FACTORISATION QUANTIQUE

PHILIPPE LANGEVIN

Résumé. Dans cette note, je rapporte quelques points de l'article de Peter Shor [**?**] sur la factorisation quantique. Un papier trés plaisant à lire qui est sans doute à l'origine d'un certain enthousiasme à l'égard du calcul quantique.

1. Factoriser

Il n'existe pas d'algorithme polynomial pour factoriser un entier N. Le temps de calcul du crible par les corps de nombre est de la forme :

$$\exp(\kappa \sqrt[3]{\log N (\log\log N)^2})$$

où κ est une constante inférieure à 2. En décembre 2009, la factorisation du challenge RSA-768, un entier de 232 chiffres décimaux a été annoncée, résultat obtenu après 2 ans et demi de calculs.

(1) 5To de données traitées ;

(2) Calcul distribué sur plus de 1700 coeurs.

Comme la plupart des bons algorithmes classiques, il tente de construire une solution non triviale à l'équation :

$$X^2 = Y^2 \pmod N,$$

de laquelle on peut tirer un facteur de N en calculant un diviseur commun à N et $Y - X$.

D'un autre coté, il suffirait d'engendrer les racines carrées de l'unité. Par le théorème chinois des restes, si N est impair alors il y en a 2^f où f est le nombre de facteurs premier de N.

Un algoritme capable de calculer l'ordre multiplicatif d'un inversible arbitraire donne automatiquement naissance à un algorithme de factorisation probabiliste. En effet, on choisit x au hasard, s'il n'est pas inversible c'est terminé. Sinon, son ordre b à de bonnes chances d'être pair et $y := x^{b/2}$ est une racine carrée de l'unité aléatoire.

C'est le point de vue utilisé par Shor.

2. Algorithme basique

Dans son article, Shor montre comment construire des circuits quantique pour calculer une transformation de Fourier discrète, ainsi qu'une exponentiation modulaire. Je suppose que le lecteur est familier avec le premier algorithme, et peut-être pas avec le second. Rappelons, qu'il s'agit de calculer $x^t \pmod n$, où x, t et n sont des entiers de grandes taille, on dispose d'un algorithme de complexité $\mathrm{O}\big((\log \mathrm{n})^3\big)$.

Date: Hiver 2012.

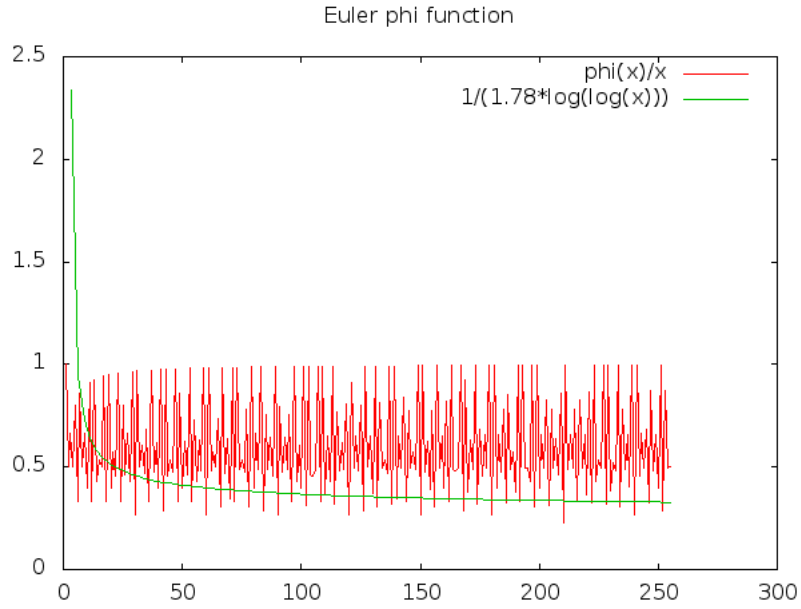

FIGURE 1. Dans Hardy et Wright [?] page , $\liminf \frac{\varphi(n)}{n} \log\log n = e^{-\gamma}$. où $\gamma = 0.577215665\ldots$ est la constante d'Euler. $e^{\gamma} = 1.7810724\ldots$.

```
Exponentiation( x, t, n : nombre )
variable
        y : nombre
debut
      y ← 1
      tant que ( t > 0 )
          si impair( n ) alors
              y ← y * x mod n
          fsi
          t ← t div 2
          x ← x * x  mod n
      ftq
      retourner y
fin
```

