Transformée de Fourier discrète

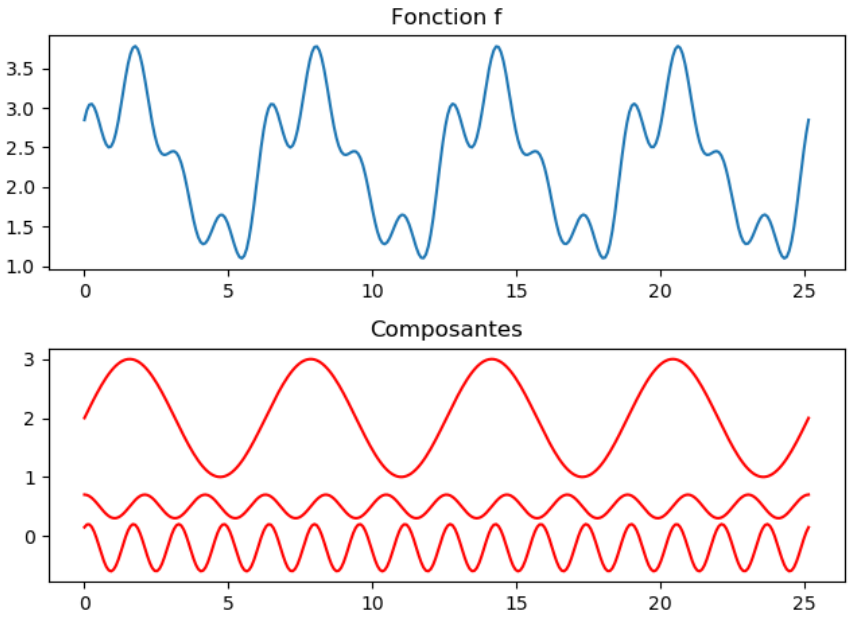
Nous revenons sur l'outil principal de l'algorithme de Shor : la transformée de Fourier. Nous expliquons comment elle est construite, comment la réaliser par un circuit quantique et quelles sont ses autres applications.

1. Comprendre la transformée de Fourier

La transformée de Fourier, c'est la magie de pouvoir récupérer chacune des couleurs qu'on a mélangées dans un pot de peinture !

1.1. Les transformées de Fourier

Voici un exemple : on prend trois fonctions sinusoïdales f_1, f_2, f_3 (figure du bas) que l'on additionne pour obtenir une fonction compliquée $f(x) = f_1(x) + f_2(x) + f_3(x)$ (figure du haut). Alors la transformée de Fourier permet de retrouver chacune des composantes f_1, f_2, f_3 à partir de f.



Le monde de Fourier est assez vaste, voici un petit lexique :

- la transformée de Fourier concerne une fonction quelconque, elle se calcule à l'aide d'une intégrale,
- les séries de Fourier s'appliquent à des fonctions périodiques (comme ci-dessus),
- la transformée de Fourier discrète s'applique à une liste de nombres réels ou complexes,
- la transformée de Fourier discrète quantique est une variante de la précédente et transforme un qubit en un autre qubit.

1.2. La transformée de Fourier discrète classique

Nous allons expliquer le principe de la transformée de Fourier discrète (non quantique) et justifier comment elle permet de retrouver les périodes.
Voici la définition de la transformée de Fourier discrète. Soit $(x_0,\dots,x_{n-1})$ une suite de n nombres (ils peuvent être complexes mais pour nos exemples ce seront des réels). La transformée de Fourier discrète de $(x_0,\dots,x_{n-1})$ est la liste de nombres complexes $(X_0,\dots,X_{n-1})$ où chaque X_k est défini par :

$$\boxed{X_k = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} x_j e^{-2i\pi \frac{k\cdot j}{n}}.}$$

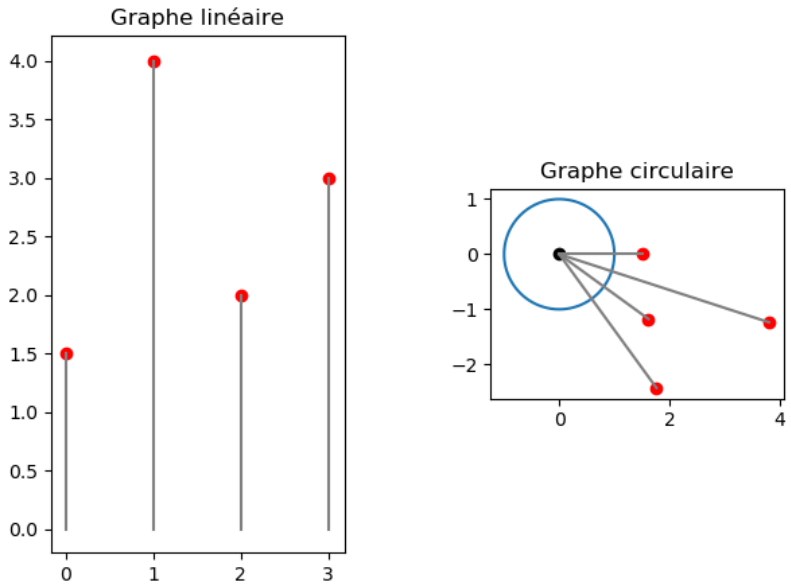
Si on note $\omega = e^{\frac{2i\pi}{n}}$ et $\omega^* = e^{-\frac{2i\pi}{n}}$, alors

$$X_k = \frac{1}{\sqrt{n}} \left(x_0(\omega^*)^{k\cdot 0} + x_1(\omega^*)^{k\cdot 1} + \cdots + x_{n-1}(\omega^*)^{k\cdot(n-1)} \right).$$

La formule n'est donc pas si difficile à comprendre. Mais pourquoi vouloir transformer une suite de nombres par une opération aussi compliquée ?

1.3. Construction de la transformée de Fourier discrète

L'idée de la construction de la transformée de Fourier est très simple ! Nous avons des données x_j (pour nous $x_j \in \mathbb{R}$). Nous représentons traditionnellement x_j sous la forme d'un point (où l'ordonnée du point est la valeur x_j, les points étant placés de gauche à droite). Mais on peut aussi utiliser une représentation circulaire : chaque point est à une distance x_j de l'origine, et les points sont répartis dans le sens des aiguilles d'une montre.



Les données sont $(x_0, x_1, x_2, x_3) = (1.5, 4, 2, 3)$.
Figure de gauche : les données sont présentées sous la forme de points (j, x_j).
Figure de droite les mêmes données sous forme d'écriture polaire : l'angle est proportionnel à j *et le rayon est* x_j.

Le point clé de la représentation circulaire est qu'on peut répartir les données sur un angle plus ou moins grand. Notons $2\pi t$ l'angle total d'étalement, alors plus précisément l'angle entre deux données est $\frac{2\pi t}{n}$.

Comment est calculée cette représentation circulaire ? La donnée x_j correspond au point du plan situé à distance x_j de l'origine et faisant un angle $-\frac{2\pi t}{n} \times j$ avec l'horizontale : c'est donc le nombre complexe $z_j = x_j e^{-2i\pi \frac{t}{n} j}$. On voit apparaître le terme de la définition de la transformée de Fourier.
Voici différents étalements possibles, ils correspondent à différentes valeurs du paramètre t. Pour $t = \frac{1}{4}$ les données sont réparties sur un quart de cercle, pour $t = \frac{1}{2}$ un demi-cercle, pour $t = 1$ le cercle entier et pour $t > 1$ les données s'enroulent plusieurs fois autour du cercle.

