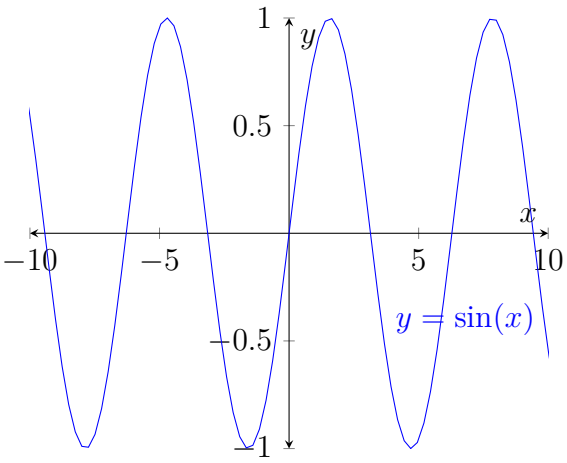
Algorithme de Shor

1 Problème à résoudre

Définition 1. *Une fonction f définie sur un ensemble $D \in \mathbb{R}$ est dite périodique de période $t \in \mathbb{R}$ si $\forall x \in D, x + t \in D$ et $f(x + t) = f(x)$.*

Exemple 1. *Soit la fonction f telle que $f : x \to \sin x$. Cette fonction est périodique puisque $f(x + 2 \times \pi) = \sin(x + 2 \times \pi) = \sin x = f(x)$; la période est ici $2 \times \pi$.*



Remarque 1. *Déterminer la périodicité d'une fonction simple (comme* sin *ou* cos*) peut paraître évident, mais cela se complique dès qu'on a une fonction non sinusoïdale, de période non évidente, voire une période non visible sur l'intervalle d'étude.*

Problème 1 (Estimation de phase quantique)**.** *Soit une fonction f périodique définie sur un ensemble $D \in \mathbb{R}$. Le problème est de déterminer la période t telle que $f(x + t) = f(x)$*

Classiquement, l'algorithme permettant de résoudre ce problème est en $\mathcal{O}(\exp n^{\frac{1}{3}} (\log n)^{\frac{2}{3}})$. On a donc besoin de n bits pour décrire la période.

En quantique, l'algorithme de Shor permet de résoudre ce problème en $\mathcal{O}(n^2 \log n \log\log n)$, ce qui est légèrement plus rapide que du $\mathcal{O}(n^3)$. On a ici un algorithme de complexité polynomiale. Cet algorithme est composé de deux parties : la **transformation quantique de Fourier** (QFT, Quantum Fourier Transform) et l'**estimation de phase quantique** (QPE, Quantum Phase Estimation).

2 Transformation quantique de Fourier

La transformation quantique de Fourier permet de passer de la base classique $\{|0\rangle, |1\rangle\}$ à la base de Fourier $\{|+\rangle, |-\rangle\}$.

La première base permet d'encoder les informations avec la valeur du bit. La base de Fourier va elle coder les informations avec la phase des qubits. Sur la sphere de Bloch, la première base va permettre de coder les informations sur plusieurs qubits en alternant sur l'axe vertical, c'est du calcul binaire classique. En revanche, la deuxième va faire tourner les qubits sur l'axe de l'équateur.

Remarque 2. *La transformation quantique de Fourier est l'analogue en classique de la transformation de Fourier discrète inverse*

En exemple, si on a 2 qubits, en base de Fourier, le premier aura pour phases successives $\{0, \pi\}$, et le deuxième aura $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$.

Dans le domaine classique, la transformation de Fourier discrète inverse est définie de la façon suivante :

$$x_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} y_j e^{2\pi\imath \frac{jk}{N}}$$

De façon équivalente, on définit la transformation de Fourier quantique :

$$|\tilde{x}\rangle = QFT|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi\imath \frac{xy}{N}} |y\rangle$$

2.1 Implémentation de la QFT

On note $\sum_{y=0}^{N-1} |y\rangle$. Néanmoins, on est en base 2, et écrire $|7\rangle$ par example n'a pas forcément de sens. La notation binaire de y est : $y = \sum_{k=0}^{n} y_k 2^{n-k}$. On peut donc remplacer dans l'équation définie précédement :

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi\imath x \sum_{k=0}^{n} \frac{y_k}{2^k}} |y_1, y_2, \ldots, y_n\rangle$$

La somme dans l'exponentielle nous permet de sortir un produit. On peut développer pour avoir une autre forme :

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \prod_{k=1}^{n} e^{2\pi\imath x \frac{y_k}{2^k}} |y_1, y_2, \ldots, y_n\rangle$$

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y_0=0}^{1} \sum_{y_1=0}^{1} \cdots \sum_{y_n=0}^{1} \prod_{k=1}^{n} e^{2\pi\imath x \frac{y_k}{2^k}} |y_1, y_2, \ldots, y_n\rangle$$

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \prod_{k=1}^{n} \sum_{y_0=0}^{1} \sum_{y_1=0}^{1} \cdots \sum_{y_n=0}^{1} e^{2\pi\imath x \frac{y_k}{2^k}} |y_1, y_2, \ldots, y_n\rangle$$

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} (|0\rangle + e^{2\pi\imath \frac{x}{2^1}} |1\rangle) \otimes (|0\rangle + e^{2\pi\imath \frac{x}{2^2}} |1\rangle) \otimes \cdots \otimes (|0\rangle + e^{2\pi\imath \frac{x}{2^n}} |1\rangle)$$

Exemple 2. *Soit* $|x\rangle = |5\rangle = |101\rangle$.

On a alors $QFT|x\rangle = |\tilde{x}\rangle = \frac{1}{\sqrt{8}}(|0\rangle + e^{5\pi\imath}|1\rangle) \otimes (|0\rangle + e^{\frac{1}{2}\pi\imath 5}|1\rangle) \otimes (|0\rangle + e^{\frac{1}{4}\pi\imath 5}|1\rangle)$

Pour chaque qubit, on effectue la transformation suivante :

$$H|x_k\rangle = |0\rangle + e^{2\pi\imath \frac{x_k}{2^k}} |1\rangle$$

Deux portes quantiques vont être utiles pour implémenter la QFT :

1. La porte de hadamard, de forme générale : $H|x_k\rangle = |0\rangle + e^{2\pi\imath \frac{x_k}{2}} |1\rangle$
2. La rotation unitaire $UROT_k|x_j\rangle = e^{2\pi\imath \frac{x_k}{2^k}} |x_j\rangle$. On note que si $x_j = 0$, alors $e^{2\pi\imath \frac{x_k}{2^k}} |x_j\rangle = |0\rangle$. De même, si $x_j = 1$, alors $e^{2\pi\imath \frac{x_k}{2^k}} |x_j\rangle = e^{\frac{2\pi\imath}{2^k}} |1\rangle$.

3 Estimation de phase quantique

4 Algorithme de Shor

Problème 2 (Shor)**.** *Soit un entier* $N = p \times q$*, avec* p *et* q *nombres premiers grands. Le problème est de trouver les facteurs premiers* p *et* q *de* N *dans un temps raisonnable.*

```
Data: N
repeat
    choose a coprime with N ;
    find smallest r such that a^r ≡ 1(modN) ;
    if r is even then
        x ≡ a^(r/2)(modN) ;
        if x + 1 ≢ 0(modN) then
            at least one of {p, q} ∈ {gcd(x + 1, N), gcd(x − 1, N)} ;
            break ;
        else
            continue ;
        end
    else
        continue ;
    end
until;
```