul de ces entiers ne permet pas de retrouver r. Malheureusement on ne peut pas refaire l'expérience pour obtenir un autre entier de la liste, car lors de la nouvelle expérience on n'obtiendra pas nécessairement le même β_0.
Il va falloir compléter le circuit pour obtenir r. Cela va nous demander pas mal d'efforts et tout le reste de ce chapitre.

2.5. Exemple de $N = 15$

Essayons de factoriser $N = 15$. On prend alors $n = 4$, car $2^4 = 16 \geqslant N$. Le circuit est donc composé de deux registres de 4-bits (donc 8 lignes en tout).
On fixe un entier a premier avec N. Pour un exemple concret on prendra $a = 2$.

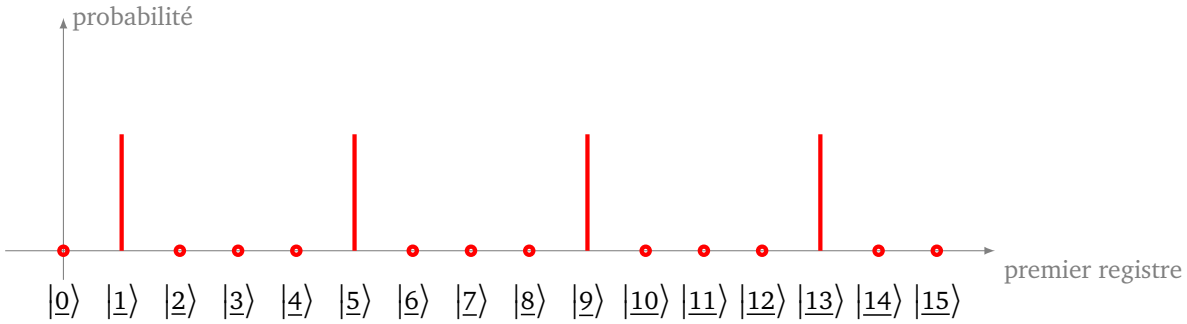
- **Initialisation.**
$$|\psi_0\rangle = |0.0.0.0\rangle \otimes |0.0.0.0\rangle = \left|\underline{0}\right\rangle \otimes \left|\underline{0}\right\rangle.$$
- **Transformation de Hadamard.**
$$|\psi_1\rangle = H^{\otimes 4} \left|\underline{0}\right\rangle \otimes \left|\underline{0}\right\rangle = \frac{1}{4}\left(\left|\underline{0}\right\rangle + \left|\underline{1}\right\rangle + \left|\underline{2}\right\rangle + \cdots + \left|\underline{15}\right\rangle\right) \otimes \left|\underline{0}\right\rangle.$$
- **Oracle.**
$$|\psi_2\rangle = \frac{1}{4}\left(\left|\underline{0}\right\rangle \cdot \left|\underline{a^0}\right\rangle + \left|\underline{1}\right\rangle \cdot \left|\underline{a^1}\right\rangle + \left|\underline{2}\right\rangle \cdot \left|\underline{a^2}\right\rangle + \cdots + \left|\underline{15}\right\rangle \cdot \left|\underline{a^{15}}\right\rangle\right)$$
Souvenons-nous que les termes des seconds facteurs sont calculés modulo N. Considérons le choix de $a = 2$, alors l'ordre que l'on veut déterminer est $r = 4$:
$$2^0 \equiv 1 \pmod{15} \qquad 2^1 \equiv 2 \pmod{15} \qquad 2^2 \equiv 4 \pmod{15} \qquad 2^3 \equiv 8 \pmod{15}$$
$$2^4 \equiv 16 \equiv 1 \pmod{15} \qquad 2^5 \equiv 32 \equiv 2 \pmod{15} \qquad \cdots$$
Donc
$$\begin{aligned}|\psi_2\rangle = \tfrac{1}{4}\Big(&\left|\underline{0}\right\rangle\left|\underline{1}\right\rangle + \left|\underline{1}\right\rangle\left|\underline{2}\right\rangle + \left|\underline{2}\right\rangle\left|\underline{4}\right\rangle + \left|\underline{3}\right\rangle\left|\underline{8}\right\rangle \\ &+ \left|\underline{4}\right\rangle\left|\underline{1}\right\rangle + \left|\underline{5}\right\rangle\left|\underline{2}\right\rangle + \left|\underline{6}\right\rangle\left|\underline{4}\right\rangle + \left|\underline{7}\right\rangle\left|\underline{8}\right\rangle \\ &+ \left|\underline{8}\right\rangle\left|\underline{1}\right\rangle + \left|\underline{9}\right\rangle\left|\underline{2}\right\rangle + \left|\underline{10}\right\rangle\left|\underline{4}\right\rangle + \left|\underline{11}\right\rangle\left|\underline{8}\right\rangle \\ &+ \left|\underline{12}\right\rangle\left|\underline{1}\right\rangle + \left|\underline{13}\right\rangle\left|\underline{2}\right\rangle + \left|\underline{14}\right\rangle\left|\underline{4}\right\rangle + \left|\underline{15}\right\rangle\left|\underline{8}\right\rangle\Big)\end{aligned}$$
On peut regrouper les termes selon le second facteur :
$$\begin{aligned}|\psi_2\rangle = &\tfrac{1}{4}\Big(\left|\underline{0}\right\rangle + \left|\underline{4}\right\rangle + \left|\underline{8}\right\rangle + \left|\underline{12}\right\rangle\Big)\left|\underline{1}\right\rangle \\ &+ \tfrac{1}{4}\Big(\left|\underline{1}\right\rangle + \left|\underline{5}\right\rangle + \left|\underline{9}\right\rangle + \left|\underline{13}\right\rangle\Big)\left|\underline{2}\right\rangle \\ &+ \tfrac{1}{4}\Big(\left|\underline{2}\right\rangle + \left|\underline{6}\right\rangle + \left|\underline{10}\right\rangle + \left|\underline{14}\right\rangle\Big)\left|\underline{4}\right\rangle \\ &+ \tfrac{1}{4}\Big(\left|\underline{3}\right\rangle + \left|\underline{7}\right\rangle + \left|\underline{11}\right\rangle + \left|\underline{15}\right\rangle\Big)\left|\underline{8}\right\rangle\end{aligned}$$

