Transformée de Fourier quantique - Algorithmes

Philippe Jorrand
Notes de cours - Module Informatique Quantique
M2R Maths-Info - UJF Grenoble

19 février 2006

1 Théorie des groupes, rappels

1.1 Groupes

Un *groupe* $(G, \times, ^{-1}, e)$ est un ensemble G muni d'une opération de composition interne $\times$ telle que [1] :

- $\forall g_1, g_2, g_3 \in G, (g_1 \times g_2) \times g_3 = g_1 \times (g_2 \times g_3)$ (associativité de l'opération de composition interne)
- Il existe un unique élément $e \in G$ tel que $\forall g \in G,\ g \times e = e \times g = g$ (existence d'un *élément neutre* pour $\times$)
- $\forall g \in G, \exists g^{-1} \in G$ tel que $g \times g^{-1} = g^{-1} \times g = e$ (existence d'un *inverse* pour tout élément du groupe)

Si, en plus de ces trois propriétés, le groupe $(G, \times, ^{-1}, e)$ est aussi tel que :

- $\forall g_1, g_2 \in G, g_1 \times g_2 = g_2 \times g_1$ (commutativité de l'opération interne)

alors le groupe est dit *abélien*.

Dans la suite, on adoptera, selon les cas, soit une notation additive, soit une notation multiplicative pour l'opération interne du groupe. Dans le cas de la notation additive, le groupe est $(G, +, -, 0)$:

- $\forall g_1, g_2, g_3 \in G, (g_1 + g_2) + g_3 = g_1 + (g_2 + g_3)$
- $\forall g \in G, g + 0 = 0 + g = g$
- $\forall g \in G, \exists -g \in G$ tel que $g + (-g) = -g + g = 0$, où $g_1 + (-g_2)$ sera noté plus simplement $g_1 - g_2$

Dans le cas de la notation multiplicative, le groupe est $(G, ., ^{-1}, 1)$, et on omettra en général l'opérateur "." dans l'écriture :

- $\forall g_1, g_2, g_3 \in G, (g_1 g_2) g_3 = g_1 (g_2 g_3)$
- $\forall g \in G, g1 = 1g = g$
- $\forall g \in G, \exists g^{-1} \in G$ tel que $g g^{-1} = g^{-1} g = 1$

Quand le contexte lève toute ambiguïté, ce qui sera en général le cas, on désignera un groupe $(G, \times, ^{-1}, e)$ simplement par G.

Exemples :

- Les entiers relatifs munis de l'addition forment le groupe abélien $(\mathbb{Z}, +, -, 0)$, simplement appelé $\mathbb{Z}$;
- Les complexes sauf 0 munis du produit de deux nombres complexes forment le groupe abélien $(\mathbb{C}\backslash\{0\}, ., ^{-1}, 1)$, simplement appelé $\mathbb{C}\backslash\{0\}$.

[1] Ces notes, notamment les rappels sur la théorie des groupes, doivent beaucoup à la section 8.1 de *Quantum Computing*, par Mika Hirvensalo, Springer, 2001.

Par contre, l'ensemble $\mathbb{N}$ des entiers naturels, qu'il soit muni de l'addition des entiers ou du produit des entiers, ne forme pas un groupe car, dans les deux cas, il n'y a pas d'inverse dans $\mathbb{N}$.

1.2 Sous-groupes et cosets

Soit un groupe G noté multiplicativement : $(G, ., ^{-1}, 1)$. $H \subseteq G$ est un *sous-groupe* de G si $(H, ., ^{-1}, 1)$ est un groupe. On écrit $H \leqslant G$ pour exprimer que H est un sous-groupe de G. On remarquera que si $H \leqslant G$, alors $\forall h_1, h_2 \in H, h_1 h_2 \in H$, et l'élément neutre de G est nécessairement dans H.

$\forall H \leqslant G$ et $\forall g \in G$, l'ensemble $gH = \{gh | h \in H\}$ est le *coset de H déterminé par g* (en français : *classe à gauche de g modulo H*, mais on préfèrera ici la terminologie anglaise de *coset*). Quand il n'y a pas d'ambiguïté, on parlera simplement d'un coset de H.

On utilisera dans la suite quelques définitions et quelques propriétés (énoncées ici sans preuve) autour de la notion de coset. Soit $H \leqslant G$:

- $\forall h \in H, hH = H$;
- Tous les cosets de H ont $|H|$ éléments ;
- Si $g_1 H = g_2 H$, on dit que g_1 et g_2 sont *congrus modulo H* ;
- Si $g_1 H \neq g_2 H$, alors $g_1 H \cap g_2 H = \varnothing$;
- Les cosets de H forment une partition de G ;
- Le nombre de cosets de H est appelé l'*indice* de H dans G, et est noté $[G : H]$;
- Comme tous les cosets de H ont la même cardinalité, celle de H, on a : $|G| = [G : H].|H|$ (c'est le théorème de Lagrange) ;
- Un sous-groupe $H \leqslant G$ est dit *normal* si, $\forall g \in G$, $h \in H$, on a $ghg^{-1} \in H$;
- Le *produit* de 2 cosets $g_1 H$ et $g_2 H$ d'un sous-groupe normal $H \leqslant G$ est défini comme $(g_1 H)(g_2 H) = (g_1 g_2) H$;
- Le *quotient* de G par un sous-groupe normal $H \leqslant G$, noté G/H, est un groupe dont :
  - Les éléments sont les cosets de H dans G ;
  - L'opération interne est le produit de cosets ;
  - L'inverse est défini par $(gH)^{-1} = g^{-1} H$;
  - L'élément neutre est H.

Considérons par exemple le groupe $\mathbb{Z}$ et définissons $n\mathbb{Z}$, le sous-groupe des entiers relatifs divisibles par n :

$$n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$$

Le coset de $n\mathbb{Z}$ déterminé par $k \in \mathbb{Z}$ est alors :

$$k + n\mathbb{Z} = \{\ldots, k-2n, k-n, k, k+n, k+2n, \ldots\}$$

Deux entiers relatifs k_1 et k_2 sont congrus modulo $n\mathbb{Z}$ si $k_1 + n\mathbb{Z} = k_2 + n\mathbb{Z}$, c'est-à-dire si $k_1 - k_2$ est divisible par n. Enfin, comme $n\mathbb{Z}$ est aussi un sous-groupe normal de $\mathbb{Z}$, on peut définir le groupe quotient $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$: c'est le groupe additif des *entiers modulo n*.

1.3 Ordre d'un élément dans un groupe fini

Si G est un groupe fini, $\forall\, g \in G$, l'ensemble $\{g^0, g^1, g^2, \ldots\}$, où $g^0 = 1, g^1 = g, g^2 = gg, \ldots$, est aussi fini, donc $\forall j, \exists i > j$ tel que $g^i = g^j$, c'est-à-dire $g^{i-j} = 1$: le plus petit entier r tel que $g^r = 1$ est appelé l'*ordre* de g dans G, ce qui est noté $r = \mathrm{ord}(g)$ (notation qui suppose G déterminé sans ambiguïté par le contexte).

On a alors les propriétés et définitions utiles suivantes :

- $\forall l, m, g^{l+mr} = g^l$;
- $\{g^0, g^1, g^2, ...\}$ est un sous-groupe abélien de G, le *groupe cyclique* dont g est le *générateur* ;
- Le groupe cyclique dont g est le générateur est noté $\langle g \rangle$, et ses éléments sont $\{g^0, g^1, g^2, ..., g^{r-1}\}$;
- Comme $r = \mathrm{ord}(g) = |\langle g \rangle|$ divise $|G|$ (théorème de Lagrange), $g^{|G|} = 1$.

