Chapitre 3 : Algorithme de Shor

ENSIIE - Informatique quantique pour la recherche opérationnelle

Dimitri Watel (dimitri.watel@ensiie.fr)

2023

Algorithmes du chapitre

- **Algorithme de Shor** : décomposer un entier en facteurs premiers

- Plus rapide que les meilleurs algorithmes déterministes ou probabilistes
- Beaucoup d'arithmétique
- Utilise la transformée de Fourier quantique
- Basé sur la recherche d'une période d'une fonction dans un groupe fini

Problème à résoudre

Factorisation d'entier

Soit $n \in \mathbb{N}$ non premier produit de deux nombres premiers p et q, trouver p ou q.

Plan

Cas facile

Soit $a \in \mathbb{Z}/n\mathbb{Z}$ choisi au hasard.

Si $PGCD(n, a) = d \neq 1$ alors $d = p$ ou $d = q$.

Trouver un tel a est très improbable. Dans la suite, on suppose que $PGCD(a, n) = 1$.

Tactique arithmétique

Ordre d'un entier

Il existe $0 < r \leq n$ tel que $a^r \equiv 1 \mod n$.
Le plus petit entier r vérifiant cette proposition est l'ordre de a.

Preuve :
si $\varphi(n) = \#\{x \in \mathbb{Z}/n\mathbb{Z} | PGCD(x, n) = 1\}$, alors $a^{\varphi(n)} \equiv 1 \mod n$.

Tactique arithmétique

Décomposition d'un entier

Si

- a est d'ordre r
- si r est pair
- si $a^{r/2} + 1 \not\equiv 0 \mod n$

alors $(a^{r/2} + 1)$ et $(a^{r/2} - 1)$ sont des multiples de p et q.

Preuve :

- $a^r - 1 \equiv 0 \mod n$ donc $(a^{r/2} + 1) \cdot (a^{r/2} - 1) \equiv 0 \mod n$
- $a^{r/2} - 1 \not\equiv 0 \mod n$ par définition de r
- si $x \not\equiv 0 \mod n$ et $y \not\equiv 0 \mod n$ mais $xy \equiv 0 \mod n$ alors $PGCD(x, n) \neq 1$ et $PGCD(y, n) \neq 1$.

