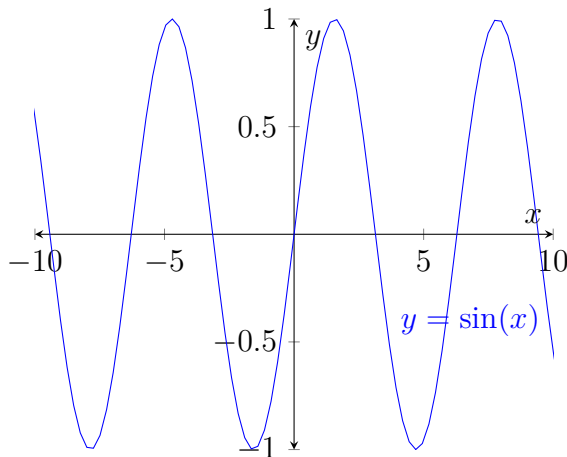


Algorithme de Shor

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 $f : x \rightarrow \sin x$. 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.

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

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 ;
until;

```