1.4 Caractères d'un groupe abélien fini

Soit G un groupe abélien fini, $|G| = n$, noté additivement : $(G, +, -, 0)$. On appelle *caractère* de G tout morphisme $\chi : G \to \mathbb{C}\backslash\{0\}$, c'est-à-dire tel que $\forall\ g_1,\ g_2 \in G,\ \chi(g_1 + g_2) = \chi(g_1)\chi(g_2)$ et $\chi(0) = 1$.

$\forall g \in G$, ce qui s'écrivait multiplicativement $g^{|G|} = 1$ s'écrit additivement $|G|g = ng = 0$, et on a alors $(\chi(g))^n = \chi(ng) = \chi(0) = 1$. Conclusion : la valeur dans $\mathbb{C}\backslash\{0\}$ de tout caractère de G est une racine $n^{\text{ème}}$ de l'unité ($z \in \mathbb{C}$ est une racine $n^{\text{ème}}$ de l'unité si z^n=1).

1.5 Caractères de $\mathbb{Z}_n$ et de $\mathbb{F}_2^n$

Etant donné un groupe abélien additif G, $\forall g \in G$, le groupe cyclique $\{g, 2g, ..., (n-1)g, ng = 0\}$ est isomorphe à $\mathbb{Z}_n$: nous allons considérer dans la suite que $\mathbb{Z}_n$ est le "prototype" des groupes cycliques.

$\forall y \in \mathbb{Z}$, on définit une application $\chi_y : \mathbb{Z} \to \mathbb{C}\backslash\{0\}$ telle que $\chi_y(x) = e^{\frac{2\pi i x y}{n}}$. Puisque $e^{2\pi i} = 1$, χ_y a pour période n. Ainsi, χ_y, initialement défini sur $\mathbb{Z}$, est en fait un morphisme de $\mathbb{Z}_n \to \mathbb{C}\backslash\{0\}$. C'est aussi un caractère de $\mathbb{Z}_n$. En effet :

$$\begin{aligned}\chi_y(x+z) &= e^{\frac{2\pi i y(x+z)}{n}} \\ &= e^{\frac{2\pi i y x}{n}} e^{\frac{2\pi i y z}{n}} \\ &= \chi_y(x)\chi_y(z)\end{aligned}$$

et $\chi_y(0) = 1$.

De plus, comme par définition de χ_y, $\chi_y(x) = \chi_x(y)$, on peut toujours supposer que $y \in \mathbb{Z}_n$. De ce fait, $|\{\chi_y\}| = |\mathbb{Z}_n| = n$. On peut alors montrer que les caractères de $\mathbb{Z}_n$ forment un groupe isomorphe à $\mathbb{Z}_n$. C'est d'ailleurs une propriété générale : le groupe $\hat{G}$ des caractères d'un groupe abélien G est isomorphe à G.

Prenons un exemple. $\mathbb{F}_2 = \{0, 1\}$ est isomorphe à $\mathbb{Z}_2$. Ses caractères sont donc :

$$\begin{aligned}\chi_y(x) &= e^{\frac{2\pi i x y}{2}} \\ &= e^{\pi i x y} \\ &= (-1)^{xy}\end{aligned}$$

pour $x, y \in \mathbb{F}_2$.

$\mathbb{F}_2^n$ a 2^n éléments de la forme $x = (x_1, x_2, ..., x_n)$, pour $x_i \in \{0, 1\}$. On notera que $\forall x \in \mathbb{F}_2^n, \mathrm{ord}(x) = 2$. On obtient facilement les caractères de $\mathbb{F}_2^n$ à partir de ceux de $\mathbb{F}_2$:

$$\begin{aligned}\chi_y(x) &= (-1)^{x_1 y 1}(-1)^{x_1 y 1}...(-1)^{x_1 y 1} \\ &= (-1)^{x.y}\end{aligned}$$

avec $x.y = \sum_{i=1}^{n} x_i y_i$, où la somme est modulo 2.

2 Transformée de Fourier discrète (DFT)

2.1 Espace vectoriel des fonctions $f : G \to \mathbb{C}$

Soit $G = \{g_1, ..., g_n\}$ un groupe abélien fini et f, h des fonctions $G \to \mathbb{C}$. De telles fonctions appartiennent à un espace vectoriel V sur $\mathbb{C}$, où, $\forall g \in G$ et $\forall c \in \mathbb{C}$:

$$(f + h)(g) = f(g) + h(g)$$

$$(c.f)(g) = c.f(g)$$

On considèrera alors que $\forall f : G \to \mathbb{C}$, $f \in V$, et f peut être vue comme un n-uplet $(f(g_1), ...f(g_n))$. L'espace vectoriel V est de dimension $n = |G|$, et n fonctions $e_i, i \in [1, n]$ formeront la *base standard* de V, avec $e_i(g_j) = 1$ si $i = j$, 0 sinon :

$$e_1 = (1, 0, ..., 0)$$

$$e_2 = (0, 1, ..., 0)$$

$$...$$

$$e_n = (0, 0, ..., 1)$$

$\forall f, h \in V$, le produit scalaire est défini de la façon habituelle : $\langle f, g\rangle = \sum_{i=1}^{n}(f(g_i)^*)h(g_i)$, ce qui permet de définir la norme de f : $\| f \| = \sqrt{\langle f, f\rangle}$. On vérifie alors facilement que la base standard $E = \{e_1, ..., e_n\}$ est une base orthonormée dans laquelle on peut écrire $f \in V$ sous la forme $f = (f_1, ..., f_n), f_i \in \mathbb{C}$.

2.2 DFT de $f : G \to \mathbb{C}$

Mais les caractères du groupe abélien fini G permettent de définir une autre base de ce même espace vectoriel V. En effet, soient χ_i et χ_j deux caractères de G. D'abord, ce sont bien des fonctions $G \to \mathbb{C}$, donc $\chi_i, \chi_j \in V$. On prouve ensuite (preuve omise ici) que χ_i et χ_j sont orthogonaux :

$$\langle \chi_i, \chi_j\rangle = \begin{cases} 0 & \text{si } i \neq j \\ n & \text{si } i = j \end{cases}$$

Comme $|G| = n$, il y a n caractères distincts de G, qui sont tous de norme $\sqrt{n}$. On peut normaliser χ_i pour définir $\mathcal{B}_i = \frac{\chi i}{\sqrt{n}}$ et établir ainsi une autre base orthonormée de V : $\mathcal{B} = \{\mathcal{B}_1, ..., \mathcal{B}_n\}$, la *base de Fourier* de V, dans laquelle $f : G \to \mathbb{C}$, c'est-à-dire $f \in V$, pourra s'écrire $f = (\hat{f}_1, ..., \hat{f}_n), \hat{f}_i \in \mathbb{C}$.

On a donc désormais deux représentations de $f \in V$, l'une dans la base E :

$$f = f_1 e_1 + ... + f_n e_n, f_i \in \mathbb{C}$$

l'autre dans la base $\mathcal{B}$:

$$f = \hat{f}_1 \mathcal{B}_1 + ... + \hat{f}_n \mathcal{B}_n, \hat{f}_i \in \mathbb{C}$$

La fonction $\hat{f} : G \to \mathbb{C}$ définie par $\hat{f}(g_i) = \hat{f}_i, \forall i \in [1, n]$ est la *transformée de Fourier discrète* (DFT) de f.