Algorithme de Shor

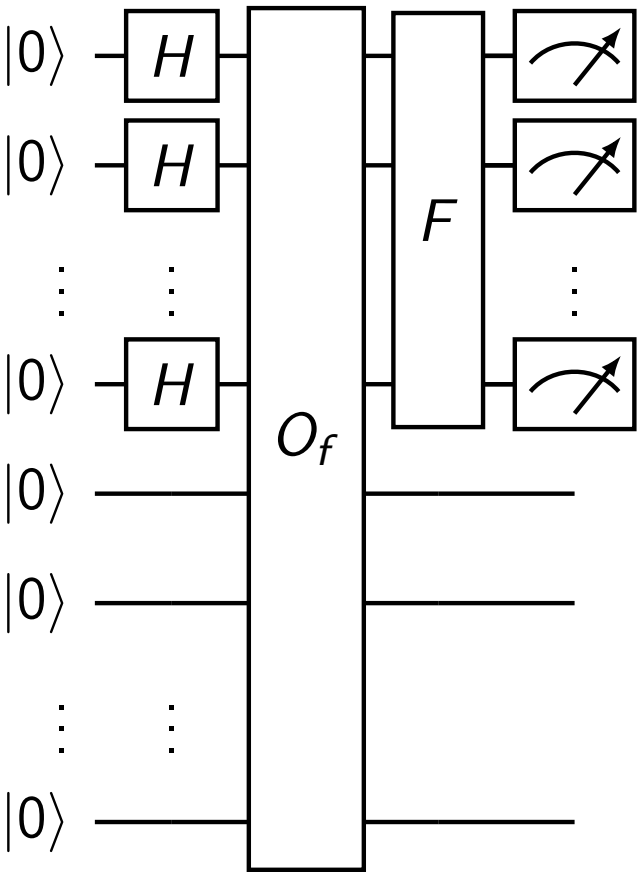
Comment casser RSA en 6 étapes

- Prendre $a \in \mathbb{Z}/n\mathbb{Z}$ au hasard
- Si $PGCD(a, n) = d \neq 1$, renvoyer d
- Sinon, trouver l'ordre r de a
- Si r est impair, recommencer
- Si $a^{r/2} + 1 \equiv 0 \mod n$, recommencer
- Sinon renvoyer $PGCD(a^{r/2} + 1, n)$ et $PGCD(a^{r/2} - 1, n)$.

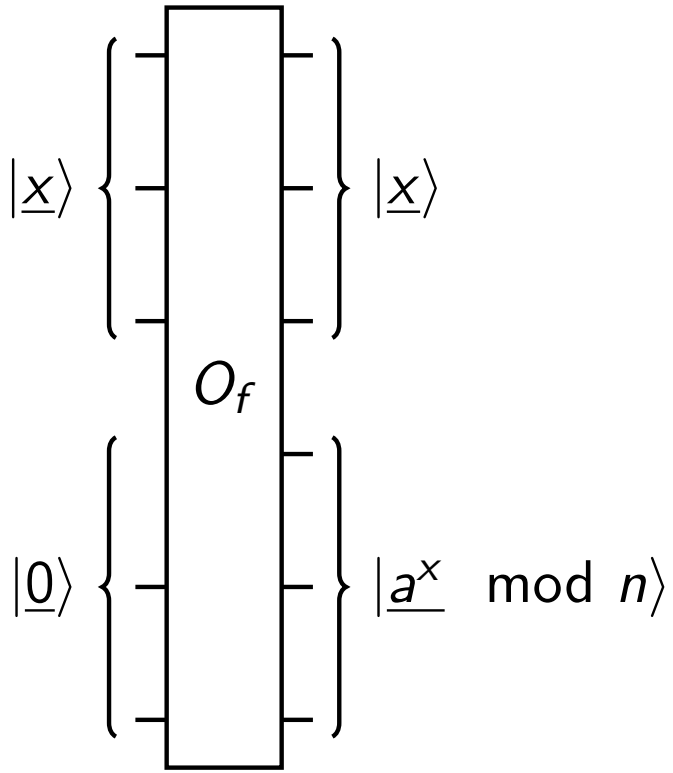
Problème : comment trouver r?