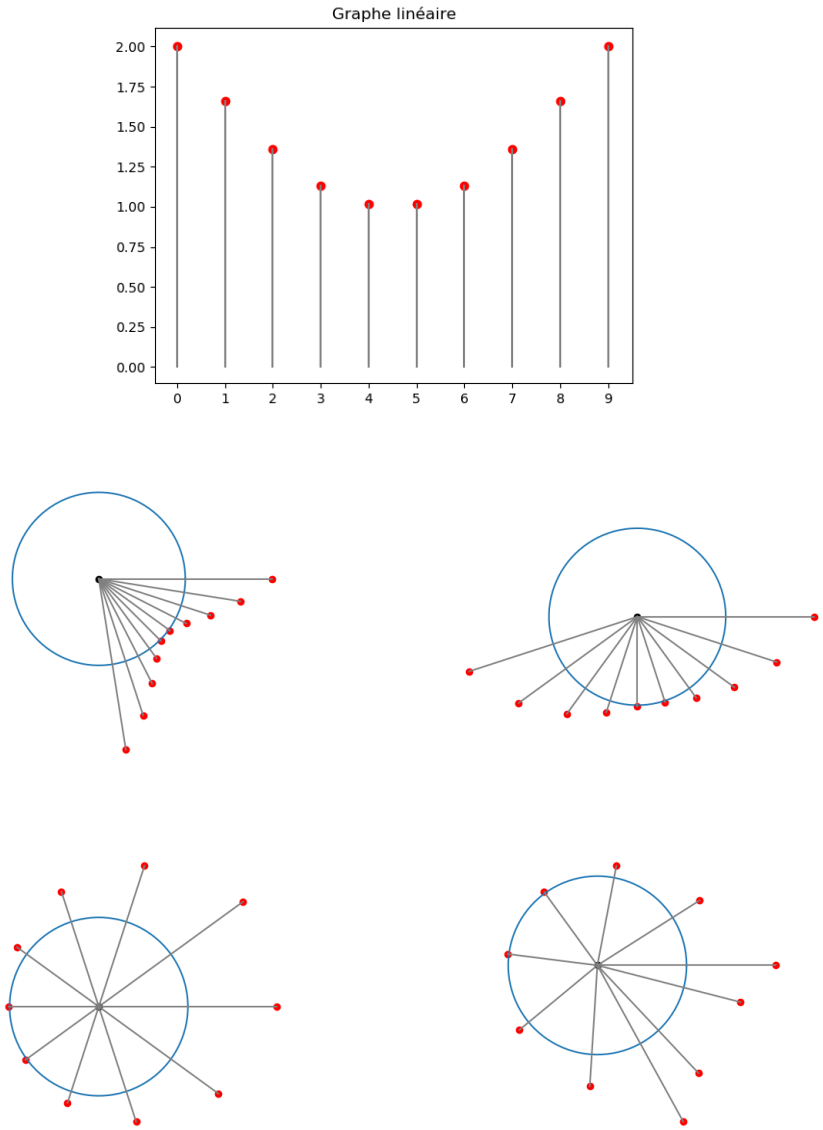
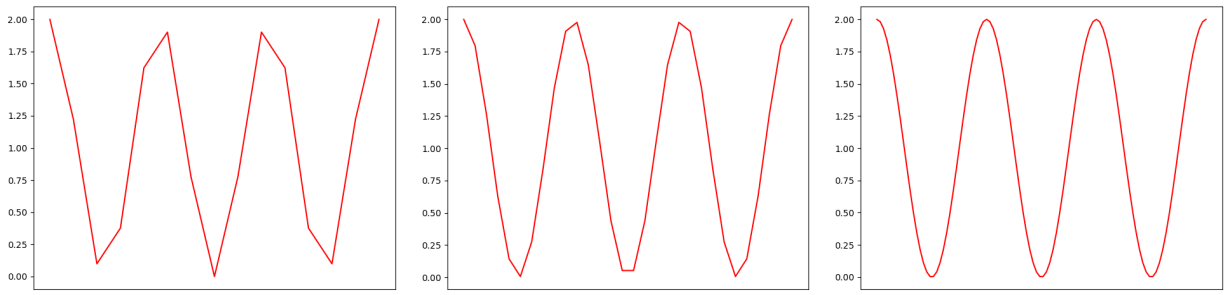


Figure de dessus : les données sont sous la forme de points (j, x_j).
Figures du dessous : les mêmes données sous forme circulaire avec $t = \frac{1}{4}$, $t = \frac{1}{2}$, $t = 1$ et $t > 1$.

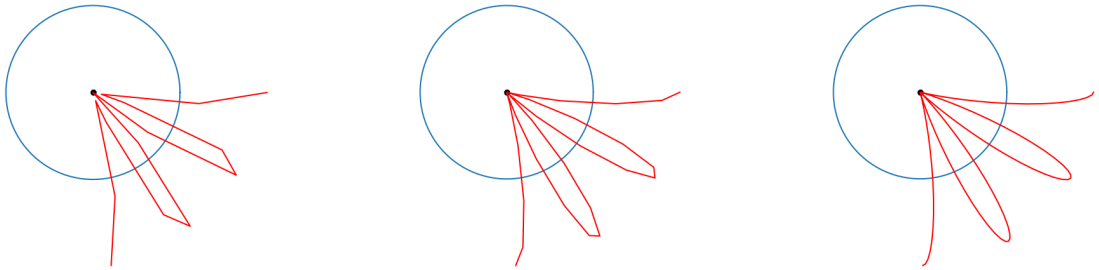
1.4. Enroulements particuliers

On remplace l'étude d'une fonction $f : [a, b] \to \mathbb{R}$ par l'étude de valeurs $x_j = f(a_j)$ pour une subdivision (a_j) de l'intervalle $[a, b]$. Pour avoir une meilleure précision, il suffit d'augmenter le nombre n de points dans la subdivision. On relie les points de ces données pour approcher le graphe de f.



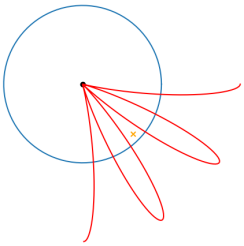
Fonction $f(x) = 1 + \cos(3x)$ *sur l'intervalle* $[0, 2\pi]$.
Les données sont les $x_j = f(a_j)$ *avec une subdivision de* $n = 15$ *points à gauche,* $n = 30$ *au centre,* $n = 100$ *à droite.*

On peut aussi relier les points du graphe circulaire. Géométriquement on a ainsi enroulé le graphe de la fonction f, sur le cercle.

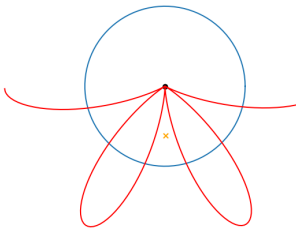


Les mêmes données sur le graphe circulaire avec $n = 15$ *points à gauche,* $n = 30$ *au centre,* $n = 100$ *à droite.*

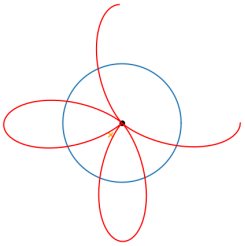
Regardons maintenant les différents enroulements selon le paramètre d'étalement t. Tout d'abord on exclut les t avec $t < 1$ car le graphe ne s'enroule pas totalement autour du cercle. Pour la plupart des paramètres on obtient une jolie figure symétrique autour de l'origine, mais il y a des exceptions. Pour $t = 3$ on obtient une figure complètement décalée à droite. Que se passe-t-il en $t = 3$? Le graphe de f est périodique et pour cette valeur de t la courbe enroulée vient se superposer à elle-même lors des enroulements successifs.