- **Mesure du second registre.**
Une mesure sur le second registre renvoie de façon équiprobable :
$$\underline{1} \quad \text{ou} \quad \underline{2} \quad \text{ou} \quad \underline{4} \quad \text{ou} \quad \underline{8}.$$
Le qubit $\left|\bar{\psi}_3\right\rangle$ du premier registre dépend alors de cette mesure :
— si la mesure du second registre est $\underline{1}$ alors $\left|\bar{\psi}_3\right\rangle = \frac{1}{2}\left(\left|\underline{0}\right\rangle + \left|\underline{4}\right\rangle + \left|\underline{8}\right\rangle + \left|\underline{12}\right\rangle\right)$,
— si la mesure du second registre est $\underline{2}$ alors $\left|\bar{\psi}_3\right\rangle = \frac{1}{2}\left(\left|\underline{1}\right\rangle + \left|\underline{5}\right\rangle + \left|\underline{9}\right\rangle + \left|\underline{13}\right\rangle\right)$,

— si la mesure du second registre est $\underline{4}$ alors $|\bar{\psi}_3\rangle = \frac{1}{2}\big(|\underline{2}\rangle + |\underline{6}\rangle + |\underline{10}\rangle + |\underline{14}\rangle\big)$,
— si la mesure du second registre est $\underline{8}$ alors $|\bar{\psi}_3\rangle = \frac{1}{2}\big(|\underline{3}\rangle + |\underline{7}\rangle + |\underline{11}\rangle + |\underline{15}\rangle\big)$.

- **Mesure du premier registre.**
  On effectue ensuite une mesure sur le premier registre. Par exemple, plaçons-nous dans le cas où le second registre a donné la mesure $\underline{2}$, alors le qubit $|\bar{\psi}_3\rangle = \frac{1}{2}\big(|\underline{1}\rangle + |\underline{5}\rangle + |\underline{9}\rangle + |\underline{13}\rangle\big)$ se mesure de façon équiprobable en :

$$\underline{1} \quad \text{ou} \quad \underline{5} \quad \text{ou} \quad \underline{9} \quad \text{ou} \quad \underline{13}.$$



La mesure donne donc un entier parmi $1, 5, 9, 13$, qui ont un écart entre eux de $r = 4$ (la période que l'on veut trouver), mais comme on n'obtient qu'un seul de ces entiers cela ne permet pas de retrouver ce r.
Autre exemple : si le second registre a donné la mesure $\underline{8}$, alors la mesure du premier registre donne l'un des entiers 3, 7, 11 ou bien 15, mais ne permet pas de retrouver r.

3. Transformée de Fourier discrète

3.1. Préambule sur les nombres complexes

Rappelons quelques résultats sur l'écriture trigonométrique des nombres complexes :

- tout nombre complexe $z \in \mathbb{C}$ s'écrit $z = re^{i\theta}$ où $r \geqslant 0$ et $\theta \in \mathbb{R}$,
- un nombre complexe de module 1 s'écrit $z = e^{i\theta}$ où $\theta \in \mathbb{R}$,
- $e^{2i\pi} = 1$,
- $(e^{i\theta})^* = e^{-i\theta}$ où z^* désigne le conjugué de z.