Plan

Description du circuit permettant de trouver r



avec

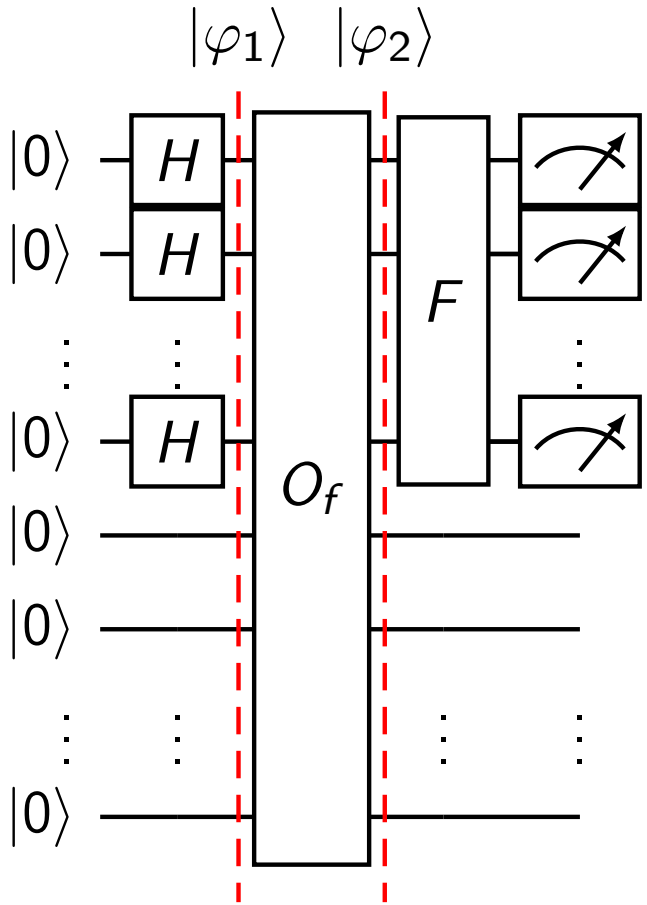


Il y a $2m$ qbits avec $2^m > n^2$.

O_f est un oracle, F est une transformée de Fourier quantique.

Valeur de $|\varphi_1\rangle$

Étudions les premiers qbits de ce circuit (on verra F plus tard).

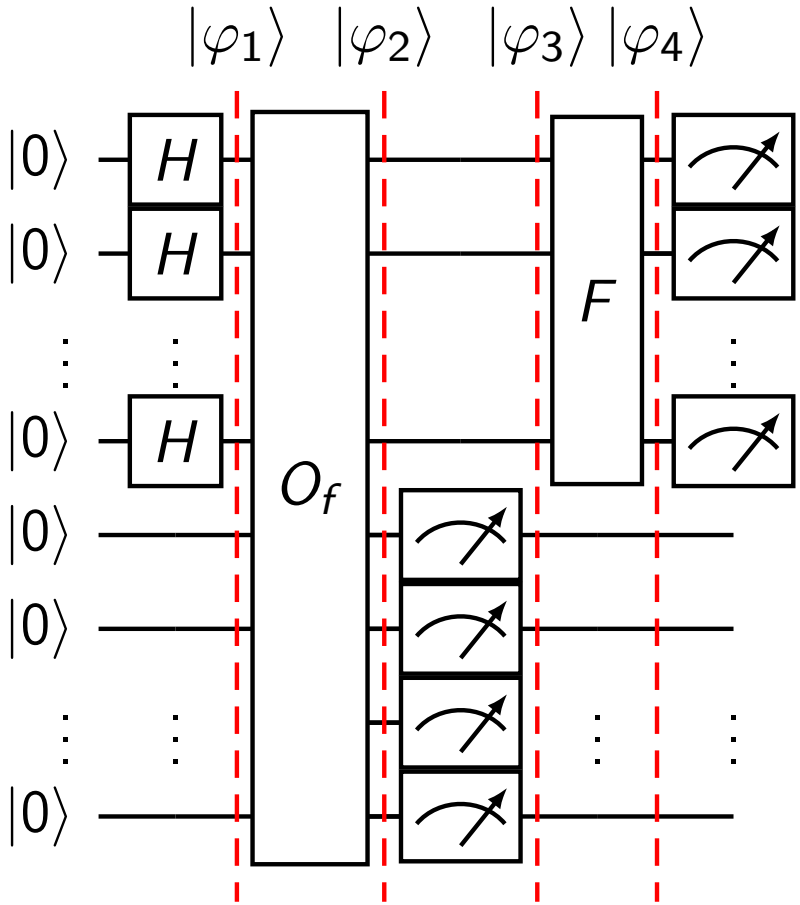


$$|\varphi_1\rangle = \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |\underline{x}\rangle \otimes |\underline{0}\rangle$$

Valeur de $|\varphi_2\rangle$

$$
\begin{aligned}
|\varphi_2\rangle &= O_f\,|\varphi_1\rangle \\
&= O_f \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |\underline{x}\rangle \otimes |\underline{0}\rangle \\
&= \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |\underline{x}\rangle \otimes |\underline{a^x \mod n}\rangle
\end{aligned}
$$