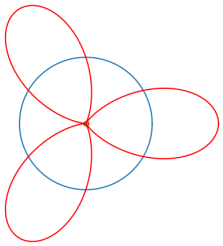
$t = 0.25$



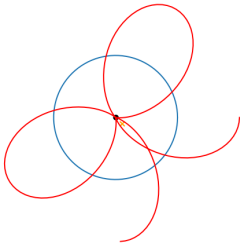
$t = 0.5$



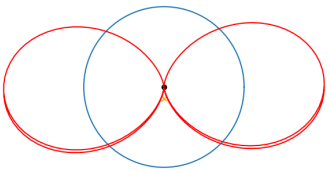
$t = 0.75$



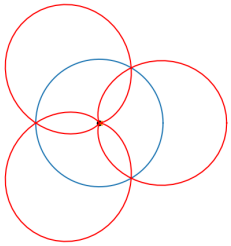
$t = 1$



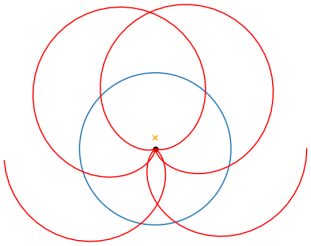
$t = 1.25$



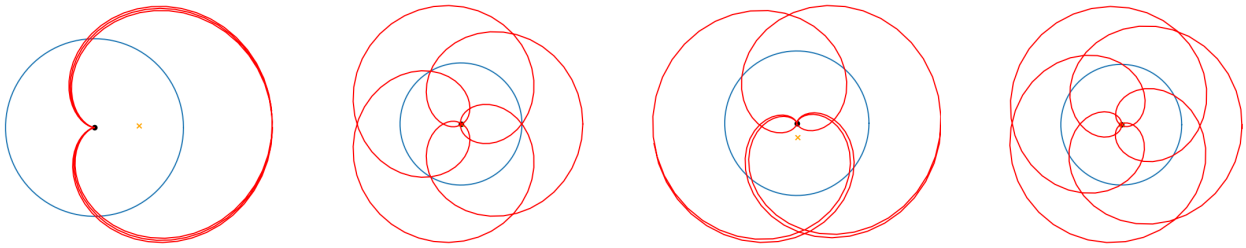
$t = 1.50$



$t = 2$



$t = 2.5$



$t = 3$ $t = 4$ $t = 4.5$ $t = 5$

Graphe de $f(x) = 1 + \cos(3x)$ sur l'intervalle $[0, 2\pi]$
enroulé sur le cercle pour différentes valeurs de t.
Pour $t = 3$ la figure n'est plus symétrique par rapport à l'origine.
La petite croix orange désigne le centre de gravité.

Ce cas particulier $t = 3$ est le cas qui nous intéresse ! Le paramètre $t = 3$ correspond à la période de notre fonction. En effet, la fonction $f(x) = 1 + \cos(3x)$ est $\frac{2\pi}{3}$ périodique et le paramètre spécial est $t = 3$. Pour une fonction $f(x) = 1 + \cos(\alpha x)$, la période est $\frac{2\pi}{\alpha}$ et le paramètre spécial est $t = \alpha$ (en fait t correspond à la fréquence qui est l'inverse de la période).

1.5. Centre de gravité

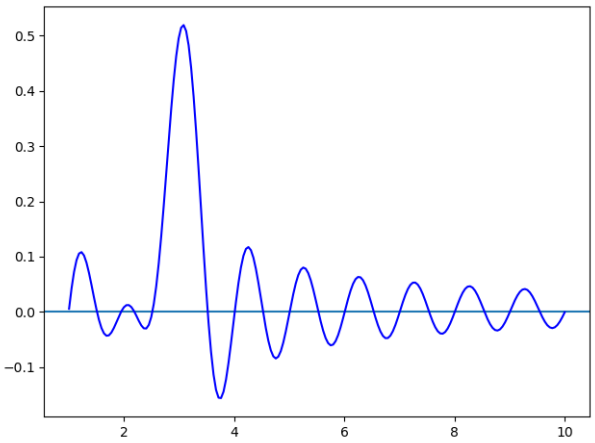
Est-ce que cette technique permet d'obtenir les différentes périodes d'un signal obtenu par superposition (comme dans l'exemple du tout début de ce chapitre) ? La réponse est oui ! Voyons comment repérer ces paramètres particuliers qui correspondent à des périodes. Pour la plupart des paramètres les figures obtenues sont symétriques par rapport à l'origine, donc le centre de gravité est proche de l'origine (en physique on parle d'interférence destructive). Par contre, pour certains paramètres particuliers, le centre de gravité s'éloigne de l'origine. Nous obtenons donc un critère numérique simple.
Le centre de gravité des points se calcule comme une moyenne des points :

$$X_t = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} x_j e^{-2i\pi \frac{t \cdot j}{n}}.$$

Quelques remarques :

- Sur les dessins précédents ce centre de gravité était représenté par une petite croix orange.
- Nous préférons le choix du coefficient $\frac{1}{\sqrt{n}}$ (au lieu du coefficient $\frac{1}{n}$ du vrai centre de gravité).
- Pour $t = k$ la formule est exactement celle de la transformée de Fourier discrète des (x_j).

Comment évolue X_t en fonction de t et comment repérer les paramètres particuliers ? Le nombre X_t est un nombre complexe, on se contente de regarder sa partie réelle $\mathrm{Re}(X_t)$. La fonction $t \mapsto \mathrm{Re}(X_t)$ mesure donc l'abscisse du centre de gravité.

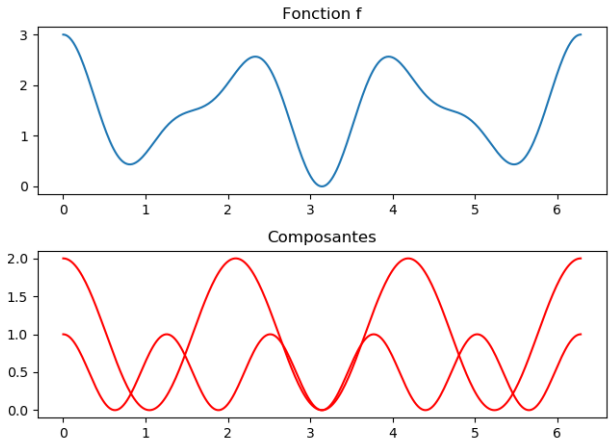


Graphe de la fonction $t \mapsto \mathrm{Re}(X_t)$ qui mesure l'abscisse du centre de gravité de l'enroulement de la fonction $f(x) = 1 + \cos(3x)$ sur l'intervalle $[0, 2\pi]$ pour différentes valeurs de t. Le pic à $t = 3$ marque la rupture de symétrie.

Pour la plupart des valeurs de t, $\mathrm{Re}(X_t)$ est proche de 0, les pics correspondent à la rupture de symétrie centrale et déterminent les périodes des composantes de la fonction.

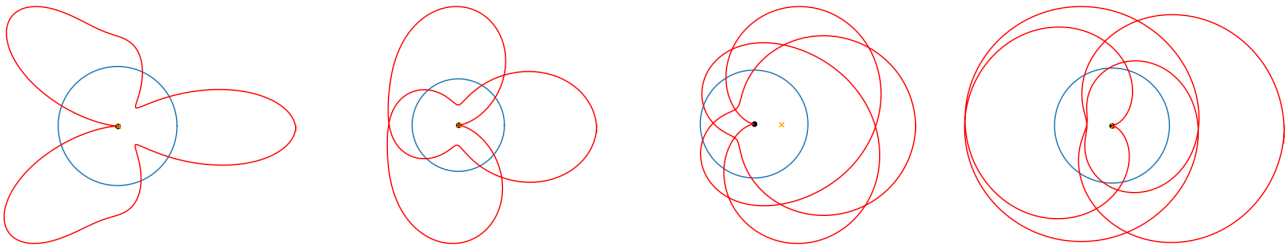
1.6. Autre exemple

Soient $f_1(x) = 1 + \cos(3x)$ et $f_2(x) = \frac{1}{2}(1 + \cos(5x))$ et leur somme $f(x) = f_1(x) + f_2(x)$ définie sur l'intervalle $[0, 2\pi]$. À partir de f, nous souhaitons retrouver les périodes $\frac{2\pi}{3}$ et $\frac{2\pi}{5}$ de ses deux composantes.

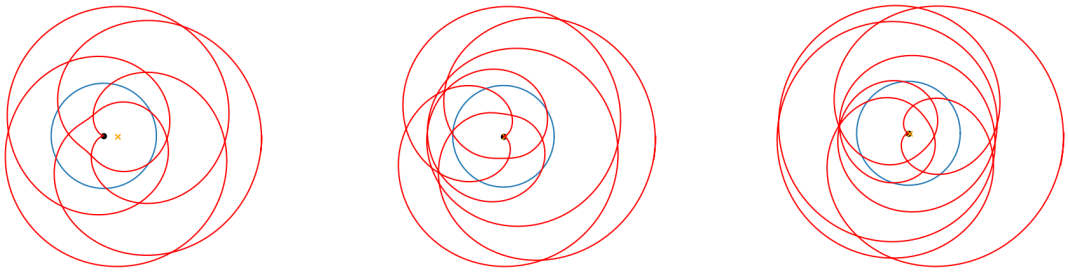


Le graphe de la fonction $f(x) = f_1(x) + f_2(x)$ sur $[0, 2\pi]$ avec $f_1(x) = 1 + \cos(3x)$ et $f_2(x) = \frac{1}{2}(1 + \cos(5x))$.