Lemme 2 (Somme d'une suite géométrique)**.**
Soit $z \in \mathbb{C}$. Soit $n \geqslant 0$. Alors

$$1 + z + z^2 + \cdots + z^{n-1} = \begin{cases} n & \text{si } z = 1, \\ \frac{1-z^n}{1-z} & \text{sinon.} \end{cases}$$

Démonstration. Notons $S_n = \sum_{k=0}^{n-1} z^k$ la somme à calculer. Si $z = 1$ alors S_n est la somme de n termes égaux à 1. Sinon en développant $(1-z)\cdot S_n = S_n - z \cdot S_n = 1 - z^n$ car presque tous les termes se télescopent. □

Le lemme suivant est le point-clé de la transformée de Fourier discrète que l'on étudiera plus loin.

Lemme 3 (Lemme crucial)**.**
Soient $n \in \mathbb{N}^*$ et $j \in \mathbb{Z}$.

$$\boxed{\frac{1}{n}\sum_{k=0}^{n-1} e^{2i\pi\frac{kj}{n}} = \begin{cases} 1 & \text{si } \frac{j}{n} \text{ est un entier,} \\ 0 & \text{sinon.} \end{cases}}$$

Noter que si on pose $\omega = e^{\frac{2i\pi}{n}}$ et $z = \omega^j = e^{\frac{2i\pi j}{n}}$ alors la somme à calculer est simplement $\Sigma_n = \frac{1}{n}\sum_{k=0}^{n-1} z^k$.

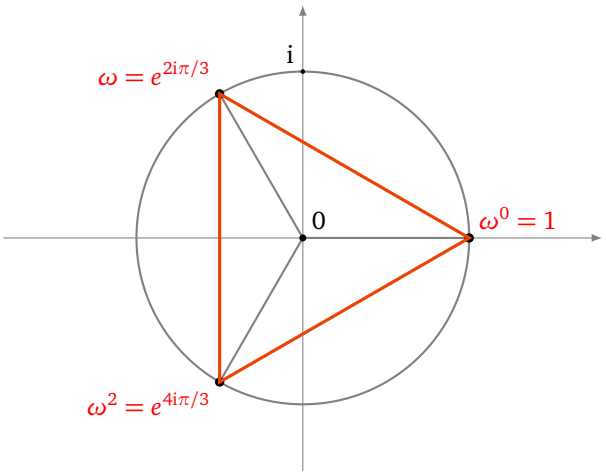
Démonstration. Par la remarque précédente il s'agit de calculer la somme d'une suite géométrique (au facteur $\frac{1}{n}$ près) : $\Sigma_n = \frac{1}{n}\sum_{k=0}^{n-1} z^k$.
Si j/n est un entier alors $z = e^{\frac{2i\pi j}{n}} = e^{2i\pi} = 1$ et par le premier cas du lemme 2, alors $\Sigma_n = 1$.
Sinon, $z \neq 1$ et à l'aide du second cas du lemme 2 :

$$\Sigma_n = \frac{1}{n}\sum_{k=0}^{n-1} z^k = \frac{1}{n}\cdot\frac{1-z^n}{1-z}.$$

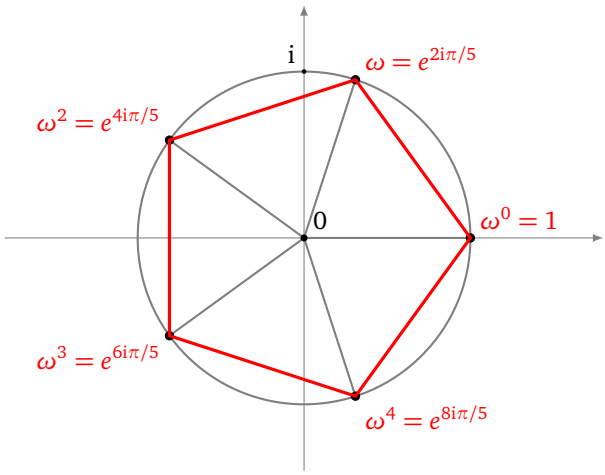
Mais $z^n = \left(e^{\frac{2i\pi j}{n}}\right)^n = e^{2i\pi j} = 1$ et ainsi $\Sigma_n = 0$.

□

Voici l'interprétation géométrique de ce lemme. Notons de nouveau $\omega = e^{\frac{2i\pi}{n}}$, c'est une racine n-ième de l'unité. Alors les ω^k forment les sommets d'un polygone régulier à n côtés. Le barycentre de ces points a pour coordonnées $\frac{1}{n}\sum_{k=0}^{n-1}\omega^k = 0$ par le lemme, c'est donc bien l'origine ! D'un point de vue physique on parle d'interférence destructive.