Ceci pouvant s'écrire $\hat{f}(g_i) = \langle \mathcal{B}_i, f\rangle$, la DFT de $f : G \to \mathbb{C}$ a donc la forme générale :

$$\hat{f}(g_i) = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} (\chi_i(g_k)^*) f(g_k) \tag{1}$$

Prenons deux exemples, l'un où $G = \mathbb{Z}_n$, l'autre où $G = \mathbb{F}_2^n$. Les caractères de $\mathbb{Z}_n$ ayant la forme $\chi_y(x) = e^{\frac{2\pi i x y}{n}}$, la définition (1) devient :

$$\hat{f}(x) = \frac{1}{\sqrt{n}} \sum_{y \in \mathbb{Z}_n} e^{\frac{-2\pi i x y}{n}} f(y) \tag{2}$$

Dans le cas de $G = \mathbb{F}_2^n$, les caractères sont $\chi_y(x) = (-1)^{xy}$, et la définition (1) devient alors :

$$\hat{f}(x) = \frac{1}{\sqrt{2^n}} \sum_{y \in \mathbb{F}_2^n} (-1)^{xy} f(y) \tag{3}$$

2.3 DFT inverse

La défintion (1) de DFT peut s'écrire sous forme matricielle :

$$\begin{pmatrix} \hat{f}(g_1) \\ \vdots \\ \hat{f}(g_n) \end{pmatrix} = \frac{1}{\sqrt{n}} \begin{pmatrix} \chi_1(g_1)^* & \cdots & \chi_1(g_n)^* \\ \vdots & & \vdots \\ \chi_n(g_1)^* & \cdots & \chi_n(g_n)^* \end{pmatrix} \begin{pmatrix} f(g_1) \\ \vdots \\ f(g_n) \end{pmatrix}$$

On montre (il y a des preuves très élégantes de ceci) que cette matrice est unitaire. Son adjointe (la conjuguée de sa transposée) est donc aussi son inverse, ce qui nous donne :

$$\begin{pmatrix} f(g_1) \\ \vdots \\ f(g_n) \end{pmatrix} = \frac{1}{\sqrt{n}} \begin{pmatrix} \chi_1(g_1) & \cdots & \chi_n(g_1) \\ \vdots & & \vdots \\ \chi_1(g_n) & \cdots & \chi_n(g_n) \end{pmatrix} \begin{pmatrix} \hat{f}(g_1) \\ \vdots \\ \hat{f}(g_n) \end{pmatrix}$$

Ainsi, étant donnée une fonction $f : G \in \mathbb{C}$, on définit sa *transformée de Fourier inverse*, dont l'écriture sous une forme semblable à celle de (1) sera :

$$\tilde{f}(g_i) = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \chi_k(g_i) f(g_k) \tag{4}$$

On note qu'on a évidemment $\hat{\tilde{f}} = \tilde{\hat{f}} = f$. Dans $\mathbb{Z}_n$, la DFT inverse a la forme :

$$\tilde{f}(x) = \frac{1}{\sqrt{n}} \sum_{y \in \mathbb{Z}_n} e^{\frac{2\pi i x y}{n}} f(y) \tag{5}$$

Dans $\mathbb{F}_2^n$, comme $\chi_y(x) = (-1)^{xy}$, il est facile de vérifier que $\tilde{f}(x) = \hat{f}(x)$.

2.4 DFT de $f : G \to \mathbb{C}$ périodique

Soit maintenant une fonction $f : G \to \mathbb{C}$ périodique, de période r : $\forall g \in G, f(g + r) = f(g)$. Sa transformée de Fourier, donnée par (1), peut être réécrite en jouant avec cette périodicité :

$$\begin{aligned} \hat{f}(g_i) &= \frac{1}{\sqrt{n}} \sum_{k=1}^{n} (\chi_i(g_k)^*) f(g_k) \\ &= \frac{1}{\sqrt{n}} \sum_{k=1}^{n} (\chi_i(g_k + r - r)^*) f(g_k + r) \\ &= (\chi_i(-r)^*) \frac{1}{\sqrt{n}} \sum_{k=1}^{n} (\chi_i(g_k + r)^*) f(g_k + r) \\ &= (\chi_i(-r)^*) \hat{f}(g_i) \end{aligned} \tag{6}$$

Conclusion : si f est périodique, de période r, $\hat{f}(g_i) \neq 0$ seulement si $\chi_i(-r) = 1$. Partout ailleurs, puisque $\chi_i(-r)$ n'est jamais nul, $\hat{f}(g_i) = 0$. Ainsi, pour une fonction f : $\mathbb{Z}_n \to \mathbb{C}$ de période r, l'équation (6) s'écrira :

$$\hat{f}(x) = e^{\frac{2\pi i r x}{n}} \hat{f}(x)$$

$\hat{f}(x)$ ne sera donc différent de 0 que lorsque $e^{\frac{2\pi i x r}{n}} = 1$, c'est-à-dire, de façon périodique, pour tous les x multiples de $\frac{n}{r}$, et $\hat{f}(x)$ sera nul partout ailleurs. On conçoit alors l'intérêt de la DFT pour trouver la période r d'une fonction f.

3 Transformée de Fourier quantique (QFT)

3.1 DFT d'un état quantique

Soit $G = \{g_1, g_2, ..., g_n\}$ un groupe abélien fini et $\{\chi_1, \chi_2, ..., \chi_n\}$ les caractères de G. On considère désormais que $\{|g_i\rangle \, | g_i \in G\}$ est une base orthonormée de l'espace des états d'un système quantique $\mathcal{H}$. Tout état $|\psi\rangle$ de $\mathcal{H}$ peut donc s'écrire :

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_i \, |g_i\rangle$$

où $\forall i \in [1, n], \alpha_i \in \mathbb{C}$ et $\sum_{i=1}^{n} |\alpha_i|^2 = 1$.

On peut associer à $|\psi\rangle$ la fonction qui à $g_i \in G$ fait correspondre $\alpha_i \in \mathbb{C}$. Nous n'allons considérer dans la suite que la DFT inverse. En utilisant la définition (4) pour construire cette DFT sur G, on obtient la DFT d'un état de base $|g_i\rangle$:

$$|g_i\rangle \xrightarrow{\text{DFT}} \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \chi_k(g_i) \, |g_k\rangle$$

Par linéarité, la DFT (inverse) de l'état $|\psi\rangle$ est alors :

$$|\psi\rangle \xrightarrow{\text{DFT}} \frac{1}{\sqrt{n}} \sum_{k=1}^{n} (\sum_{i=1}^{n} \chi_k(g_i)\alpha_i) \, |g_k\rangle$$

Il est important de noter, à ce point, que la DFT d'un état quantique, comme toute opération sur un état quantique, opère sur les amplitudes, en général complexes (et inconnaissable par le monde classique), de cet état : les amplitudes de l'état $|\psi\rangle$ fourni en entrée sont les paramètres de la transformation effectuée par la DFT pour construire un nouvel état quantique. Pour que cela soit *quantiquement légal*, cette transformation doit être unitaire, ce qui est bien le cas de la DFT. Mais pour que cela soit *quantiquement intéressant*, il faut aussi qu'il y ait un gain en complexité par rapport à ce que permet le calcul classique.

