2022-09-27

2.11 Estimation de phase (QPE)

UNe tranformation unitaire U, n'est pas nécessairement hérimitique. U n'est donc pas un observable (en générale). On peut toujours écrire U avec un observable A comme

$$U = e^{2\pi i A} = \sum_{\lambda=1}^{N} e^{2\pi i \varphi_\lambda} |\lambda\rangle\langle\lambda|$$

Si on suppose qu'on peut préparer un état $|\lambda\rangle$ et qu'un oracle puisse évaluer U. On veut estimer φ_λ

Pour se faire, on sépare le circuit en 2 registres

1. Un registre de t qubits $|0\rangle$
   plus t est grand et plus l'algorithme est précis et plus le succès est probable
2. l'état $|\lambda\rangle$

2.12 Algorithme de Shor

On veut, à partir de $a \in \mathbb{N}$, trouver $a_1, a_2 \in \mathbb{N} | a = a_1 \cdot a_2$

On combine la QFT et la QPW pour résoudre ce problème avec un ordinateur quantique

Classiquement, le meilleur algorithme connu à ce jour (number field sieve) à une complexité de $\exp\left\{O(n^{1/3}\log^{2/3} n)\right\}$
Quantiquement, en revanche, la complexité est de $O(n^2 \log n \log(\log n))$. Il y a donc un avantage exponentiel.

Le record de factorization classique est un nombre de 795 bits ! L'avantage quantique devra donc attendre pour des ordinateur quantique beaucoup plus performant que ceux qui existent actuellement.

L'algorithme de factorisation est basé sur le problème de la recherche d'ordre. On commence donc par cet aspect.

Rappel de notions d'arithmétique

On travaille ici avec seulement des entiers positifis ($\in \mathbb{N}^*$). Avec 2 nombres x et n, il existe une manière unique d'écrire

$$x = kn + r$$

où r est le reste ($x \mod n = r$) et $0 \leq r \leq n-1$.

- On dit que a divise b (a|b), si $b = ca$ avec $c \in \mathbb{N}$
- Le plus grand commun diviseur entre 2 nombres (a, b), noté pgcd(a, b), est sup$(c|(c|a)(\wedge c|b))$
- Si gcd$(a, b) = 1$, on dit que a et b sont co-premiers
- On peut trouver le gcd entre 2 nombres grace à l'algorithme d'Euclide
- Si $ab = cN$, N est composite et $a, b \neq dN$ alors soit gcd(a, N) ou gcd(b, N) est un facteur not-trivial de N

2.12.1 recherche d'ordre

Soit x, n des entiers positifs tel que $x < N$ est n'ayant aucun facteur commun. L' ordre de $x \mod n$ est le plus petit entier positif r tel que

$$x^r \mod N = 1$$

On veut déterminer r à partir de x et N (Un problème difficile classiquement)

ex : ordre de (4,7) : 3

En général, $x^{r+1} \mod N = x$ ou pour $t = ar + b$

$$x^t \mod N = x^b \mod N$$

Ce problème se résout à l'aide de l'algorithme QPE !

$$U_x |y\rangle = |xy \mod N\rangle$$

ave $y \in \mathbb{Z}_2^L$ où L est le nombre de bits nécéssaire pour représenter N ($L = \lceil \log_2 N \rceil$)

Il est important que (x,N) soit co premiers, sinon U_x n'est pas unitaire !

Pour $N \leq y \leq 2^L - 1$ on prend la convention que $xy \mod N = y$
U_x agit non-triviallemnt seulement sur $0 \leq y \leq N - 1$

On peut toujours écrire $U_x = \exp\{2\pi i A_x\}$ où

$$A_x = \begin{pmatrix} A_x & 0 \\ 0 & \mathbb{1}_{2^2-N} \end{pmatrix}$$

Si on applique U_x sur l'état suivant

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi isk}{r}} \left|x^k \mod N\right\rangle$$

On a

$$U_x |u_s\rangle = \cdots = e^{2\pi is/r} |u - x\rangle$$

$\implies |u_s\rangle$ est un état propre de U_x avec valeur propre $e^{2<piis/r}$

Pour préparer $|u_s\rangle$, Il faut connaître r (et donc la réponse). Il faut donc utiliser une astuce

$$\begin{aligned}
\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle &= \frac{1}{r} \sum_{sk} e^{-2\pi isk} r \left|x^k \mod N\right\rangle \\
&= \sum_k \left(\frac{1}{r} \sum_s e^{-2\pi isk/r} \right) \left|x^k \mod N\right\rangle \\
&= \sum_k \delta_{k,0} \left|x^k \mod N\right\rangle \\
&= |1\rangle
\end{aligned}$$

On peut donc initialiser l'algorithme de phase avec $|1\rangle$, ce qui est simple.

Avec l'algorithme QPE, on obtiens un estimé de $\varphi \approx \frac{s}{r}$ avec un s aléatoire

Il reste à extraire r de $\varphi \approx \frac{s}{r}$

On peut faire cela avec la méthode de l'expension de fraction continues.