$n = 3$, $\omega = e^{\frac{2i\pi}{3}}$



$n = 5$, $\omega = e^{\frac{2i\pi}{5}}$

3.2. Transformée de Fourier

Fixons un entier $n \geqslant 1$. La ***transformée de Fourier discrète*** $\hat{F}$ transforme un n-qubit de base en une somme de n-qubits de base selon la formule :

$$\boxed{\hat{F}\left|\underline{k}\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1} e^{2i\pi\frac{kj}{2^n}}\left|\underline{j}\right\rangle}$$

Si on note $\omega = e^{\frac{2i\pi}{2^n}}$ alors la formule s'écrit aussi :

$$\boxed{\hat{F}\left|\underline{k}\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1} (\omega^k)^j\left|\underline{j}\right\rangle}$$

Ensuite $\hat{F}$ est étendue par linéarité à n'importe quel n-qubit $|\psi\rangle$. Si $|\psi\rangle = \sum_{k=0}^{2^n-1}\alpha_k\left|\underline{k}\right\rangle$ alors

$$\hat{F}|\psi\rangle = \sum_{k=0}^{2^n-1}\alpha_k\hat{F}\left|\underline{k}\right\rangle.$$

Commençons par des exemples avec de petites valeurs de n.

Exemple.
Fixons $n = 1$. Les deux 1-qubits de base sont $|0\rangle$ et $|1\rangle$. On a alors $2^n = 2$ et $\omega = e^{\frac{2i\pi}{2}} = e^{i\pi} = -1$.
Pour $k = 0$, les coefficients seront $(\omega^0)^0 = 1$ et $(\omega^0)^1 = 1$, donc :

$$\hat{F}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Pour $k = 1$, les coefficients seront $(\omega^1)^0 = 1$ et $(\omega^1)^1 = -1$, donc :

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

Résumons les coefficients par le tableau des valeurs $(\omega^k)^j$, avec ici $\omega = -1$.

	$j=0$	$j=1$
$k=0$	$(\omega^0)^0$	$(\omega^0)^1$
$k=1$	$(\omega^1)^0$	$(\omega^1)^1$

	$j=0$	$j=1$
$k=0$	1	1
$k=1$	1	-1

Pour un qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ alors

$$\begin{aligned}\hat{F}|\psi\rangle &= \hat{F}(\alpha|0\rangle + \beta|1\rangle) = \alpha\hat{F}|0\rangle + \beta\hat{F}|1\rangle \\ &= \frac{1}{\sqrt{2}}\alpha(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}\beta(|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{2}}(\alpha+\beta)|0\rangle + \frac{1}{\sqrt{2}}(\alpha-\beta)|1\rangle\end{aligned}$$

Noter qu'au final pour $n = 1$, $\hat{F}$ est égale à la porte de Hadamard H.

Exemple.
Fixons $n = 2$. Les 2-qubits de base sont $\left|\underline{0}\right\rangle = |0.0\rangle$, $\left|\underline{1}\right\rangle = |0.1\rangle$, $\left|\underline{2}\right\rangle = |1.0\rangle$ et $\left|\underline{3}\right\rangle = |1.1\rangle$. On a alors $2^n = 4$ et $\omega = e^{\frac{2i\pi}{4}} = e^{i\frac{\pi}{2}} = i$.
Les coefficients de $\hat{F}\left|\underline{k}\right\rangle$ sont les $(\omega^k)^j$.

- Pour $k = 0$, les coefficients sont tous 1,
- Pour $k = 1$, les coefficients sont les i^j,
- Pour $k = 2$, les coefficients sont les $(-1)^j$,
- Pour $k = 3$, les coefficients sont les $(-i)^j$.

Voici le tableau des coefficients $(\omega^k)^j$ avec $\omega = i$.

	$j=0$	$j=1$	$j=2$	$j=3$
$k=0$	$(\omega^0)^0$	$(\omega^0)^1$	$(\omega^0)^2$	$(\omega^0)^3$
$k=1$	$(\omega^1)^0$	$(\omega^1)^1$	$(\omega^1)^2$	$(\omega^1)^3$
$k=2$	$(\omega^2)^0$	$(\omega^2)^1$	$(\omega^2)^2$	$(\omega^2)^3$
$k=3$	$(\omega^3)^0$	$(\omega^3)^1$	$(\omega^3)^2$	$(\omega^3)^3$

	$j=0$	$j=1$	$j=2$	$j=3$
$k=0$	1	1	1	1
$k=1$	1	i	-1	$-i$
$k=2$	1	-1	1	-1
$k=3$	1	$-i$	-1	i