3. Faits Arithmétiques

La figure FIG. ?? illustre un premier fait arithmétique important pour l'approche de Shor. On peut montrer que pour $n > 2$,

$$\frac{n}{e^{\gamma}\ \log\log n + \frac{3}{\log\log n}} \leq \varphi(n)$$

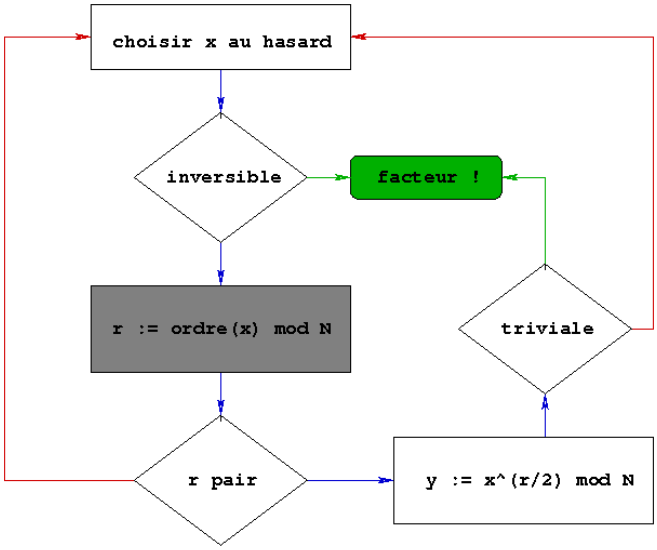

FIGURE 2. Au coeur de la méthode de Shor, le calcul quantique à pour objectif de déterminer la période multiplicative d'un élément arbitraire.

et pour une infinité de n :

$$\varphi(n) < \frac{n}{e^{\gamma} \log\log n}$$

La preuve de la seconde assertion est intéressante (Ribenboim) : elle se fait en deux temps. Dans un premier temps sous l'hypothèse de Riemann, puis dans un second temps, sans l'hypotèse de Riemann.

4. Méthode de Shor

On note Q une puissance de 2 satisfaisant à

$$N^2 \leq Q < 2N^2, \quad Q := 2^m \tag{1}$$

Soit x un résidu inversible modulo N de période p. Shor décrit les circuits de deux opérateurs unitaires. Le premier réalise une exponentiation modulaire, le second un calcul de la transformée de Fourier discrète :

$$X\colon |n\rangle|0\rangle \mapsto |n\rangle|x^n\rangle \quad F\colon |n\rangle \mapsto \frac{1}{\sqrt{Q}} \sum_{s=0}^{Q-1} \zeta_Q^{ns} |s\rangle$$

Comme d'hab, ζ_Q désigne la racine Q-ième primitive standard i.e. $\exp(2i\pi/Q)$.

On initialise uniformément un registre quantique de $2m$ bits :

$$|\psi\rangle = \frac{1}{\sqrt{Q}} \sum_{n=0}^{Q-1} |n\rangle|0\rangle$$

Un circuit quantique est appliqué pour réaliser X

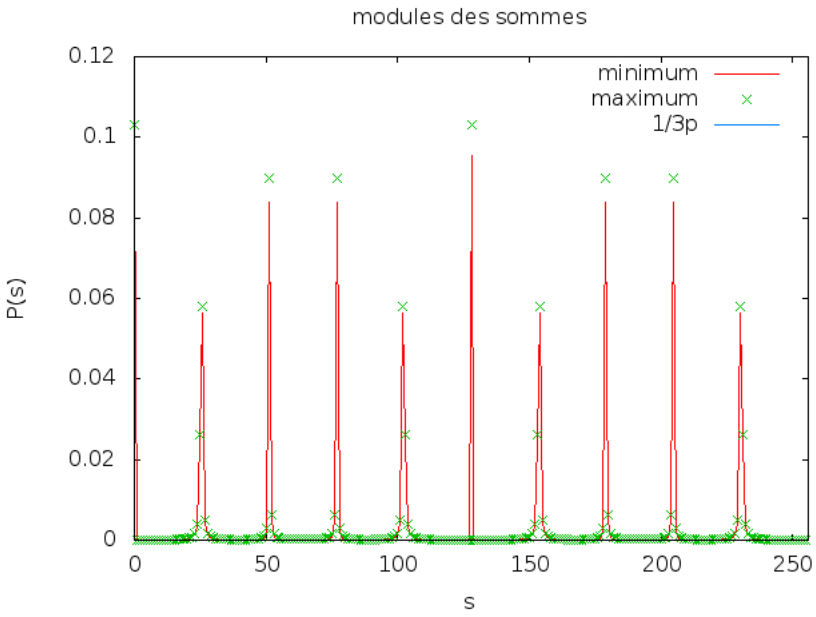

FIGURE 3. Modules des sommes partielles dans le cas $p = 13$ et $Q = 512$. Les pics se produisent quand s est multiples de p. Lorsque le reste minimal $\{ps\}_Q$ est inférieur à $p/2$ le module carré des sommes est minoré par $\frac{1}{3p^2}$

$$|X\psi\rangle = \frac{1}{\sqrt{Q}} \sum_{n=0}^{Q-1} |n\rangle|x^n\rangle$$

Un circuit de Fourier

$$|FX\psi\rangle = \frac{1}{Q} \sum_{n=0}^{Q-1} \sum_{s=0}^{Q-1} \zeta_Q^{ns} |s\rangle|x^n\rangle$$

On observe les composantes, par définition d'un système quantique, la propabilité de mesurer la direction $|s\rangle|y\rangle$ est égale au carré du module de la somme :

$$\frac{1}{Q} \sum_{x^n=y} \zeta_Q^{ns} \tag{2}$$

Condidérant $\{ps\}_Q$, le reste minimal de la division de ns par Q, Shor montre que si

$$|\{ps\}_Q| \leq \frac{p}{2} \tag{3}$$

alors la probabilité de l'observable $|s\rangle|y\rangle$ est supérieure à $\frac{1}{3p^2}$.