Les espaces d'états des systèmes quantiques de n qubits sont de dimension 2^n. En calcul classique, pour une DFT définie sur un groupe de cardinalité $|G| = 2^n$, l'application brutale de la définition (le produit d'un vecteur par une matrice) comporte 2^{2n} produits de deux nombres complexes. On sait faire mieux : FFT (Fast Fourier Transform) arrive au même résultat avec $n2^n$ produits complexes.

On va voir que le calcul quantique permet de faire beaucoup mieux, de décomposer la définition de la DFT en un produit (matriciel, tensoriel) d'opérations unitaires primitives sur 1 et 2 qubits, en quantité linéaire en n pour une DFT sur $\mathbb{F}_2^n$, en quantité quadratique en n pour une DFT sur $\mathbb{Z}_{2^n}$. On verra ensuite comment des algorithmes quantiques peuvent exploiter cette chute exponentielle de complexité pour résoudre des problèmes pour lesquels on ne connaît pas d'algorithmes classiques polynomiaux.

3.2 QFT sur $\mathbb{F}_2^n$ est linéaire en n

C'est, de loin, le cas le plus simple, où la seule brique de base est la transformation d'Hadamard :

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

On sait que H transforme $|0\rangle$ en une superposition uniforme :

$$|0\rangle \; —\boxed{H}— \; \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

et que cette même opération effectuée sur n qubits :

$$\begin{array}{ccc} |0\rangle & —\boxed{H}— & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |0\rangle & —\boxed{H}— & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ \vdots & \vdots & \vdots \\ |0\rangle & —\boxed{H}— & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \end{array}$$

est la $n^{\text{ème}}$ puissance tensorielle de l'opération sur 1 qubit :

$$|00...0\rangle \; —\boxed{H^{\otimes n}}— \; (\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle))^{\otimes n}$$

dont le résultat est la superposition uniforme (avec la même amplitude $\frac{1}{\sqrt{2^n}}$) de tous les états de base $|x\rangle \, , \forall x \in [0, 2^n]$:

$$H^{\otimes n} \, |00...0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Mais c'est un cas particulier : quid de $(H^{\otimes n}) \, |x\rangle$ quand $|x\rangle = |x_1 x_2 ... x_n\rangle$ où $\forall i \in [1, n], x_i \in \{0, 1\}$? La réponse est immédiate. Si on réécrit l'effet de H sur 1 qubit $|x\rangle \, , x \in \{0, 1\}$ comme $H \, |x\rangle = \frac{1}{\sqrt{2}} \sum_{z \in \{0,1\}} (-1)^{xz} \, |z\rangle$, l'opération effectuée, qubit par qubit, est alors :

$$\begin{array}{ccc} |x_1\rangle & —\boxed{H}— & \frac{1}{\sqrt{2}} \sum_{z_1 \in \{0,1\}} (-1)^{x_1 z_1} \, |z_1\rangle \\ |x_2\rangle & —\boxed{H}— & \frac{1}{\sqrt{2}} \sum_{z_2 \in \{0,1\}} (-1)^{x_2 z_2} \, |z_2\rangle \\ \vdots & \vdots & \vdots \\ |x_n\rangle & —\boxed{H}— & \frac{1}{\sqrt{2}} \sum_{z_n \in \{0,1\}} (-1)^{x_n z_n} \, |z_n\rangle \end{array}$$

ce qui s'écrit aussi :

$$H^{\otimes n} \, |x_1 ... x_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{z_1 ... z_n \in \{0,1\}^n} (-1)^{x_1 z_1 \oplus ... x_n z_n} \, |z_1 ... z_n\rangle$$

ou encore, avec $|x\rangle = |x_1...x_n\rangle$, $|z\rangle = |z_1...z_n\rangle$, et en adoptant la convention que $x.z = \sum_{x=1}^{n} x_i z_i$, où la somme est modulo 2 :

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{x.z} |z\rangle$$

La transformation d'Hadamard, qu'elle soit sur 1 ou n qubits, parvient donc au même résultat que la transformée de Fourier discrète sur $\mathbb{F}_2^n$. Ce qui est remarquable, c'est que sur n qubits, il suffit de n opérations sur 1 qubit pour effectuer le calcul. C'est le produit tensoriel des espaces d'états qui permet au calcul quantique de réaliser cette transformée de Fourier quantique (QFT) avec une complexité exponentiellement moindre que le calcul classique de la DFT.

3.3 QFT sur $\mathbb{Z}_{2^n}$ est quadratique en n

Les caractères de $\mathbb{Z}_{2^n}$ étant de la forme $\chi_y(x) = e^{\frac{2\pi i x y}{2^n}}$, la DFT (inverse) de $|x\rangle, x \in \mathbb{Z}_{2^n}$, est l'opération :

$$|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i x y}{2^n}} |y\rangle$$

D'autre part, $\forall x \in \mathbb{Z}_{2^n}$, on peut écrire $|x\rangle = |x_{n-1}\rangle |x_{n-2}\rangle ... |x_1\rangle |x_0\rangle, x_i \in \{0,1\}$ (il faut lire $|x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes ... \otimes |x_1\rangle \otimes |x_0\rangle$ mais, pour alléger l'écriture, on omettra les opérateurs $\otimes$ dans cette section).

Lemme 1.

$$\sum_{y=0}^{2^n-1} e^{\frac{2\pi i x y}{2^n}} |y\rangle$$
$$= (|0\rangle + e^{\frac{\pi i x}{2^0}} |1\rangle)(|0\rangle + e^{\frac{\pi i x}{2^1}} |1\rangle)...(|0\rangle + e^{\frac{\pi i x}{2^{n-1}}} |1\rangle) \quad (7)$$

Démonstration. $|y\rangle = |y_{n-1}\rangle |y_{n-2}\rangle ... |y_1\rangle |y_0\rangle$ peut aussi s'écrire $|y\rangle = |u\rangle |y_0\rangle$, où $|u\rangle = |y_{n-1}\rangle |y_{n-2}\rangle ... |y_1\rangle$. On peut alors scinder la somme sur y en 2 termes :

$$\sum_{y=0}^{2^n-1} e^{\frac{2\pi i x y}{2^n}} |y\rangle = \overbrace{\sum_{u=0}^{2^n-1} e^{\frac{2\pi i x.2u}{2^n}} |u\rangle |0\rangle}^{\text{les } y \text{ pairs}}$$
$$+ \overbrace{\sum_{u=0}^{2^n-1} e^{\frac{2\pi i x.2(u+1)}{2^n}} |u\rangle |1\rangle}^{\text{les } y \text{ impairs}}$$
$$= \sum_{u=0}^{2^n-1} e^{\frac{2\pi i x.u}{2^{n-1}}} |u\rangle |0\rangle + \sum_{u=0}^{2^n-1} e^{\frac{2\pi i x.u}{2^{n-1}}} e^{\frac{\pi i x}{2^{n-1}}} |u\rangle |1\rangle$$
$$= (\sum_{u=0}^{2^n-1} e^{\frac{2\pi i x.u}{2^{n-1}}} |u\rangle)(|0\rangle + e^{\frac{\pi i x}{2^{n-1}}} |1\rangle)$$

Suite et fin de la démonstration : par induction sur le premier terme de ce produit. □