Ainsi :

$$\hat{F}\left|\underline{0}\right\rangle = \frac{1}{2}\left(\left|\underline{0}\right\rangle + \left|\underline{1}\right\rangle + \left|\underline{2}\right\rangle + \left|\underline{3}\right\rangle\right)$$
$$\hat{F}\left|\underline{1}\right\rangle = \frac{1}{2}\left(\left|\underline{0}\right\rangle + \mathrm{i}\left|\underline{1}\right\rangle - \left|\underline{2}\right\rangle - \mathrm{i}\left|\underline{3}\right\rangle\right)$$
$$\hat{F}\left|\underline{2}\right\rangle = \frac{1}{2}\left(\left|\underline{0}\right\rangle - \left|\underline{1}\right\rangle + \left|\underline{2}\right\rangle - \left|\underline{3}\right\rangle\right)$$
$$\hat{F}\left|\underline{3}\right\rangle = \frac{1}{2}\left(\left|\underline{0}\right\rangle - \mathrm{i}\left|\underline{1}\right\rangle - \left|\underline{2}\right\rangle + \mathrm{i}\left|\underline{3}\right\rangle\right)$$

De façon générale pour n quelconque et $\omega = e^{\frac{2\mathrm{i}\pi}{2^n}}$, alors voici comment s'organise le tableau des $(\omega^k)^j$.

	$j=0$	$j=1$	$j=2$	$j=3$	$\cdots$
$k=0$	1	1	1	1	$\cdots$
$k=1$	1	ω	ω^2	ω^3	$\cdots$
$k=2$	1	ω^2	$(\omega^2)^2$	$(\omega^2)^3$	$\cdots$
$k=3$	1	ω^3	$(\omega^3)^2$	$(\omega^3)^3$	$\cdots$
$k=4$	1	ω^4	$\cdots$		
$\cdots$	$\cdots$	$\cdots$			

3.3. La transformée de Fourier discrète est unitaire

Proposition 4.
La transformation de Fourier discrète est une application unitaire.

Commençons par le vérifier sur des exemples.

- Pour $n=1$, notons $|\psi_0\rangle = \hat{F}\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et $|\psi_1\rangle = \hat{F}\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Alors la base $(|0\rangle, |1\rangle)$ est envoyée sur la base $(|\psi_0\rangle, |\psi_1\rangle)$. Comme une base orthonormale est envoyée sur une base orthonormale, $\hat{F}$ est une transformation unitaire.
- Pour $n=2$, notons de même $|\psi_k\rangle = \hat{F}\left|\underline{k}\right\rangle$ pour $k=0,1,2,3$ que l'on a calculé auparavant. On vérifie que les $|\psi_k\rangle$ forment une base orthonormale. Par exemple, montrons que $|\psi_1\rangle$ et $|\psi_2\rangle$ sont orthogonaux. Tout d'abord
$$\langle\psi_1| = |\psi_1\rangle^* = \frac{1}{2}\left(\left\langle\underline{0}\right| - \mathrm{i}\left\langle\underline{1}\right| - \left\langle\underline{2}\right| + \mathrm{i}\left\langle\underline{3}\right|\right)$$
Donc :
$$\langle\psi_1|\psi_2\rangle = \frac{1}{4}\left(\left\langle\underline{0}\right| - \mathrm{i}\left\langle\underline{1}\right| - \left\langle\underline{2}\right| + \mathrm{i}\left\langle\underline{3}\right|\right)\cdot\left(\left|\underline{0}\right\rangle - \left|\underline{1}\right\rangle + \left|\underline{2}\right\rangle - \left|\underline{3}\right\rangle\right).$$
On développe tout, et on utilise que $\left\langle\underline{p}\middle|\underline{q}\right\rangle = 0$ si $p \neq q$ et $\left\langle\underline{p}\middle|\underline{p}\right\rangle = 1$:
$$\langle\psi_1|\psi_2\rangle = \frac{1}{4}\left(\left\langle\underline{0}\middle|\underline{0}\right\rangle + \mathrm{i}\left\langle\underline{1}\middle|\underline{1}\right\rangle - \left\langle\underline{2}\middle|\underline{2}\right\rangle - \mathrm{i}\left\langle\underline{3}\middle|\underline{3}\right\rangle\right) = \frac{1}{4}(1+\mathrm{i}-1-\mathrm{i}) = 0.$$

Démonstration. Nous allons montrer que la base canonique des $\left|\underline{k}\right\rangle$ s'envoie sur une base orthonormale $|\psi_k\rangle$. Ainsi $\hat{F}$ envoie une base orthonormale sur une base orthonormale et est donc une transformation unitaire (voir le chapitre « Portes quantiques »).