Simplification : mesure partielle des m derniers qbits



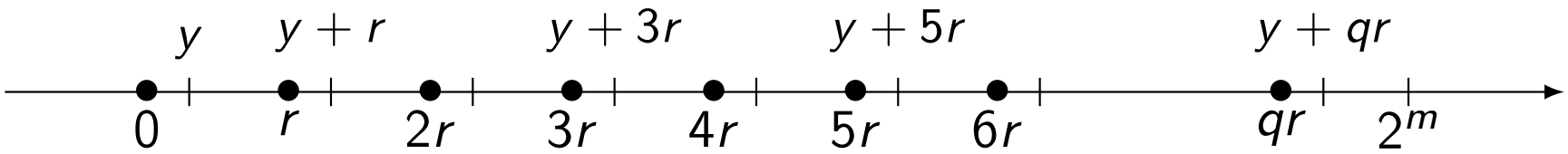
On mesure une valeur $a^y \mod n$ sur les derniers registres.

Simplification : mesure partielle des m derniers qbits

Les premiers registres s'effondrent sur les valeurs x telles que $a^x \equiv a^y \mod n$. On suppose $y < r$.

On pose

$$\begin{aligned} X_y &= \{x \leq 2^m - 1 | a^x \equiv a^y \mod n\} \\ &= \{x \leq 2^m - 1 | a^{x-y} \equiv 1 \mod n\} \\ &= \{x \leq 2^m - 1 | x - y = kr, k \in \mathbb{N}\} \end{aligned}$$



Posons $2^m = qr + r'$

si $y < r'$ alors $|X_y| = q + 1$

si $y \geq r'$ alors $|X_y| = q$

Cas simple : $2^m = qr$

Si r divise 2^m alors $|X_y| = q$ pour tout y

$$|\varphi_3\rangle = \frac{1}{\sqrt{|X_y|}} \sum_{x \in X_y} |x\rangle \otimes |\underline{a^y \mod n}\rangle$$

$$= \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} |\underline{kr + y}\rangle \otimes |\underline{a^y \mod n}\rangle$$

Alerte : confusion

Cette mesure partielle n'est pas nécessaire à l'algorithme, elle simplifie juste le calcul. On peut très bien s'en passer.

A ce stade, mesurer une valeur $kr + y$ ne nous apprend rien car nous ne connaîtrions ni k ni y.

Cas pas simple : $2^m \neq qr$

$$|\varphi_3\rangle = \frac{1}{\sqrt{|X_y|}} \sum_{x \in X_y} |\underline{x}\rangle \otimes |\underline{a^y \mod n}\rangle$$

$$= \frac{1}{\sqrt{|X_y|}} \sum_{k=0}^{\left\lfloor \frac{2^m - 1 - y}{r} \right\rfloor} |\underline{kr + y}\rangle \otimes |\underline{a^y \mod n}\rangle$$

On reviendra sur ce cas plus tard.

Transformée de Fourier quantique

Définition

Posons $\omega = e^{\frac{2i\pi}{2^m}}$. La transformée de Fourier quantique F est la porte :

$$F\left|\underline{x}\right\rangle = \sum_{y=0}^{2^m-1} \omega^{xy} \left|\underline{y}\right\rangle$$

Note : $\omega^{2^m} = 1$

A quoi sert la transformée de Fourier quantique?

Ressemblance

$$F\left|\underline{x}\right\rangle = \frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^m-1} \omega^{xy} \left|\underline{y}\right\rangle$$

$$H^{\otimes m}\left|\underline{x}\right\rangle = \frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^m-1} (-1)^{\underline{x}\cdot\underline{y}} \left|\underline{y}\right\rangle$$

On peut noter que $F\left|\underline{0}\right\rangle = H^{\otimes m}\left|\underline{0}\right\rangle$

La transformée de Fourier quantique est une autre manière de superposer des qbits.

Transformation unitaire

Exercice

Montrer que la transformée de Fourier quantique est une transformation unitaire.