La conséquence importante de ce lemme est que la DFT de $|x\rangle$ est un produit tensoriel des états de n qubits : l'état du $l^{\text{ème}}$ qubit, qui était $|x_{n-l}\rangle$ avant la DFT, devient $(|0\rangle + e^{\frac{\pi i x}{2^{l-1}}} |1\rangle)$ après la DFT (pour simplifier l'écriture, on ignore momentanément l'amplitude $\frac{1}{\sqrt{2^n}}$)

Considérons donc d'abord le $l^{\text{ème}}$ terme à partir de la gauche du développement (7) : $(|0\rangle + e^{\frac{\pi i x}{2^{l-1}}} |1\rangle)$. En développant x bit à bit, le coefficient de $|1\rangle$ dans ce terme devient :

$$e^{\pi i \frac{2^{n-1}x_{n-1}+...+2^l x_l + 2^{l-1}x_{l-1} + 2^{l-2}x_{l-2}+...+2x_1+x_0}{2^{l-1}}}$$

On note qu'une première partie de ce développement, à gauche, est composée de facteurs qui sont tous de la forme $e^{2^r \pi i x_k}$ avec $r \geq 1$, c'est-à-dire qu'ils ont tous la valeur 1 :

$$e^{\pi i \frac{2^{n-1}x_{n-1}+...+2^l x_l}{2^{l-1}}} = 1$$

Le facteur suivant est $e^{\pi i \frac{2^{l-1}x_{l-1}}{2^{l-1}}} = (-1)^{x_{l-1}}$. Le coefficient de $|1\rangle$ dans le $l^{\text{ème}}$ terme du développement (7), c'est-à-dire dans l'état du $l^{\text{ème}}$ qubit après application de la DFT à $|x\rangle$, se réduit donc à :

$$(-1)^{x_{l-1}} e^{\pi i \frac{2^{l-2}x_{l-2}+...+2^{l-k}x_{l-k}+...+2x_1+x_0}{2^{l-1}}}$$
$$= (-1)^{x_{l-1}} e^{\frac{\pi i x_{l-2}}{2^1}} ... e^{\frac{\pi i x_{l-k}}{2^{k-1}}} ... e^{\frac{\pi i x_1}{2^{l-2}}} e^{\frac{\pi i x_0}{2^{l-1}}} \quad (8)$$

On va maintenant voir comment construire un tel état pour le $l^{\text{ème}}$ qubit en opérant sur tout ou partie des n qubits qui sont initialement dans l'état $|x\rangle$. Pour simplifier la suite, commençons par renverser l'écriture de $|x\rangle$:

$$|x\rangle = |x_0\rangle ... |x_{l-k-1}\rangle ... |x_{l-2}\rangle |x_{l-1}\rangle ... |x_{n-1}\rangle$$

Considérons alors le $l^{\text{ème}}$ qubit à partir de la gauche. Il est dans l'état $|x_{l-1}\rangle$, Appliquer H, la transformation d'Hadamard, à ce qubit modifie l'état du système quantique que forment ces n qubits (on ignore l'amplitude $\frac{1}{\sqrt{2}}$ que cela introduit) :

$$|x_0\rangle ... |x_{l-k-1}\rangle ... |x_{l-2}\rangle (|0\rangle + (-1)^{x_{l-1}} |1\rangle)... |x_{n-1}\rangle$$

Cette opération dote le coefficient de $|1\rangle$ dans l'état du $l^{\text{ème}}$ qubit à partir de la gauche d'un premier facteur, $(-1)^{x_{l-1}}$. Selon (8), le facteur suivant dépend de l'état $|x_{l-2}\rangle$ du $(l-1)^{\text{ème}}$ qubit : si $|x_{l-2}\rangle = |1\rangle$, il faut insérer $e^{\frac{\pi i}{2}}$ dans le coefficfient de $|1\rangle$, l'état du $l^{\text{ème}}$ qubit devenant alors $(|0\rangle + (-1)^{x_{l-1}} e^{\frac{\pi i}{2}} |1\rangle)$, sinon, si $|x_{l-2}\rangle = |0\rangle$, aucun facteur ne doit être inséré.

Ce même raisonnement s'applique à tous les facteurs qui composent le coefficient de $|1\rangle$ dans l'état du $l^{\text{ème}}$ qubit défini par (8), en considérant successivement $|x_{l-3}\rangle$, ..., $|x_{l-k-1}\rangle$..., $|x_1\rangle$, $|x_0\rangle$: on introduit $e^{\frac{\pi i}{2^k}}$ dans le coefficient de $|1\rangle$ dans l'état du $l^{\text{ème}}$ qubit si et seulement si $|x_{l-k-1}\rangle = |1\rangle$.

Pour chaque qubit ainsi considéré, le $(l-k)^{\text{ème}}$ par exemple, qui est dans l'état $|x_{l-k-1}\rangle$, ceci correspond à une opération unitaire sur deux qubits, le $l^{\text{ème}}$ et le $(l-k)^{\text{ème}}$. L'effet de cette opération (ajouter le facteur $e^{\frac{\pi i}{2^k}}$ au coefficient de $|1\rangle$ dans l'état du $l^{\text{ème}}$ qubit) sera conditionné par l'état ($|1\rangle$ ou $|0\rangle$) du $(l-k)^{\text{ème}}$ qubit. Appellons R_θ l'opération unitaire sur un qubit :

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

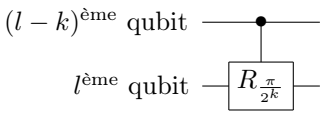
L'effet de cette opération est :

$$R_\theta(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + e^{i\theta}\beta|1\rangle$$

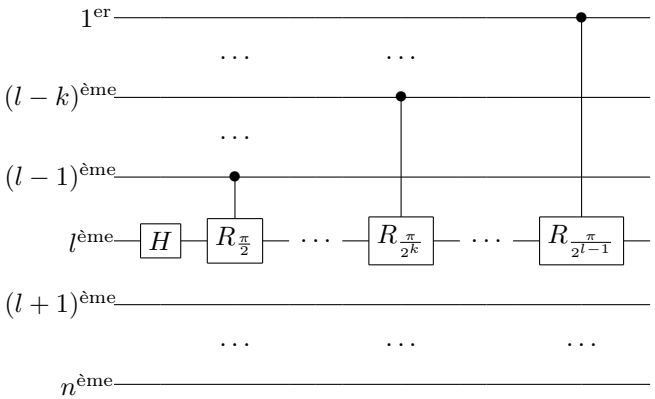
L'opération conditionnelle recherchée est donc l'opération *Controlled* R_θ agissant sur le $l^{\text{ème}}$ qubit sous le contrôle du $(l-k)^{\text{ème}}$ qubit, avec $\theta = \frac{\pi}{2^k}$:

$$CR_\theta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\frac{\pi}{2^k}} \end{pmatrix}$$

On représentera cette opération comme une porte quantique de la façon suivante :



L'état du $l^{\text{ème}}$ qubit est donc modifié successivement par $H, CR_{\frac{\pi}{2}}, ... CR_{\frac{\pi}{2^k}}, ...$ etc, jusqu'à $CR_{\frac{\pi}{2^{l-1}}}$ de la façon suivante :

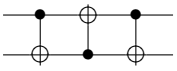


Le même genre de transformation est appliqué à tous les qubits :

- H sur le 1^{er} qubit ;
- H et $CR_{\frac{\pi}{2}}$ sur le $2^{\text{ème}}$ qubit ;
- ...
- $H, CR_{\frac{\pi}{2}}, ... CR_{\frac{\pi}{2^{n-1}}}$ sur le $n^{\text{ème}}$ qubit.