Notons $|\psi_k\rangle = \hat{F}\left|\underline{k}\right\rangle$, pour $0 \leqslant k \leqslant 2^n - 1$.

$$\begin{aligned}
\langle\psi_k|\psi_\ell\rangle &= \left(\hat{F}\left|\underline{k}\right\rangle\right)^* \cdot \hat{F}\left|\underline{\ell}\right\rangle \\
&= \left(\frac{1}{\sqrt{2^n}}\sum_{p=0}^{2^n-1} e^{-2i\pi\frac{kp}{2^n}}\left\langle\underline{p}\right|\right)\cdot\left(\frac{1}{\sqrt{2^n}}\sum_{q=0}^{2^n-1} e^{2i\pi\frac{\ell q}{2^n}}\left|\underline{q}\right\rangle\right) \\
&= \frac{1}{2^n}\sum_{p=0}^{2^n-1}\sum_{q=0}^{2^n-1} e^{-2i\pi\frac{kp}{2^n}} e^{2i\pi\frac{\ell q}{2^n}}\left\langle\underline{p}\middle|\underline{q}\right\rangle \\
&= \frac{1}{2^n}\sum_{p=0}^{2^n-1} e^{-2i\pi\frac{kp}{2^n}+2i\pi\frac{\ell p}{2^n}}\left\langle\underline{p}\middle|\underline{p}\right\rangle \qquad \text{car } \left\langle\underline{p}\middle|\underline{q}\right\rangle = 0 \text{ si } p \neq q \\
&= \frac{1}{2^n}\sum_{p=0}^{2^n-1} e^{2i\pi\frac{(\ell-k)p}{2^n}} \qquad \text{car } \left\langle\underline{p}\middle|\underline{p}\right\rangle = 1
\end{aligned}$$

Si $k = \ell$ alors $e^{2i\pi\frac{(\ell-k)p}{2^n}} = e^0 = 1$, et ainsi $\langle\psi_k|\psi_k\rangle = 1$. Si $k \neq \ell$, alors $\frac{\ell-k}{2^n}$ n'est pas un entier, et par le lemme crucial 3, $\langle\psi_k|\psi_\ell\rangle = 0$. Ainsi les $|\psi_k\rangle$ forment une base orthonormée et $\hat{F}$ est une transformation unitaire. □

3.4. Transformée de Fourier inverse

Comme $\hat{F}$ est unitaire alors $\hat{F}$ est inversible et $\hat{F}^{-1} = \hat{F}^*$. Ainsi la formule de $\hat{F}^{-1}\left|\underline{k}\right\rangle$ est celle de $\hat{F}\left|\underline{k}\right\rangle$ mais avec un signe moins dans l'exponentielle :

$$\boxed{\hat{F}^{-1}\left|\underline{k}\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1} e^{-2i\pi\frac{kj}{2^n}}\left|\underline{j}\right\rangle}$$

Si on note $\omega = e^{\frac{2i\pi}{2^n}}$, alors $\omega^* = e^{\frac{-2i\pi}{2^n}}$ et ainsi

$$\hat{F}^{-1}\left|\underline{k}\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}(\omega^{*k})^j\left|\underline{j}\right\rangle.$$

Exemple.
Fixons $n = 1$, $\omega^* = -1$.

$$\hat{F}^{-1}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{et} \quad \hat{F}^{-1}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Dans ce cas $\hat{F}^{-1} = \hat{F}$.

Exemple.
Fixons $n = 2$, $\omega^* = -i$.

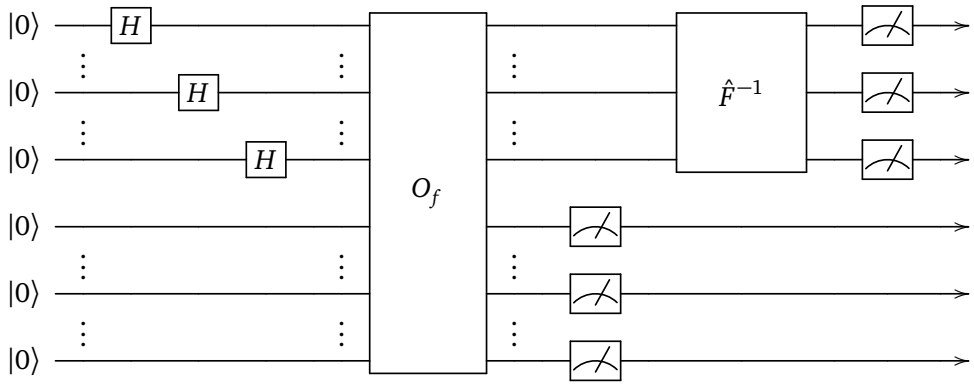
$$\begin{aligned}
\hat{F}^{-1}\left|\underline{0}\right\rangle &= \frac{1}{2}\left(\left|\underline{0}\right\rangle + \left|\underline{1}\right\rangle + \left|\underline{2}\right\rangle + \left|\underline{3}\right\rangle\right) \\
\hat{F}^{-1}\left|\underline{1}\right\rangle &= \frac{1}{2}\left(\left|\underline{0}\right\rangle - i\left|\underline{1}\right\rangle - \left|\underline{2}\right\rangle + i\left|\underline{3}\right\rangle\right) \\
\hat{F}^{-1}\left|\underline{2}\right\rangle &= \frac{1}{2}\left(\left|\underline{0}\right\rangle - \left|\underline{1}\right\rangle + \left|\underline{2}\right\rangle - \left|\underline{3}\right\rangle\right) \\
\hat{F}^{-1}\left|\underline{3}\right\rangle &= \frac{1}{2}\left(\left|\underline{0}\right\rangle + i\left|\underline{1}\right\rangle - \left|\underline{2}\right\rangle - i\left|\underline{3}\right\rangle\right)
\end{aligned}$$

> *Exercice.* Vérifier à la main que $\hat{F}^{-1}\left(\hat{F}\left|\underline{1}\right\rangle\right) = \left|\underline{1}\right\rangle$.