Preuve :

- Idée 1 : une transformation est unitaire si elle envoie une base orthonormée sur une autre base orthonormée. Pour $|\varphi_1\rangle = F\,|\underline{x}\rangle$ et $|\varphi_2\rangle = F\,|\underline{y}\rangle$ montrer que $\langle\varphi_1|\varphi_2\rangle = 1$ si $x = y$ et 0 sinon.
- Idée 2 : montrer que $F^* = F^{-1}$.

Comment l'implanter ?

Théorème

On peut implanter la transformer de Fourier quantique avec $O(n^2)$ portes à 1 ou 2 qbits.

Preuve : plus tard, on finit l'algorithme d'abord.

Valeur de $|\varphi_4\rangle$

$$
\begin{aligned}
|\varphi_4\rangle &= (F \otimes Id)\,|\varphi_3\rangle \\
&= F\left(\frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\left|\underline{kr+y}\right\rangle\right) \otimes \left|\underline{a^y \mod n}\right\rangle
\end{aligned}
$$

Exercice

Montrer que $|\varphi_4\rangle = \frac{1}{\sqrt{q2^m}}\sum_{z=0}^{2^m-1}\left(\sum_{k=0}^{q-1}\omega^{krz}\right)\omega^{yz}\,|\underline{z}\rangle \otimes \left|\underline{a^y \mod n}\right\rangle$

Valeur de $|\varphi_4\rangle$

$$|\varphi_4\rangle = \frac{1}{\sqrt{q2^m}} \sum_{z=0}^{2^m-1} \left(\sum_{k=0}^{q-1} \omega^{krz} \right) \omega^{yz} |\underline{z}\rangle \otimes |\underline{a^y \mod n}\rangle$$

$$\sum_{k=0}^{q-1} \omega^{krz} = \sum_{k=0}^{q-1} e^{\frac{2i\pi}{2^m} krz} = \sum_{k=0}^{q-1} e^{\frac{2i\pi}{q} kz} = \begin{cases} q \text{ si } z = 0 \mod q \\ 0 \text{ sinon} \end{cases}$$

$$|\varphi_4\rangle = \frac{1}{\sqrt{r}} \sum_{\substack{z=0 \\ z=0 \mod q}}^{2^m-1} \omega^{yz} |\underline{z}\rangle \otimes |\underline{a^y \mod n}\rangle$$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{2^m/q-1} \omega^{ykq} |\underline{kq}\rangle \otimes |\underline{a^y \mod n}\rangle$$

Mesure de $|\varphi_4\rangle$

$$|\varphi_4\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{2^m/q-1} \omega^{ykq} \left|\underline{kq}\right\rangle \otimes \left|\underline{a^y \mod n}\right\rangle$$

Mesure

En mesurant $|\varphi_4\rangle$, on obtient un entier kq multiple de $q = \frac{2^m}{r}$.

$$\frac{kq}{2^m} = \frac{k}{r} \begin{cases} \nearrow\ k = 0? \to \☹ \\ \searrow\ \frac{k}{r} = \frac{PGCD(k,r)k'}{PGCD(k,r)r'} = \frac{k'}{r'} \begin{cases} \nearrow\ r' \neq r? \to \☹ \\ \qquad (PGCD(r,k) \neq 1) \\ \searrow\ r' = r? \to \☺ \end{cases} \end{cases}$$

On s'arrête dans le dernier cas, sinon on recommence et on croise les doigts.

Plan

Et maintenant ?

Questions en suspens

- Comment faire F ?
- Et si r ne divise pas 2^m ?
- Pourquoi avoir pris $2^m > n^2$?
- On recommence l'algo si
  - r est impair
  - $a^{\frac{r}{2}} + 1 \equiv 0 \mod n$
  - $k = 0$ ou $PGCD(r, k) \neq 1$

Combient de fois faut-il le recommencer ?

Commence faire F : étape 1, réécrire $F|x\rangle$?