On enroule le graphe de f sur un cercle, selon différentes valeurs de t.



$t = 1$ $t = 2$ $t = 3$ $t = 4$



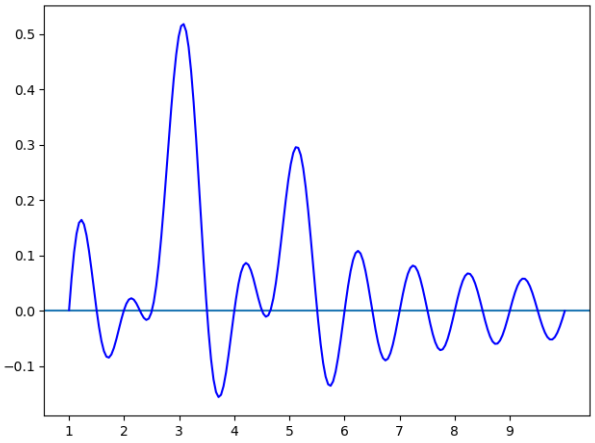
$t = 5$ $t = 6$ $t = 7$

Enroulement du graphe de f pour différentes valeurs de t.
Noter le décalage du centre de gravité (la croix orange) en $t = 3$ et $t = 5$.

Le centre de gravité se calcule selon la formule de la transformée de Fourier discrète, pour nos paramètres $t = 1, t = 2, \ldots$

$$X_t = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} x_j e^{-2i\pi \frac{t \cdot j}{n}}.$$

où $x_j = f\left(\frac{j}{n}\right)$



Graphe de de la fonction $t \mapsto \mathrm{Re}(X_t)$ qui mesure l'abscisse du centre de gravité de l'enroulement de la fonction $f(x)$ sur l'intervalle $[0, 2\pi]$ pour différentes valeurs de t.
On remarque des pics en $t = 3$ et $t = 5$.

1.7. L'inverse de la transformée de Fourier discrète

On a donc vu l'intérêt de la transformée de Fourier : elle permet de retrouver les caractéristiques d'une fonction (ou d'une série de données). Mais de plus cette transformation ne perd pas d'information. D'un point de vue mathématique la transformation est bijective. On peut retrouver les (x_k) connaissant les (X_j) par une formule similaire (seul le signe de l'exponentielle change) :

$$x_k = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} X_j e^{+2i\pi \frac{k \cdot j}{n}}.$$

Conclusion : la transformée de Fourier discrète transforme une liste de n nombres en une autre liste de n nombres. Cette transformation est bijective et permet en particulier de déterminer la période d'un signal périodique.

1.8. La transformée de Fourier discrète quantique

La transformée de Fourier discrète quantique est par définition cette variante de la transformée de Fourier discrète :

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

Les différences sont les suivantes :

- Par convention on choisit un signe « + » pour l'exposant de la transformée quantique (comme pour la transformée de Fourier discrète *inverse* classique).
- Les données sont remplacées par les qubits de bases $\left|\underline{0}\right\rangle$, $\left|\underline{1}\right\rangle$,…
- En conséquence le nombre total de données est une puissance de 2. Pour les n-qubits, il y a 2^n qubits de base $\left|\underline{0}\right\rangle$,…, $\left|\underline{2^n-1}\right\rangle$.
- La fonction $\hat{F}$ s'étend par linéarité à n'importe quel n-qubit. Si $|\psi\rangle = \alpha_0 \left|\underline{0}\right\rangle + \alpha_1 \left|\underline{1}\right\rangle + \cdots$ alors $\hat{F}|\psi\rangle = \alpha_0 \hat{F}\left|\underline{0}\right\rangle + \alpha_1 \hat{F}\left|\underline{1}\right\rangle + \cdots$

2. Écritures de la transformée de Fourier

2.1. Définition de la transformée de Fourier

On rappelle la définition de la transformée de Fourier discrète quantique pour un n-qubit de base $\left|\underline{k}\right\rangle$:

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

Dans toute la suite du chapitre la notion de « transformée de Fourier » désigne la transformée de Fourier discrète quantique. On renvoie au chapitre « Algorithme de Shor » pour les détails et les premières propriétés.

2.2. Factorisation de la transformée de Fourier

Voici le résultat fondamental de ce chapitre qui permettra de réaliser le circuit quantique de la transformée de Fourier.

Théorème 1.

$$\boxed{\hat{F}\left|\underline{k}\right\rangle = \frac{1}{\sqrt{2^n}} \prod_{\ell=1}^{n} \left(|0\rangle + e^{2\mathrm{i}\pi\frac{k}{2^\ell}}|1\rangle\right)}$$

Notation : on note le produit sous la forme $\prod_{\ell=1}^{n}$ afin de ne pas effrayer le lecteur, alors qu'en toute rigueur il s'agit d'un produit tensoriel :

$$\hat{F}\left|\underline{k}\right\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{\ell=1}^{n} \left(|0\rangle + e^{2\mathrm{i}\pi\frac{k}{2^\ell}}|1\rangle\right).$$

De façon développée la factorisation s'écrit :

$$\hat{F}\left|\underline{k}\right\rangle = \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\mathrm{i}\pi\frac{k}{2}}|1\rangle\right) \otimes \left(|0\rangle + e^{2\mathrm{i}\pi\frac{k}{2^2}}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{2\mathrm{i}\pi\frac{k}{2^n}}|1\rangle\right).$$

Exemple.

- Pour $n = 1$ le produit est réduit à un seul élément, $\hat{F}\left|\underline{k}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\mathrm{i}\pi\frac{k}{2}}|1\rangle\right)$. Ainsi pour $k = 0$, $\hat{F}\left|\underline{0}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et pour $k = 1$, $e^{\mathrm{i}\pi} = -1$ donc $\hat{F}\left|\underline{1}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. On retrouve bien que pour $n = 1$, la transformée de Fourier correspond à la porte de Hadamard H.

- Pour $n=2$, on écrit pour $\ell=1$, $e^{2i\pi\frac{k}{2}}=(-1)^k$ et pour $\ell=2$, $e^{2i\pi\frac{k}{2^2}}=i^k$, la factorisation s'écrit donc
$$\hat{F}\left|\underline{k}\right\rangle=\frac{1}{2}\left(|0\rangle+(-1)^k|1\rangle\right)\left(|0\rangle+i^k|1\rangle\right).$$
- Pour $n=3$, notons $\omega=e^{\frac{2i\pi}{2^3}}=e^{\frac{i\pi}{4}}$, la factorisation s'écrit :
$$\hat{F}\left|\underline{k}\right\rangle=\frac{1}{\sqrt{8}}\left(|0\rangle+(-1)^k|1\rangle\right)\left(|0\rangle+i^k|1\rangle\right)\left(|0\rangle+\omega^k|1\rangle\right).$$
Mais comme $\omega^2=i$ et $\omega^4=-1$, on peut aussi l'écrire :
$$\hat{F}\left|\underline{k}\right\rangle=\frac{1}{\sqrt{8}}\left(|0\rangle+\omega^{2^2\cdot k}|1\rangle\right)\left(|0\rangle+\omega^{2\cdot k}|1\rangle\right)\left(|0\rangle+\omega^k|1\rangle\right).$$