4. Fin de l'algorithme de Shor

4.1. Fin du circuit

Après l'oracle, nous en étions restés à une mesure du second registre, et nous avions vu que la mesure du premier registre ne permettait pas de conclure. Après la mesure du second registre, nous allons faire agir sur le premier registre la transformée de Fourier discrète inverse $\hat{F}^{-1}$.



4.2. Calculs

On se souvient que la mesure du second registre a donné $\underline{a^{\beta_0}}$ (on peut aussi considérer que l'état quantique du second registre s'est effondré à $\left|\underline{a^{\beta_0}}\right\rangle$). Alors le qubit du premier registre est :

$$\left|\bar{\psi}_3\right\rangle = \frac{\sqrt{r}}{\sqrt{2^n}} \sum_{\alpha=0}^{2^n/r-1} \left|\underline{\alpha r + \beta_0}\right\rangle.$$

Calculons le qubit $\left|\bar{\psi}_4\right\rangle$ obtenu après l'action de la transformée de Fourier inverse :

$$\begin{aligned}
\left|\bar{\psi}_4\right\rangle &= \hat{F}^{-1}\left|\bar{\psi}_3\right\rangle \\
&= \hat{F}^{-1}\left(\frac{\sqrt{r}}{\sqrt{2^n}} \sum_{\alpha=0}^{2^n/r-1} \left|\underline{\alpha r + \beta_0}\right\rangle\right) \\
&= \frac{\sqrt{r}}{\sqrt{2^n}} \sum_{\alpha=0}^{2^n/r-1} \hat{F}^{-1}\left|\underline{\alpha r + \beta_0}\right\rangle \\
&= \frac{\sqrt{r}}{\sqrt{2^n}} \sum_{\alpha=0}^{2^n/r-1} \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{-2i\pi\frac{(\alpha r+\beta_0)j}{2^n}} \left|\underline{j}\right\rangle \\
&= \frac{\sqrt{r}}{2^n} \sum_{j=0}^{2^n-1} \left(\sum_{\alpha=0}^{2^n/r-1} e^{-2i\pi\frac{\alpha j}{2^n/r}}\right) e^{-2i\pi\frac{\beta_0 j}{2^n}} \left|\underline{j}\right\rangle
\end{aligned}$$

Pour la dernière égalité nous avons interverti les deux sommes et utilisé que r divise 2^n. Calculons le coefficient qui intervient dans cette somme à l'aide du lemme crucial 3 :

$$\frac{1}{2^n/r} \sum_{\alpha=0}^{2^n/r-1} e^{-2i\pi\frac{\alpha j}{2^n/r}} = \begin{cases} 1 & \text{si } \frac{j}{2^n/r} \text{ est un entier,} \\ 0 & \text{sinon.} \end{cases}$$

Ainsi

$$\left|\bar{\psi}_4\right\rangle = \frac{1}{\sqrt{r}} \sum_{\substack{j=0,\dots,2^n-1 \\ \text{avec } \frac{j}{2^n/r} \text{entier}}} e^{-2i\pi\frac{\beta_0 j}{2^n}} \left|\underline{j}\right\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{-2i\pi\beta_0\frac{\ell}{r}} \left|\underline{\frac{2^n\ell}{r}}\right\rangle.$$

Pour la dernière égalité, nous avons juste changé la notation des indices en posant $j = \frac{2^n\ell}{r}$.
Qu'avons-nous gagné avec l'action de la transformée de Fourier ? Tout d'abord la constante β_0 n'apparaît que dans les coefficients des qubits et n'intervient plus après mesure. Ensuite la période r que l'on veut déterminer est au dénominateur dans l'expression de l'entier $\frac{2^n\ell}{r}$.

4.3. Mesure du premier registre

La mesure du premier registre donne un entier $\frac{2^n\ell}{r}$, correspondant à l'un des états $\left|\underline{\frac{2^n\ell}{r}}\right\rangle$ du qubit $\left|\bar{\psi}_4\right\rangle$.
Nous obtenons donc un entier $m = \frac{2^n\ell}{r}$ et nous voulons en déduire la période r. L'entier n est connu, par contre ℓ n'est pas connu (on sait $0 \leqslant \ell \leqslant r-1$).
Commençons par diviser par 2^n (valeur connue) pour obtenir le rationnel $x = \frac{m}{2^n} = \frac{\ell}{r}$.