Théorème

Posons $\underline{x} = x_{m-1} \dots x_2 x_1 x_0$

$$F|\underline{x}\rangle = \frac{1}{\sqrt{2^m}} \bigotimes_{k=1}^{m} \left(|0\rangle + \exp(2i\pi \cdot \sum_{j=0}^{k-1} \frac{x_j}{2^{k-j}}) |1\rangle \right)$$

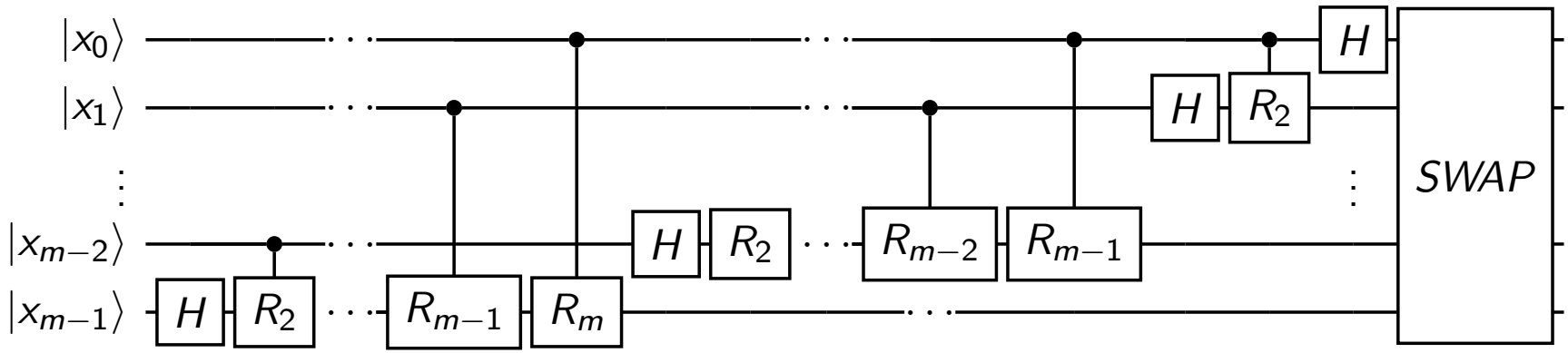
Preuve :

- Montrer que $F|\underline{x}\rangle = \frac{1}{\sqrt{2^m}} \bigotimes_{k=1}^{m} \left(|0\rangle + \exp(2i\pi \cdot \frac{x}{2^k}) |1\rangle \right)$ en développant ce produit.
- Poser $x = \sum_{j=0}^{m-1} x_j 2^j$
- Déduire le résultat

Commence faire F : étape 2, encoder $F|x\rangle$?

$$F|\underline{x}\rangle = \frac{1}{\sqrt{2^m}} \bigotimes_{k=1}^{m} \left(|0\rangle + \exp(2i\pi \cdot \sum_{j=0}^{k-1} \frac{x_j}{2^{k-j}}) |1\rangle \right)$$

Soit R_k la porte $\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^k}} \end{pmatrix}$, alors ce circuit code F:



Et si r ne divise pas 2^m ? Pourquoi $2^m > n^2$?

On pose $2^m = qr + r'$ avec $r' > 0$

Ce qui change

Si r ne divise pas 2^m, alors:

- $\omega^r = e^{\frac{2i\pi r}{2^m}} \neq e^{\frac{2i\pi}{q}}$
- Donc $\sum_{k=0}^{q-1} \omega^{krz} = \sum_{k=0}^{q-1} e^{\frac{2i\pi}{2^m} rkz} \neq \begin{cases} q \text{ si } z = 0 \mod q \\ 0 \text{ sinon} \end{cases}$

À la place, on a

$$\sum_{k=0}^{q-1} \omega^{krz} = \sum_{k=0}^{q-1} e^{\frac{2i\pi}{2^m} rkz} \simeq \begin{cases} q \text{ si } z \approxeq 0 \mod \frac{2^m}{r} \\ 0 \text{ sinon} \end{cases}$$

Les entiers z proches des multiples de $\frac{2^m}{r}$ tombent avec une bonne probabilité.