La preuve du théorème repose sur l'écriture binaire des entiers. Prenons j un entier (avec $0\leqslant j<2^n$) et écrivons sa décomposition suivant les puissances de 2 :
$$j=\sum_{\ell=0}^{n-1}j_\ell 2^\ell=j_{n-1}\cdot 2^{n-1}+\cdots+j_2\cdot 2^2+j_1\cdot 2+j_0$$
avec $j_\ell=0$ ou $j_\ell=1$, pour $\ell=0,\ldots,n-1$ et notons comme d'habitude $\underline{j}=j_{n-1}\ldots j_2.j_1.j_0$ l'écriture binaire de j.
Par définition :
$$\left|\underline{j}\right\rangle=|j_{n-1}\ldots j_2.j_1.j_0\rangle=|j_{n-1}\rangle\cdots|j_2\rangle\cdot|j_1\rangle\cdot|j_0\rangle.$$

Démonstration. Nous partons du produit
$$\prod_{\ell=1}^{n}\left(|0\rangle+e^{2i\pi\frac{k}{2^\ell}}|1\rangle\right) \tag{2}$$
que nous allons développer. Nous allons montrer que le coefficient devant le terme $\left|\underline{j}\right\rangle$ est le même que celui de la définition (1) de la transformée de Fourier.
Récrivons le produit (2) sous une forme plus explicite :
$$\begin{aligned}&\left(|0\rangle+e^{2i\pi\frac{k}{2^1}}|1\rangle\right)\\&\times\left(|0\rangle+e^{2i\pi\frac{k}{2^2}}|1\rangle\right)\\&\times\left(|0\rangle+e^{2i\pi\frac{k}{2^3}}|1\rangle\right)\\&\times\cdots\end{aligned} \tag{3}$$
Lorsque l'on développe cette expression, on obtient des termes qui résultent du choix pour chaque ligne de (3) d'un des deux éléments $|0\rangle$ ou $e^{2i\pi\frac{k}{2^\ell}}|1\rangle$.
Par exemple, si on choisit $|0\rangle$ à chaque ligne de (3), alors on obtient le terme $|0\rangle\cdot|0\rangle\cdots|0\rangle=|0.0\ldots0\rangle=\left|\underline{0}\right\rangle$ avec comme coefficient 1, exactement comme le coefficient $\left|\underline{0}\right\rangle$ de l'expression (1).
Revenons au cas général. Pour la première ligne de (3), soit on choisit le facteur $|0\rangle$ et alors on va obtenir un terme qui commence par $|0\rangle$: $\left|\underline{j}\right\rangle=|0\ldots\rangle$, soit on choisit le facteur $e^{2i\pi\frac{k}{2^1}}|1\rangle$ et on va obtenir un terme qui commence par $|1\rangle$: $\left|\underline{j}\right\rangle=|1\ldots\rangle$. On peut regrouper ces deux cas en une seule formule : notons j_{n-1} un bit (qui vaut 0 ou 1) alors le facteur de la première ligne s'écrit $e^{2i\pi\frac{k\cdot j_{n-1}}{2^1}}|j_{n-1}\rangle$. En effet si $j_{n-1}=0$ alors ce facteur vaut $e^{2i\pi\cdot 0}|0\rangle$, c'est donc $|0\rangle$, et si $j_{n-1}=1$ c'est $e^{2i\pi\frac{k\cdot 1}{2^1}}|1\rangle$. Ce facteur va produire un terme qui commence par le bit j_{n-1} : $\left|\underline{j}\right\rangle=|j_{n-1}\ldots\rangle$. Ainsi le choix du facteur de la première ligne correspond au premier bit de $\underline{j}$ (celui le plus à gauche).

Plus généralement, le facteur de la ligne ℓ de (3) s'écrit $e^{2i\pi\frac{k\cdot j_{n-\ell}}{2^\ell}}|j_{n-\ell}\rangle$. En effet, si $j_{n-\ell}=0$ alors c'est $|0\rangle$ et si $j_{n-\ell}=1$ alors c'est bien $e^{2i\pi\frac{k}{2^\ell}}|1\rangle$. Ce facteur va produire un terme avec le bit $j_{n-\ell}$: $\left|\underline{j}\right\rangle=|\ldots j_{n-\ell}\ldots\rangle$.

Ainsi le terme qui correspond au qubit $\left|\underline{j}\right\rangle$ dans le développement de (3) est le produit des facteurs $e^{2i\pi\frac{k\cdot j_{n-\ell}}{2^\ell}}\left|j_{n-\ell}\right\rangle$ pour chacune des lignes. Calculons ce terme :

$$\begin{aligned}\prod_{\ell=1}^{n}\left(e^{2i\pi\frac{k\cdot j_{n-\ell}}{2^\ell}}\left|j_{n-\ell}\right\rangle\right) &= \left(\prod_{\ell=1}^{n}e^{2i\pi\frac{k\cdot j_{n-\ell}}{2^\ell}}\right)\left|j_{n-1}\dots j_2.j_1.j_0\right\rangle\\ &= e^{2i\pi k\cdot\sum_{\ell=1}^{n}\frac{j_{n-\ell}}{2^\ell}}\left|\underline{j}\right\rangle\\ &= e^{2i\pi\frac{k}{2^n}\cdot\sum_{\ell=1}^{n}j_{n-\ell}2^{n-\ell}}\left|\underline{j}\right\rangle\\ &= e^{2i\pi\frac{k}{2^n}\cdot\sum_{\ell'=0}^{n-1}j_{\ell'}2^{\ell'}}\left|\underline{j}\right\rangle\\ &= e^{2i\pi\frac{k}{2^n}\cdot j}\left|\underline{j}\right\rangle\end{aligned}$$

Ainsi le coefficient de $\left|\underline{j}\right\rangle$ du développement de la formule (2) est $e^{2i\pi\frac{k}{2^n}\cdot j}$ qui est exactement celui du coefficient de $\left|\underline{j}\right\rangle$ dans la définition de la transformée de Fourier (1).

Ceci étant vrai quel que soit le qubit $\left|\underline{j}\right\rangle$, on a donc bien :

$$\hat{F}\left|\underline{k}\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}e^{2i\pi\frac{k\cdot j}{2^n}}\left|\underline{j}\right\rangle = \frac{1}{\sqrt{2^n}}\prod_{\ell=1}^{n}\left(\left|0\right\rangle + e^{2i\pi\frac{k}{2^\ell}}\left|1\right\rangle\right).$$

□

2.3. Variante

Commençons par introduire l'écriture binaire pour un nombre $0 \leqslant x < 1$.

$$0..j_1.j_2\dots j_n = \frac{j_1}{2} + \frac{j_2}{2^2} + \dots + \frac{j_n}{2^n} = \sum_{\ell=1}^{n}\frac{j_\ell}{2^\ell}.$$

La notation est $0..j_1.j_2\dots j_n$: les points séparent les bits, le double point symbolise la virgule car en écriture décimale le nombre s'écrit $0.abc\dots$

Par exemple $x = 0.625$ (en écriture décimale) s'écrit en écriture binaire $x = 0..1.0.1$ car $0.625 = \frac{1}{2} + \frac{0}{4} + \frac{1}{8}$.

Nous reformulons le théorème 1 de factorisation en jouant sur le passage de l'écriture binaire de l'entier k à l'écriture binaire d'un nombre à virgule.

Corollaire 1.
Si $\left|\underline{k}\right\rangle = \left|k_{n-1}\dots k_1.k_0\right\rangle$

$$\hat{F}\left|\underline{k}\right\rangle = \frac{1}{\sqrt{2^n}}\prod_{\ell=1}^{n}\left(\left|0\right\rangle + e^{2i\pi 0..k_{\ell-1}\dots k_0}\left|1\right\rangle\right).$$

Autrement dit

$$\hat{F}\left|\underline{k}\right\rangle = \frac{1}{\sqrt{2^n}}\left(\left|0\right\rangle + e^{2i\pi 0..k_0}\left|1\right\rangle\right)\otimes\left(\left|0\right\rangle + e^{2i\pi 0..k_1.k_0}\left|1\right\rangle\right)\otimes\dots\otimes\left(\left|0\right\rangle + e^{2i\pi 0..k_{n-1}\dots k_1.k_0}\left|1\right\rangle\right).$$

Démonstration. Notons tout d'abord que pour n'importe quel entier p, $e^{2i\pi p} = 1$.