- Si x est entier alors on n'obtient aucune information sur r. C'est le cas si $\ell = 0$, ou bien si r divise ℓ. Dans ce cas notre méthode échoue. Il faut recommencer l'exécution du circuit quantique. Noter que ce cas se produit assez rarement.
- Si $\text{pgcd}(\ell, r) = 1$ alors d'une part $x = \frac{m}{2^n}$ est connu et son écriture sous la forme de fraction irréductible est $\frac{\ell}{r}$. Donc en réduisant la fraction $x = \frac{m}{2^n}$ en une fraction irréductible, on obtient r (et ℓ). Par exemple si $x = \frac{26}{8}$ alors l'écriture irréductible est $\frac{13}{4}$ donc $r = 4$ et $\ell = 13$.
- Si $\text{pgcd}(\ell, r) \neq 1$, alors l'écriture irréductible de $x = \frac{m}{2^n}$ est $\frac{\ell'}{r'}$. On a

  $$x = \frac{m}{2^n} = \frac{\ell'}{r'} = \frac{\ell}{r}.$$

  Ainsi $r'\ell = r\ell'$, donc r' divise $r\ell'$, mais comme $\text{pgcd}(r', \ell') = 1$ alors par le lemme de Gauss r' divise r. Nous n'avons pas trouvé la période r mais un facteur r' de r. C'est un progrès ! On recommence notre algorithme avec le choix de $a^{r'}$ au lieu de a. En effet, comme la fonction $a \mapsto a^k$ est de période r, alors la fonction $k \mapsto (a^{r'})^k$ est de période r/r'. Nous sommes certains que ce processus se termine car r n'a qu'un nombre fini de facteurs.

4.4. Exemple

Voyons la fin de l'algorithme sur l'exemple $N = 15$.

- Si $a \in \{3, 5, 6, 9, 10, 12\}$, alors a n'est pas premier avec N et $d = \text{pgcd}(a, N) > 1$ est un diviseur strict de N et c'est terminé.
- Les entiers $a \in \{4, 11, 14\}$ sont d'ordre $r = 2$, mais par contre $a = 14$ ne vérifie pas l'hypothèse 2.
  Étudions les cas $a = 4$ et $a = 11$. La mesure finale du circuit fournit $m = \frac{2^n\ell}{r}$, on calcule $x = \frac{m}{2^n} = \frac{\ell}{r}$ avec $0 \leqslant \ell \leqslant r-1$, donc ici avec $r = 2$, $x = \frac{\ell}{2}$ avec $\ell = 0$ ou $\ell = 1$. On rappelle que l'on connaît la valeur de x, mais qu'il s'agit d'obtenir r et ℓ.
  — Dans le cas $\ell = 0$ alors on a la connaissance de $x = 0$, mais on n'obtient aucune information sur r. Il faut recommencer l'algorithme.
  — Dans le cas $\ell = 1$ alors on a la connaissance de $x = \frac{1}{2}$. Comme $x = \frac{\ell}{r}$ est une fraction irréductible, la connaissance de x permet de retrouver $\ell = 1$ et $r = 2$. Nous avons obtenu la période $r = 2$.
- Les entiers $a \in \{2, 7, 8, 13\}$ sont d'ordre $r = 4$.
  La mesure finale du circuit fournit $m = \frac{2^n\ell}{r}$, on calcule $x = \frac{m}{2^n} = \frac{\ell}{r}$ avec $0 \leqslant \ell \leqslant r-1$, donc ici avec $r = 4$, $x = \frac{\ell}{4}$ avec $\ell \in \{0, 1, 2, 3\}$.
  — Dans le cas $\ell = 0$, la connaissance de $x = 0$ ne permet pas de trouver r. Il faut recommencer l'algorithme.

— Dans le cas $\ell = 1$, on a $x = \frac{1}{4}$. Comme $x = \frac{\ell}{r}$ est une fraction irréductible, la connaissance de x permet de retrouver $\ell = 1$ et $r = 4$. Nous avons obtenu la période $r = 4$.
— Dans le cas $\ell = 2$ on a $x = \frac{1}{2}$. Nous obtenons la fraction irréductible $x = \frac{\ell'}{r'}$ avec $\ell' = 1$ et $r' = 2$. L'entier $r' = 2$ n'est pas la période (c'est facile à vérifier) mais on sait que $r' = 2$ divise r. On avait choisi un entier a au début de l'algorithme, on recommence maintenant l'algorithme avec le choix de a^2 qui a pour période $r/2$. En un nombre fini d'itérations de l'algorithme on obtiendra r.
— Dans le cas $\ell = 3$, la connaissance de $x = \frac{3}{4}$ permet de retrouver $\ell = 3$ et $r = 4$.

Nous verrons dans le chapitre suivant un exemple dans lequel l'ordre r n'est pas une puissance de 2.