Complexité : il y a 1 opération sur le 1^{er} qubit, 2 sur le $2^{\text{ème}}$, ... et n sur le $n^{\text{ème}}$, soit en tout $\frac{n(n+1)}{2}$ opérations : QFT sur $\mathbb{Z}_{2^n}$ est quadratique en n.

Il reste toutefois une dernière transformation à faire. En effet, pour produire comme résultat final la transformée de Fourier sur les n qubits selon le lemme 1, le résultat qui vient d'être obtenu doit être à la $l^{\text{ème}}$ position dans l'écriture binaire directe de $|x\rangle$, alors qu'il a été construit à la $l^{\text{ème}}$ position dans l'écriture binaire inverse. Il faut donc, pour tout $l \in [1, n]$ échanger les états des $l^{\text{ème}}$ et $(n-l+1)^{\text{ème}}$ qubits. Ceci a un coût linéaire, chaque échange pouvant être effectué par une séquence de 3 opérations $CNot$:



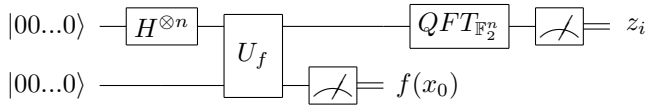
4 Algorithmes

4.1 Algorithme de Simon

Soit $f : \{0,1\}^n \to \{0,1\}^n$ une fonction telle que $f(x) = f(y)$ si et seulement si, soit $y = x$, soit $y = x \oplus r$, où $r \in \{0,1\}^n$ et $\oplus$ est l'addition modulo 2 bit à bit. Le problème est de déterminer cette période r avec probabilité de succès $\geq \frac{3}{4}$, et avec aussi peu de requêtes que possible à l'oracle f.

En calcul classique, après m requêtes à f avec des x_i différents, m réponses $f(x_1), f(x_2), ..., f(x_m)$ sont connues. Pour déterminer r, il faut qu'il y ait parmi ces m tirages un couple (i,j), $i \neq j$, tel que $f(x_i) = f(x_j)$, car alors $x_j = x_i \oplus r$, c'est-à-dire $x_i \oplus x_j = r$. Parmi ces m tirages, il y a $C_2^m \approx \frac{m^2}{2}$ paires (x_i, x_j) différentes. Comme il y a 2^n paires (x,y) dans $\{0,1\}^n$ telles que $x \oplus y = r$, la probabilité d'avoir obtenu l'une d'entre elles après m tirages est $\frac{C_2^n}{2^n} \approx \frac{m^2}{2^{n+1}}$. Une probabilité de succès $> \frac{1}{2}$ exige alors $\frac{m^2}{2^{n+1}} > \frac{1}{2}$, c'est-à-dire $m > 2^{\frac{n}{2}}$. En menant la preuve jusqu'au bout, ce qu'on ne fera pas ici, on parvient à une borne inférieure $\Omega(2^{\frac{n}{2}})$ pour ce problème. Conclusion : le problème de Simon n'est pas dans la classe BPP (Bounded Probabilistic Polynomial) relative à un oracle.

En calcul quantique, l'oracle f sera une transformation unitaire U_f qui opèrera sur deux registres de n qubits chacun. Initialement, les deux registres sont dans l'état $|00...0\rangle$. Avant la transformation U_f, tous les éléments du domaine de définition $\{0,1\}^n$ de f sont superposés dans le premier registre par une application de la transformation $H^{\otimes n}$. L'état du système quantique formé de ces deux registres est alors $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle$. Après la transformation U_f, cet état devient l'état intriqué $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$.



Le calcul se poursuit par une mesure du deuxième registre dans la base standard. Etant donnée la défintion de la fonction f, chaque valeur $f(x)$ a deux antécédants dans $\{0,1\}^n$, x et $x \oplus r$, et la fonction f prend 2^{n-1} valeurs différentes dans $\{0,1\}^n$. La mesure du deuxième registre retourne donc l'une de ces valeurs, $f(x_0)$, choisie parmi toutes les autres avec une probabilité $\frac{1}{2^{n-1}}$.

Toutefois, ni cette valeur $f(x_0)$ ni ce x_0 choisis aléatoirement n'ont d'intérêt pour la suite du calcul. L'effet intéressant de cette mesure est dû à l'état intriqué des deux registres avant la mesure : comme l'état du deuxième est projeté sur $|f(x_0)\rangle$, celui du premier devient $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus r\rangle)$, la superposition des deux antécédants de x_0.

Une QFT sur $\mathbb{F}_2^n$ est alors appliquée au premier registre dont l'état devient :

$$\frac{1}{\sqrt{2^{n+1}}}\Big(\sum_{z\in\{0,1\}^n}(-1)^{x_0\cdot z}|z\rangle + \sum_{z\in\{0,1\}^n}(-1)^{(x_0\oplus r)\cdot z}|z\rangle\Big)$$
$$=\frac{1}{\sqrt{2^{n+1}}}\sum_{z\in\{0,1\}^n}\left[(-1)^{x_0\cdot z}+(-1)^{(x_0\oplus r)\cdot z}\right]|z\rangle$$

Or, $\forall z$ tel que $r.z = 1, (-1)^{x_0\cdot z} + (-1)^{(x_0\oplus r)\cdot z} = 0$. Ne restent donc dans l'état du premier registre que les $|z\rangle$ tels que $r.z = 0$:

$$\frac{1}{\sqrt{2^{n-1}}}\sum_{z:r.z=0}(-1)^{x_0\cdot z}|z\rangle$$

Le premier registre est enfin mesuré dans la base standard. Cette mesure retourne un z_1 tel que $r.z_1 = 0$, c'est-à-dire $r_1 z_{1_1} \oplus r_2 z_{1_2} \oplus ... \oplus r_n z_{1_n} = 0$.

On itère alors l'ensemble du calcul quantique, depuis l'initialisation à $|00...0\rangle$ des deux registres jusqu'à la mesure du premier registre : chaque itération effectue une requête à l'oracle U_f et produit un z_i tel que $r_1 z_{i_1} \oplus r_2 z_{i_2} \oplus ... \oplus r_n z_{i_n} = 0$, c'est-à-dire une équation où les coefficients z_{i_j} sont connus et les n inconnues sont les bits r_i qui forment la période r recherchée. Pour déterminer r, on a donc besoin d'établir n équations linéairement indépendantes de cette forme. Pour cela, il faudra effectuer des itérations qui fourniront n z_i indépendants, c'est-à-dire tels qu'aucun d'entre eux n'est une somme modulo 2 bit à bit de tout ou partie des autres.