Alors

$$\begin{aligned}\frac{k}{2^\ell} &= \frac{k_{n-1}2^{n-1} + \cdots + k_2 2^2 + k_1 2 + k_0}{2^\ell} \\ &= \underbrace{k_{n-1}2^{n-1-\ell} + \cdots + k_\ell}_{\text{partie entière}} + \underbrace{\frac{k_{\ell-1}}{2} + \cdots + \frac{k_0}{2^\ell}}_{\text{partie décimale}} \\ &= p \quad + \quad 0..k_{\ell-1}\ldots k_0\end{aligned}$$

Ainsi

$$e^{2i\pi\frac{k}{2^\ell}} = e^{2i\pi(p+0..k_{\ell-1}\ldots k_0)} = e^{2i\pi 0..k_{\ell-1}\ldots k_0}.$$

Par exemple :

- pour $\ell = 1$, $e^{2i\pi\frac{k}{2}} = e^{2i\pi 0..k_0}$;
- pour $\ell = 2$, $e^{2i\pi\frac{k}{4}} = e^{2i\pi 0..k_1.k_0}$;
- et pour $\ell = n$, $e^{2i\pi\frac{k}{2^n}} = e^{2i\pi 0..k_{n-1}\ldots k_1.k_0}$.

Le théorème 1 donne alors la formule voulue. □

3. Circuit de la transformation Fourier

Nous allons construire un circuit quantique qui réalise la transformée de Fourier.

3.1. Porte R_k

Soit $R_k \in M_2(\mathbb{C})$ la matrice unitaire suivante :

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

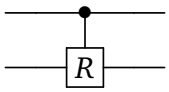
Notons aussi R_k la porte quantique correspondante :

- Pour $n = 0$, $e^{\frac{2i\pi}{1}} = 1$ donc $R_0 = I$: la transformation est l'identité.
- Pour $n = 1$, $e^{\frac{2i\pi}{2}} = -1$ donc la transformation est $R_1 = Z$ ($|0\rangle \mapsto |0\rangle$, $|1\rangle \mapsto -|1\rangle$).
- Pour $n = 2$, $e^{\frac{2i\pi}{4}} = i$, la porte R_2 est aussi appelée porte S ($|0\rangle \mapsto |0\rangle$, $|1\rangle \mapsto i|1\rangle$).
- Pour $n = 3$, $e^{\frac{2i\pi}{8}} = e^{\frac{i\pi}{4}}$, la porte R_3 est aussi appelée porte T ($|0\rangle \mapsto |0\rangle$, $|1\rangle \mapsto e^{\frac{i\pi}{4}}|1\rangle$).

$$R_0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad R_1 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad R_2 = S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad R_3 = T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$$

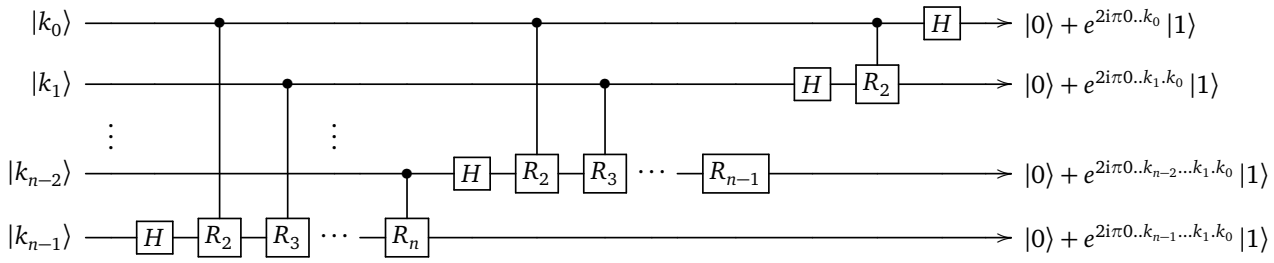
3.2. Contrôle des portes

Chaque porte R va être « contrôlée » par un autre qubit qui déterminera si on applique ou non la porte R.

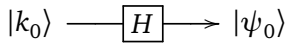


Si le premier qubit est $|0\rangle$, on ne change pas le second qubit, si le premier qubit est $|1\rangle$, on applique la porte R au second qubit restant.

3.3. Circuit



Justifions que ce circuit convient en regardant les exemples avec peu de lignes.
Cas $n = 1$. Le circuit est simplement réduit à une seule ligne contenant la seule porte H :

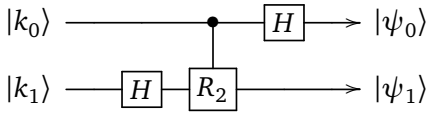


Donc $|\psi_0\rangle = H|k_0\rangle$. Ainsi $|\psi_0\rangle = |0\rangle + |1\rangle$ si $k_0 = 0$, et $|\psi_0\rangle = |0\rangle - |1\rangle$ si $k_0 = 1$ (aux coefficients $\sqrt{2}$ près).
On résume cela en une seule formule pour les deux cas :

$$|\psi_0\rangle = |0\rangle + (-1)^{k_0}|1\rangle = |0\rangle + e^{2i\pi\frac{k_0}{2}}|1\rangle = |0\rangle + e^{2i\pi 0..k_0}|1\rangle,$$

car on rappelle que $e^{2i\pi 0..k_0} = e^{2i\pi\frac{k_0}{2}} = e^{i\pi k_0} = (-1)^{k_0}$ qui vaut $+1$ si $k_0 = 0$ et -1 si $k_0 = 1$.

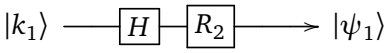
Cas $n = 2$.



Il est clair que $|\psi_0\rangle$ est le même qubit que dans le cas $n = 1$ ci-dessus.
Calculons le qubit $|\psi_1\rangle$. Si $|k_0\rangle = |0\rangle$ alors la seconde ligne est juste une porte H car la porte R_2 n'est pas activée. Donc si $k_0 = 0$, on a donc comme ci-dessus pour le cas $n = 1$:

$$|\psi_1\rangle = H|k_1\rangle = |0\rangle + e^{2i\pi\frac{k_1}{2}}|1\rangle \tag{4}$$

Par contre si $k_0 = 1$ la porte R_2 est activée et la seconde ligne devient :



Ainsi :

$$\begin{aligned}
|\psi_1\rangle &= R_2(H|k_1\rangle) \\
&= R_2\left(|0\rangle + e^{2i\pi\frac{k_1}{2}}|1\rangle\right) \\
&= R_2|0\rangle \; + \; e^{2i\pi\frac{k_1}{2}} R_2|1\rangle \\
&= |0\rangle + e^{2i\pi\frac{k_1}{2}} \cdot e^{2i\pi\frac{1}{4}}|1\rangle
\end{aligned} \tag{5}$$

On peut regrouper les cas $k_0 = 0$ et $k_0 = 1$ des équations (4) et (5) en une seule équation :

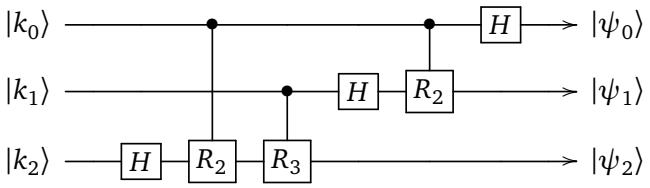
$$|\psi_1\rangle = |0\rangle + e^{2i\pi\frac{k_1}{2}} \cdot e^{2i\pi\frac{k_0}{4}}|1\rangle \tag{6}$$

où l'on a utilisé que $e^{2i\pi\frac{k_0}{4}}$ vaut 1 si $k_0 = 0$ et $e^{2i\pi\frac{1}{4}}$ si $k_0 = 1$.

Mais comme $e^{2i\pi\frac{k_1}{2}} \cdot e^{2i\pi\frac{k_0}{4}} = e^{2i\pi 0..k_1.k_0}$, on obtient bien :

$$|\psi_1\rangle = |0\rangle + e^{2i\pi 0..k_1.k_0}\,|1\rangle\,.$$

Cas $n = 3$.