Les hypothèses (**??**) faites sur Q montrent qu'une seule fraction rationnelle vérifie

$$0 < |\frac{s}{Q} - \frac{d}{p}| \leq \frac{1}{2Q} \tag{4}$$

Elle peut être déterminée par une décomposition en fraction continue. Il montre que pour chaque entier t premier avec p, il existe au moins un s vérifiant (**??**), de sorte que la probabilité de déterminer la période de x est

$$P_{\text{succes}} \geq \frac{\varphi(p)p}{3p^2} \geq \frac{C}{\log\log p} \tag{5}$$

où C est une constante connue.

5. minoration d'une somme

On souhaite minorer le module de la somme trigonométrique

$$P(r,s) := \frac{1}{Q} \sum_{n \equiv r \pmod{p}} \zeta_Q^{ns}$$

où n décrit l'ensemble des résidus modulo Q. La figure FIG. **??** montre que cette somme est de module important quand s est un multiple de $[\frac{Q}{p}]$. Plus généralement, si $\{ps\}_Q$ est inférieur à $\frac{p}{2}$ alors on a la minoration :

$$|P(r,s)|^2 \geq \frac{1}{3p^2}$$

Posons $N = \lfloor \frac{Q-1-r}{p} \rfloor$, et $T := \{ps\}_Q$, il faut estimer le module des sommes

$$\frac{1}{Q} \sum_{q=0}^{N} \zeta_Q^{(qp+r)k} \rightsquigarrow \frac{1}{Q} \sum_{q=0}^{N} \zeta_Q^{qT} =: S(r,s)$$

L'approximation de cette somme par une intégrale s'écrit :

$$\frac{1}{Q} \sum_{q=0}^{N} \zeta_Q^{qT} = \frac{1}{Q} \int_0^{N+1} \zeta_Q^{Tx} \mathrm{d}x + \frac{1}{Q}\delta$$

où $\frac{1}{Q}\delta$ désigne le terme d'erreur. On commence par estimer ce terme.

$$\begin{aligned} \delta &= \sum_{q=0}^{N} \zeta_Q^{qT} - \int_0^{N+1} \zeta_Q^{Tx} \mathrm{d}x & &= \sum_{q=0}^{N} \zeta_Q^{qT} - \int_q^{q+1} \zeta_Q^{Tx} \mathrm{d}x \\ &= \sum_{q=0}^{N} \zeta_Q^{qT} - \zeta_Q^{qT} \int_0^1 \zeta_Q^{Ty} \mathrm{d}y & &= \sum_{q=0}^{N} \zeta_Q^{qT} \int_0^1 (1 - \zeta_Q^{Ty}) \mathrm{d}y \end{aligned}$$

On voit que si $|T| \leq \frac{p}{2}$ alors δ est borné et le terme d'erreur est $\mathrm{O}(\frac{1}{\mathrm{Q}})$.

Ce qui nous ramène à l'estimation d'une intégrale plus amicale que la somme discrète :

$$\begin{aligned}\int_0^{\lfloor\frac{Q-1-r}{p}\rfloor}\zeta_Q^{Tx}\mathrm{d}x &= \int_0^{\lfloor\frac{Q-1-r}{p}\rfloor}\exp(\frac{2i\pi Tx}{Q})\mathrm{d}x\\ &= \frac{Q}{p}\int_0^{\frac{p}{Q}\lfloor\frac{Q-1-r}{p}\rfloor}\exp(\frac{2i\pi Ty}{Q}\frac{Q}{p})\mathrm{d}y\\ &= \frac{Q}{p}\int_0^1\exp(\frac{2i\pi Ty}{p})\mathrm{d}y+\mathrm{O}(\frac{\mathrm{Q}}{\mathrm{p}})\\ &= \frac{Q}{p}\int_0^1\exp(2i\pi\theta)\mathrm{d}y+\mathrm{O}(\frac{\mathrm{Q}}{\mathrm{p}})\end{aligned}$$

Sur l'intervalle $-\frac{1}{2}\leq\theta\leq\frac{1}{2}$, l'intégrale est minimale au bord, on obtient le résultat annoncé.

6. Circuit

Dernière modification : P. Langevin à Toulon, Décembre 2012.

Références

[1] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5) :1484–1509, 1997.

Imath, université du sud Toulon Var.