La complexité quantique en requêtes du problème de Simon est donc le nombre d'itérations qui permettont d'extraire ces n z_i indépendants. Supposons que l'on aie déjà trouvé m z_i indépendants. A chaque itération, après la requête à U_f et la mesure du deuxième registre, la QFT superpose 2^{n-1} z_i dans le premier registre. Lors de la mesure de ce registre, ils sont équiprobables. Parmi eux, il y en a 2^m qui *ne sont pas* linéairement indépendants des m déjà trouvés, ce qui donne la probabilité d'obtenir un $(m+1)^{\text{ème}}$ z_i indépendant des m précédents :

$$\alpha_m = 1 - \frac{2^m}{2^{n-1}}$$

Le nombre espéré d'itérations pour le trouver sera alors :

$$\frac{1}{\alpha_m} = \frac{1}{1-\frac{2^m}{2^{n-1}}} \approx 1 + \frac{2^m}{2^{n-1}} \approx 1$$

Il faudra donc de l'ordre de n itérations pour trouver n z_i indépendants avec une probabilité proche de 1. Première conclusion : le problème de Simon est dans la classe BQP (Bounded Quantum Polynomial) relative à un oracle. Deuxième conclusion : relativement à un oracle, BPP $\neq$ BQP.

4.2 Algorithme de Shor

4.2.1 Le groupe multiplicatif $\mathbb{Z}_P^*$ des entiers modulo P

Dans le groupe $\mathbb{Z}_P = \mathbb{Z}/P\mathbb{Z}$, $P \in \mathbb{N}$, l'opération est l'addition de cosets. Mais on montre facilement que le produit de cosets $(k_1 + P\mathbb{Z})(k_1 + P\mathbb{Z}) = (k_1 k_2 + P\mathbb{Z})$ est aussi une opération bien définie pour laquelle le coset $(1 + P\mathbb{Z})$ est l'élément neutre.

Cependant, les cosets $(k + P\mathbb{Z})$ ne forment pas un groupe multiplicatif, car certains d'entre eux n'ont pas d'inverse, ceux pour lesquels $\gcd(k, P) > 1$. En effet, supposons que $(k+P\mathbb{Z})$ a un inverse $(k'+P\mathbb{Z})$. Puisqu'alors $(kk' + P\mathbb{Z}) = (1 + P\mathbb{Z})$, kk' et 1 sont congrus modulo P, c'est-à-dire que $kk' - 1$ est divisible par P, et *a fortiori* par $\gcd(k, P)$ qui, divisant ainsi à la fois k et $kk' - 1$, doit aussi diviser 1. Contradiction, car $\gcd(k, P) > 1$.

Pour obtenir un groupe multiplicatif d'entiers modulo P, il faudra donc se débarasser des cosets $(k + P\mathbb{Z})$ qui « gênent », c'est-à-dire ceux pour lesquels $\gcd(k, P) > 1$. On appelle $\mathbb{Z}_P^*$ l'ensemble des cosets qui restent :

$$\mathbb{Z}_P^* = \{(k + P\mathbb{Z}) | \gcd(k, P) = 1\}$$

Si tout coset dans $\mathbb{Z}_P^*$ a un inverse, alors $\mathbb{Z}_P^*$ sera le groupe multiplicatif des entiers modulo P. Pour montrer cela, on utilise l'identité de Bezout (qu'on ne prouvera pas ici) :

$$\forall x, y \in \mathbb{N}, \exists a, b \in \mathbb{Z} \text{ tel que } ax + by = \gcd(x, y)$$

Tout coset $(k + P\mathbb{Z})$ tel que $\gcd(k, P) = 1$ a-t-il donc bien un inverse ? Soient $a, b \in \mathbb{Z}$ tels que $ak + bP = 1$: $ak - 1 = bP$ est alors divisible par P, c'est-à-dire que ak et 1 sont congrus modulo P. Donc $(ak+P\mathbb{Z}) = (1+P\mathbb{Z})$, ce qui s'écrit aussi $(a+P\mathbb{Z})(k+P\mathbb{Z}) = (1+P\mathbb{Z})$: le coset $(a + P\mathbb{Z})$ est l'inverse multiplicatif de $(k + P\mathbb{Z})$.

Le nombre d'entiers $k \in \mathbb{Z}_P$ tels que $\gcd(k, P) = 1$ est appelé le *nombre d'Euler* $\varphi(P) = |\mathbb{Z}_P^*|$, et le *théorème d'Euler* énonce une propriété vue précédemment dans le cas général des groupes finis : si $\gcd(a, P) = 1$, alors $a^{\varphi(P)} = 1$ dans $\mathbb{Z}_P^*$ (en effet, d'après le théorème de Lagrange, l'ordre de $a, \forall a \in \mathbb{Z}_P^*$, divise $\varphi(P)$). A titre anecdotique, citons un cas particulier, connu sous le nom de *petit théorème de Fermat* : si P est premier, alors $a^{(P-1)} = 1$ modulo P.

4.2.2 Factorisation de P réduite à la recherche de l'ordre d'un élément dans $\mathbb{Z}_P^*$

Soit $P \in \mathbb{N}$, que l'on supposera impair. Le problème de la factorisation de P est de trouver la décomposition de P en facteurs premiers. Il suffit de savoir trouver un facteur de P, et on saura alors trouver récursivement tous les autres. Le meilleur algorithme classique connu pour factoriser P est exponentiel, en $\mathcal{O}(e^{p^{\frac{1}{3}}(\log p)^{\frac{2}{3}}})$, où $p = \log P$, le nombre de chiffres pour écrire P, est la taille du problème.

Le problème de la factorisation de P peut être réduit à celui de la recherche de l'ordre d'un élément dans $\mathbb{Z}_P^*$, le groupe multiplicatif des entiers modulo P.

D'abord, il est facile de voir que s'il existe un algorithme polynomial pour trouver une solution non triviale (c'est-à-dire $x \neq \pm 1 \bmod P$) à l'équation $x^2 = 1 \bmod P$, alors il existe un algorithme polynomial pour factoriser P. En effet, comme cette équation peut aussi s'écrire $(x+1)(x-1) = 0 \bmod P$, si s est une solution non triviale, alors soit $(s+1)$, soit $(s-1)$, soit les deux, ont avec P un diviseur commun, qui peut être trouvé en temps polynomial avec l'algorithme d'Euclide.

Ensuite, soit $a \in \mathbb{Z}_P^*$, c'est-à-dire $1 \leq a < P$ et $\gcd(a, P) = 1$. On appelle ordre de a modulo P, l'ordre de a dans $\mathbb{Z}_P^*$, c'est-à-dire le plus petit entier r tel que $a^r = 1 \bmod P$. Connaisant a, si on sait trouver r et si r est pair, alors $a^r = 1 \bmod P$ peut aussi s'écrire :

$$(a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1) = 0 \bmod P$$

Si maintenant $a^{\frac{r}{2}} \neq -1 \bmod P$ (r étant le plus petit entier tel que $a^r = 1 \bmod P$, on a nécessairement $a^{\frac{r}{2}} \neq 1 \bmod P$), alors soit $\gcd(a^{\frac{r}{2}} + 1, P)$, soit $\gcd(a^{\frac{r}{2}} - 1, P)$, soit les deux, sont des facteurs de P. La factorisation de P est ainsi réduite à la recherche de l'ordre d'un entier $a \in \mathbb{Z}_P^*$. La parité et la non trivialité de r ($a^{\frac{r}{2}} \neq -1 \bmod P$), conditions du succès, dépendront du choix de a. On a donc un algorithme en trois étapes :

(1) Choisir au hasard a tel que $1 \leq a < P$. Si $\gcd(a, P) > 1$, stop, car c'est un facteur de P ! Sinon, on a bien $a \in \mathbb{Z}_P^*$.

(2) Appeler la procédure qui détermine r, l'ordre de a modulo P.