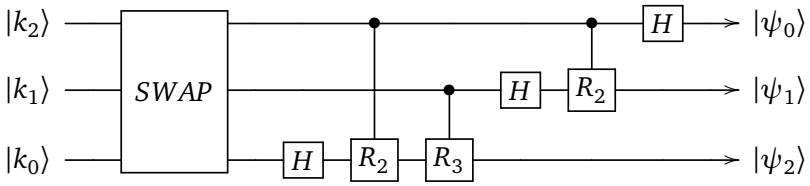
Les calculs s'effectuent sur le même principe : $|\psi_0\rangle$ et $|\psi_1\rangle$ sont les mêmes que précédemment et

$$|\psi_2\rangle = |0\rangle + e^{2i\pi\frac{k_2}{2}} \cdot e^{2i\pi\frac{k_1}{4}} \cdot e^{2i\pi\frac{k_0}{8}}\,|1\rangle = |0\rangle + e^{2i\pi 0..k_2.k_1.k_0}\,|1\rangle\,.$$

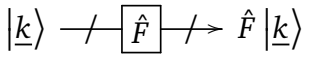
Le calcul pour un n quelconque se fait par récurrence et prouve que le circuit calcule la transformée de Fourier.

3.4. Porte *SWAP*

Il faut faire une petite modification au circuit de la transformée de Fourier qui, en effet, ne respecte pas notre convention habituelle sur l'ordre d'écriture des qubits. Dans notre circuit le qubit en entrée est $|k_0\rangle \otimes |k_1\rangle \otimes \cdots \otimes |k_{n-1}\rangle$. Mais si l'écriture binaire de $\underline{k}$ est $k_{n-1}\ldots k_1.k_0$ alors $\left|\underline{k}\right\rangle = |k_{n-1}\rangle \otimes \cdots |k_1\rangle \otimes |k_0\rangle$. Pour obtenir l'écriture voulue il suffit de renverser les qubits. Cela se fait avec une porte *SWAP* que l'on a vue lors du chapitre « Portes quantiques ».
Ainsi le circuit complet pour l'exemple de $n = 3$ devient :



En incluant une porte *SWAP*, nous avons construit un circuit qui réalise la transformée de Fourier :



4. Estimation de phase

La dernière application de la transformée de Fourier que nous allons voir est « l'estimation de phase », c'est le nom physique utilisé pour parler de la détermination d'une valeur propre d'une matrice unitaire. Cette section ne revient pas sur les détails et les motivations concernant les valeurs propres : on renvoie pour cela à un cours d'algèbre sur la réduction des endomorphismes.

4.1. Valeur propre

Définition.
Soit $A \in M_n(\mathbb{C})$ une matrice. Le scalaire $\lambda \in \mathbb{C}$ est une ***valeur propre*** associée au ***vecteur propre*** X, si X n'est pas le vecteur nul et :

$$\boxed{AX = \lambda X}$$

Les valeurs propres et les vecteurs propres jouent un rôle fondamental dans l'étude des matrices. Rappelons juste ici qu'une matrice unitaire (c'est-à-dire vérifiant $A^*A = I$) est diagonalisable, c'est-à-dire équivalente à une matrice diagonale :

$$\begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}$$

où justement les éléments λ_i sont les valeurs propres de A.
Mettons en avant deux propriétés des valeurs propres.

Lemme 1.
Soit A une matrice. Si λ est une valeur propre associée au vecteur propre X alors $A^nX = \lambda^nX$.

Autrement dit λ^n est une valeur propre de A^n.

Démonstration. La preuve se fait par récurrence en se calquant sur le modèle suivant où $n = 2$:

$$A^2X = A(AX) = A(\lambda X) = \lambda(AX) = \lambda(\lambda X) = \lambda^2 X.$$

□

Voici le second résultat qui concerne uniquement les matrices unitaires.

Lemme 2.
Soit $A \in M_n(\mathbb{C})$ une matrice unitaire. Si λ est une valeur propre alors $|\lambda| = 1$.

Ainsi on peut écrire $\lambda = e^{2i\pi\theta}$ et la valeur propre est déterminé par sa « phase » θ (la phase étant le nom donné par les physiciens à l'argument). Pour comprendre la preuve, rappelons quelques propriétés (voir le chapitre « Portes quantiques ») :

- A unitaire signifie $A^*A = I$.
- Le produit scalaire est anti-linéaire à gauche et linéaire à droite, donc pour $\lambda \in \mathbb{C}$:

  $$\langle \lambda u | v \rangle = \lambda^* \langle u | v \rangle \quad \text{et} \quad \langle u | \lambda v \rangle = \lambda \langle u | v \rangle$$

  et permet de calculer la norme : $\|u\|^2 = \langle u | u \rangle$.
- Une matrice unitaire préserve le produit scalaire : $\langle Au | Av \rangle = \langle u | v \rangle$.

Démonstration. Soit λ une valeur propre associée au vecteur propre X.

$$\begin{aligned} \langle AX | AX \rangle = \langle X | X \rangle \quad &\Longrightarrow \quad \langle \lambda X | \lambda X \rangle = \langle X | X \rangle \\ &\Longrightarrow \quad \lambda^* \langle X | \lambda X \rangle = \langle X | X \rangle \\ &\Longrightarrow \quad \lambda^* \lambda \langle X | X \rangle = \langle X | X \rangle \\ &\Longrightarrow \quad |\lambda|^2 \cdot \|X\|^2 = \|X\|^2 \\ &\Longrightarrow \quad |\lambda|^2 = 1 \\ &\Longrightarrow \quad |\lambda| = 1 \end{aligned}$$

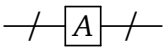
On a utilisé les propriétés rappelées précédemment ainsi que le fait qu'un vecteur propre est non nul (donc $\|X\| \neq 0$). □

4.2. Problème de l'estimation de la phase

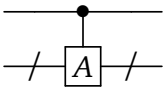
D'un point de vue mathématique le problème est le suivant. On nous donne une matrice $M \in M_N(\mathbb{C})$ unitaire et un vecteur propre X_0. Il s'agit de calculer la valeur propre $\lambda_0 = e^{2i\pi\theta_0}$ associée à ce vecteur propre. Dans notre situation informatique, on a $N = 2^n$ et $A \in M_{2^n}(\mathbb{C})$ est une matrice unitaire. Le vecteur propre est écrit sous la forme d'un n-qubit $|\psi_0\rangle$. Le but reste toujours de déterminer la valeur propre λ_0 en calculant θ_0.

4.3. Porte cA

Nous généralisons la porte $CNOT$, qui est une porte cX, c'est-à-dire une porte X conditionnelle. Soit A un matrice unitaire de $M_{2^n}(\mathbb{C})$, à laquelle on associe une porte également notée A.



La barre oblique « / » devant et après la porte A signifie que plusieurs lignes quantiques sont représentées en une seule. Ici l'entrée et la sortie sont des n-qubits. La porte cA (pour *controlled A*) est une porte ayant en entrée un 1-qubit supplémentaire, qui détermine si on applique ou non la porte A.



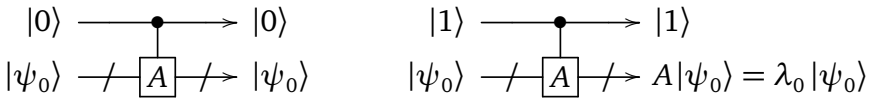
Si le premier qubit est $|0\rangle$, on ne change pas le n-qubit restant, si le premier qubit est $|1\rangle$, on applique la porte A au n-qubit restant.

4.4. Porte cA et valeurs propres

Calculons l'action de la porte cA lorsque le n-qubit est le vecteur propre $|\psi_0\rangle$ associé à la valeur propre $\lambda_0 = e^{2i\pi\theta_0}$.