Simulation

Démo en direct

Fraction continue

Définition

Soit une suite $(u_n)_{n\in\mathbb{N}}$ d'entiers, alors la fraction continue associée à cette suite est la limite de la fraction:

$$x = \lim_{n\to+\infty} f_n = u_0 + \cfrac{1}{u_1 + \cfrac{1}{u_2 + \cfrac{1}{\cdots + \cfrac{1}{u_n}}}}$$

La n^{ieme} fraction f_n est un rationnel qui approche f.

Comment trouver r ?

Soit $k \in \mathbb{N}$ et z l'entier le plus proche de $k\frac{2^m}{r}$, alors $\left|z - \frac{k2^m}{r}\right| \leq \frac{1}{2}$.

Théorème

Si $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$, alors $\frac{p}{q}$ est une des fractions du développement en fractions continues de x.

Exercice : montrer que si $2^m > n^2$ alors $\left|\frac{z}{2^m} - \frac{k}{r}\right| < \frac{1}{2r^2}$.

Théorème

Si $z = kq$ alors développer $\frac{z}{2^m}$ en fractions continues donne une fraction $\frac{k}{r}$ en $O(\log(r)^3)$ étapes.

Note : cette fraction est la dernière où le dénominateur est plus petit que n.

Quelle probabilité de succès ?

Probabilité de mesurer l'entier le plus proche de $k\frac{2^m}{r}$

Si $\left|z - \frac{k2^m}{r}\right| \leq \frac{1}{2}$, alors cette probabilité vaut au moins $\frac{1}{3r}$.

Preuve : voir le papier de Shor.

Complexité : combien de fois faut-il recommencer ?

Quelles sont les probabilités de recommencer l'algorithme ?
On rappelle que

- on mesure un entier z proche de $\frac{2^m k}{r}$
- on effectue le développement en fractions continues de $\frac{z}{2^m}$. On trouve une fraction $\frac{k'}{r'}$ égale à $\frac{k}{r}$
- si $PGCD(r,k) = 1$ alors $r' = r$

On recommence si $k' = 0$ ou $PGCD(k,r) \neq 1$

La probabilité de mesurer un entier z qui n'est pas dans cette situation est $\Theta\left(\frac{1}{\log\log(r)}\right)$

Preuve (indices)

- $\varphi(r) = \#\{k | PGCD(k,r) = 1\}$
- $\frac{\varphi(r)}{r} = \Theta\left(\frac{1}{\log\log(r)}\right)$ (cf : Wikipedia)

Complexité : combien de fois faut-il recommencer ?

Quelles sont les probabilités de recommencer l'algorithme ?

On recommence si r est pair ou $a^{r/2} + 1 \equiv 0 \mod n$

Ce cas arrive avec une probabilité au plus $\frac{1}{2}$.

Preuve : avez-vous encore 2h devant vous ?

Complexité : combien de fois faut-il recommencer ?

Théorème

L'algorithme de Shor recommence en moyenne $O(\log\log(r))$ fois avant de trouver r.

Preuve (peu rigoureuse)
R : nombre de répétitions.

- On choisi a
- On trouve r avec en moyenne $O(\log\log(r))$ répétitions
- On recommence avec une probabilité $\frac{1}{2}$
- $\Rightarrow \forall i \in \mathbb{N}$, la probabilité que $R = O(i\log\log(r))$ répétitions est $\frac{1}{2^i}$.

$$E(R) = O(\sum_{i=1}^{+\infty} \frac{i}{2^i}\log\log(r)) = O(2\log\log(r))$$

Complexité de l'algorithme

On recommence en moyenne $O(\log\log(r))$ fois

- le circuit avec $m = O(\log(n))$ qbits
- des portes H et O_f de tailles $O(m)$
- la porte F de taille $O(m^2)$
- la recherche de r avec les fractions continues en $O(\log(r)^3)$

avec $m = O(\log(n))$ et $r = O(n)$.
Donc l'algorithme est polynomial.