(3) Si r est pair et si $\frac{r}{2} \neq -1 \bmod P$, alors calculer $\gcd(a^{\frac{r}{2}} + 1, P)$ et $\gcd(a^{\frac{r}{2}} - 1, P)$ et retenir celui, ou ceux, qui sont des facteurs non triviaux de P. Sinon, échec, recommencer avec un nouvel a.

Reste à s'assurer que cet algorithme parvient à une solution avec une probabilité supérieure à $\frac{1}{2}$.

Si P a k facteurs premiers différents, on montre (on ne le fera pas ici) que la probabilité que l'ordre r de a soit impair, pour un a choisi uniformément dans $\mathbb{Z}_P^*$, est au plus égale à $\frac{1}{2^k}$. De même, si r est pair, la probabilité que $\frac{r}{2} \neq -1 \bmod P$ est elle aussi au plus égale à $\frac{1}{2^k}$. On en déduit que pour $a \in \mathbb{Z}_P^*$ chosi avec une probabilité uniforme, la probabilité que r satisfasse les conditions de parité et de non trivialité est au moins de $(1 - \frac{1}{2^k})^2$, ce qui est supérieur ou égal à $\frac{9}{16}$ si P a au moins 2 facteurs premiers différents.

Dans cet algorithme, les pas (1) et (3) sont polynomiaux, en $\mathcal{O}(p^3)$, où $p = \log P$ (algorithme d'Euclide pour $\gcd(x, y)$). Il reste a trouver, pour le pas (2), une procédure pour déterminer l'ordre de a. Pour cela, on définit une fonction :

$$\begin{aligned} f_a : \mathbb{Z} &\to \mathbb{Z}_P^* \\ k &\mapsto a^k \bmod P \end{aligned}$$

Cette fonction est périodique, de période r, l'ordre de a modulo P. En effet :

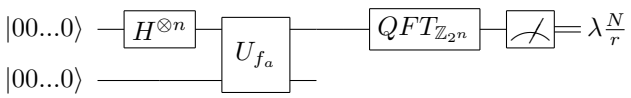
$$\begin{aligned} f_a(k + r) &= a^{k+r} \bmod P \\ &= a^k a^r \bmod P = f_a(k) \end{aligned}$$

Déterminer l'ordre de a est ainsi réduit à trouver la periode r de cette fonction.

4.2.3 Trouver la période de $f_a(k) = a^k \bmod P$ avec QFT sur $\mathbb{Z}_{2^n}$

La fonction f_a sera calculée par un opérateur unitaire U_{f_a} qui opèrera sur deux registres, le premier de n qubits pour les arguments de la fonction dans $\mathbb{Z}$, qu'on restreindra donc à $\mathbb{Z}_N$ pour un $N = 2^n$ judicieusement choisi, et le deuxième de q qubits pour les résultats dans $\mathbb{Z}_P^*$. La valeur de q sera choisie de façon à ce que 2^q soit la plus petite puissance de 2 supérieure à P, le nombre à factoriser. On choisira n pour que $N = 2^n$ soit supérieur à P, et suffisamment grand pour qu'on soit sûr que la période de f_a puisse apparaître, par exemple tel que $P^2 \leq N < 2P^2$. Pour simplifier (beaucoup) les raisonnements et les calculs dans la suite, on fera l'hypothèse (très irréaliste, mais qui ne modifie rien dans les principes essentiels de l'algorithme de Shor) que la période r qui est cherchée divise N.

Comme dans l'algorithme de Simon, les deux registres sont initialement chacun dans l'état $|00\ldots0\rangle$, puis toutes les valeurs du domaine de définition $\mathbb{Z}_{2^n}$ de f_a sont superposées dans le premier registre par $H^{\otimes n}$:



Après la transformation U_{f_a}, l'état est :

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |a^x\rangle$$

Dans la présentation de l'algorithme de Simon au paragraphe 4.1, l'opération suivante était une mesure du

deuxième registre dans la base standard. On pourrait faire la même chose ici. Mais ce serait uniquement pour des raisons pédagogiques. En effet, grâce à l'intrication entre les deux registres, cela ne ferait que simplifier l'état du premier registre pour le réduire à la superposition des antécédants par f_a de la valeur obtenue par la mesure du deuxième registre. Si le plus petit des antécédants par f_a de cette valeur est x_0, alors l'état du premier registre serait réduit à :

$$\frac{1}{\sqrt{\frac{2^n}{r}}} \sum_{k=0}^{\frac{2^n}{r}-1} |x_0 + kr\rangle$$

L'état ainsi obtenu serait donc une superposition périodique dans le premier registre, de période r, et c'est cet état qui serait ensuite transformée par $QFT_{\mathbb{Z}_{2^n}}$. Mais il n'est pas nécessaire de faire cette mesure préalable du deuxième registre. En effet, avec ou sans cette mesure, l'état des deux registres obtenu après l'application de $QFT_{\mathbb{Z}_{2^n}}$ au premier registre aura le profil suivant (voir le paragraphe 2.4 sur la DFT des fonctions périodiques pour s'en convaincre, et rappelons l'hypothèse que r divise 2^n) :

- amplitude $\frac{1}{\sqrt{r}}$ pour les $x \in \mathbb{Z}_{2^n}$ multiples de $\frac{2^n}{r}$;
- amplitude 0 pour toutes les autres valeurs de x.

Une mesure du premier registre produira donc, avec probabilité $\frac{1}{r}$, une valeur $v \in \{0, \frac{2^n}{r}, 2\frac{2^n}{r}, \ldots, (r-1)\frac{2^n}{r}\}$:

$$v = \lambda \frac{2^n}{r},\ \lambda \in [0, r-1]$$

Connaissant v et n, on trouvera alors r en utilisant encore une fois l'algorithme d'Euclide pour mettre $\frac{v}{2^n} = \frac{\lambda}{r}$ sous forme de fraction irréductible. Mais cela ne permettra de déterminer r que si λ et r sont premiers entre eux, sinon on obtient un facteur de r. Il faut donc que la mesure produise une valeur v telle que $\gcd(\lambda, r) = 1$, c'est-à-dire telle que $\lambda \in \mathbb{Z}_r^*$. La probabilité d'obtenir une telle valeur est $\frac{\varphi(r)}{r}$, où $\varphi(r)$ est le nombre d'Euler, ce qui vérifie (preuve omise ici) :

$$\frac{\varphi(r)}{r} > \frac{1}{\log\log r} > \frac{1}{\log\log P}$$

Analyse de la complexité de l'algorithme de Shor :

- Le pas (1), qui fait appel à l'algorithme d'Euclide, est en $\mathcal{O}(p^3)$, avec $p = \log P$;
- Le pas (2), U_{f_a} en $\mathcal{O}(n)\mathcal{O}(p^2)$, puis $QFT_{\mathbb{Z}_{2^n}}$ en $\mathcal{O}(n^2)$, est en $\mathcal{O}(p^3)$ (on avait choisi $2^n < 2P^2$) ;
- Le pas (3), qui fait appel à l'algorithme d'Euclide, est en $\mathcal{O}(p^3)$.

Le nombre d'essais espérés pour mesurer une valeur $v = \lambda\frac{2^n}{r}$ telle que $\gcd(\lambda, r) = 1$ étant $\log p$, la factorisation d'un entier P par l'algorithme de Shor est donc en $\mathcal{O}(p^3 \log p)$.