- Si l'entrée est $|0\rangle \otimes |\psi_0\rangle$ alors la sortie est $|0\rangle \otimes |\psi_0\rangle$.
- Si l'entrée est $|1\rangle \otimes |\psi_0\rangle$ alors la sortie est :

$$|1\rangle \otimes A|\psi_0\rangle = |1\rangle \otimes \lambda_0 |\psi_0\rangle = e^{2i\pi\theta_0} |1\rangle \otimes |\psi_0\rangle .$$



Si le 1-qubit de la première ligne est $\alpha|0\rangle + \beta|1\rangle$ alors calculons le $(n+1)$-qubit de sortie :

$$\begin{aligned} \alpha|0\rangle + \beta|1\rangle \xmapsto{cA} & \alpha|0\rangle \otimes |\psi_0\rangle + \beta|1\rangle \otimes A|\psi_0\rangle \\ & = \alpha|0\rangle \otimes |\psi_0\rangle + \beta\lambda_0|1\rangle \otimes |\psi_0\rangle \\ & = \alpha|0\rangle \otimes |\psi_0\rangle + e^{2i\pi\theta_0}\beta|1\rangle \otimes |\psi_0\rangle \end{aligned}$$

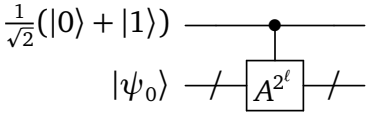
Ainsi le qubit de sortie s'écrit :

$$\boxed{\left(\alpha|0\rangle + e^{2i\pi\theta_0}\beta|1\rangle\right) \otimes |\psi_0\rangle}$$

Remarquons qu'après la factorisation par $|\psi_0\rangle$ le premier qubit de sortie est écrit $\alpha|0\rangle + e^{2i\pi\theta_0}\beta|1\rangle$. Cela peut sembler contradictoire avec le fait que la porte cA laisse inchangé le premier qubit qui devrait donc être $\alpha|0\rangle + \beta|1\rangle$, mais ici on inclut le coefficient provenant de la valeur propre ; mathématiquement on a simplement utilisé la bilinéarité $u \otimes (\lambda v) = (\lambda u) \otimes v$.

4.5. Bloc pour l'estimation de phase

La brique de base du circuit va être ce bloc :



La phase θ_0 est un réel qui vérifie $0 \leqslant \theta_0 < 1$. Supposons qu'il admette l'écriture binaire :

$$\theta_0 = 0..j_1.j_2 \ldots j_n = \frac{j_1}{2} + \frac{j_2}{2^2} + \cdots + \frac{j_n}{2^n}.$$

Lemme 3.
Le qubit de sortie du bloc précédent est :

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2i\pi 0..j_{\ell+1}\ldots j_n}|1\rangle\right) \otimes |\psi_0\rangle\,.$$

Démonstration. Par le lemme 1 la valeur propre de la matrice A^{2^ℓ} associée au vecteur propre $|\psi_0\rangle$ est

$$\lambda_0^{2^\ell} = e^{2i\pi 2^\ell \theta_0}.$$

Or

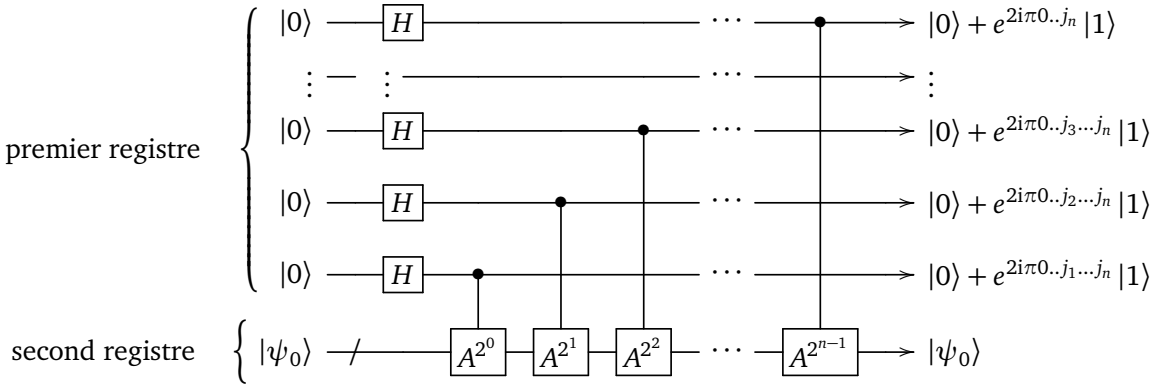
$$\begin{aligned} 2^\ell \theta_0 &= 2^\ell \left(\frac{j_1}{2} + \frac{j_2}{2^2} + \cdots + \frac{j_n}{2^n}\right) \\ &= \underbrace{j_1 2^{\ell-1} + \cdots + j_\ell}_{\text{partie entière}} + \underbrace{\frac{j_{\ell+1}}{2} + \cdots + \frac{j_n}{2^{n-\ell}}}_{\text{partie décimale}} \\ &= k + 0..j_{\ell+1}\ldots j_n \end{aligned}$$

Mais pour tout entier k, $e^{2i\pi k} = 1$ donc

$$\lambda_0^{2^\ell} = e^{2i\pi 2^\ell \theta_0} = e^{2i\pi 0..j_{\ell+1}\ldots j_n}.$$

Maintenant, la porte cA^{2^ℓ} appliquée à $|0\rangle \otimes |\psi_0\rangle$ a pour sortie $|0\rangle \otimes |\psi_0\rangle$ et appliquée à $|1\rangle \otimes |\psi_0\rangle$ elle a pour sortie $\lambda_0^{2\ell}|1\rangle \otimes |\psi_0\rangle$. Donc pour l'entrée du bloc $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_0\rangle$ la sortie est $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2i\pi 0..j_{\ell+1}\ldots j_n}|1\rangle\right) \otimes |\psi_0\rangle$. □

4.6. Circuit d'estimation de phase



Le qubit de sortie de ce circuit est présenté sous la forme factorisée par le vecteur propre $|\psi_0\rangle$ (voir le lemme 3). Les coefficients $\frac{1}{\sqrt{2}}$ sont omis.

Proposition 1.
Le qubit de sortie du circuit d'estimation de phase est $|\phi\rangle \otimes |\psi_0\rangle$ *où :*

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2i\pi 0..j_n} |1\rangle\right) \otimes \left(|0\rangle + e^{2i\pi 0..j_{n-1}j_n} |1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{2i\pi 0..j_1 \ldots j_n} |1\rangle\right).$$

Ainsi le premier registre de sortie est égal à $\hat{F}\,|j_1.j_2 \ldots j_n\rangle$*. Donc en composant le circuit à l'aide du circuit inverse de* $\hat{F}$ *(c'est-à-dire le circuit de* $\hat{F}^{-1}$*), on obtient le qubit* $|j_1.j_2 \ldots j_n\rangle$*, donc les « décimales »* $j_1, j_2, \ldots, j_n$ *de l'écriture binaire de* θ_0*.*

Démonstration. Une porte de Hadamard H transforme l'entrée $|0\rangle$ des premières lignes en $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Ainsi le circuit est composé de blocs de type cA^{2^ℓ} comme étudiés précédemment. Chacune de ces portes transforme le qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi_0\rangle$ en $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2i\pi 0..j_{\ell+1}\ldots j_n} |1\rangle\right) \otimes |\psi_0\rangle$. Ce qui conduit au résultat.
Par le circuit de la section 3 qui réalise la transformée de Fourier, on vérifie immédiatement que la sortie P du premier registre est $\hat{F}\,|j_1.j_2 \ldots j_n\rangle$. Ainsi $|j_1.j_2 \ldots j_n\rangle = \hat{F}^{-1}(P)$. Nous savons réaliser un circuit quantique pour $\hat{F}$. Comment réaliser un circuit pour $\hat{F}^{-1}$? Tout simplement en reprenant le circuit de $\hat{F}$ et en le lisant de droite à gauche (au lieu de la lecture habituelle de gauche à droite). Cette opération est possible car toutes les portes quantiques sont inversibles : donc obtenir la porte A^{-1}, c'est lire une porte A de droite à gauche.
Nous obtenons donc l'état quantique de base $|j_1.j_2 \ldots j_n\rangle$ dont la mesure donne les bits $j_1, j_2, \ldots, j_n$ qui permettent ainsi de retrouver la phase $\theta_0 = \frac{j_1}{2} + \frac{j2}{4} + \cdots$ et donc la valeur propre λ_0. □