Analyse du Proc de Mesure Algo de Shor.

- Comment extraire la période r de f à partir des entiers y obtenus lors de plusieurs mesures ?

- $$\mathrm{Prob}(y) = \frac{1}{M^2} \sum_{x_0=0}^{r-1} \left| \sum_{j=0}^{j_{max}(x_0)} e^{2\pi i \frac{jy}{M/r}} \right|^2 .$$

(ds les notes du cours $j_{max}(x_0) = A(x_0) - 1$).

(en gros $j_{max}(x_0) \approx \frac{M}{r} - 1 \ldots$).

Allure de Prob(y) ? deux cas

cas irréaliste mais mathématiquement simple

$\frac{M}{r}$ est entier.

$$j_{max}(x_0) = \frac{M}{r}$$

$\Rightarrow$ Calculer Prob(y).

cas réaliste.

r ne divise pas M

r : inconnu ; M : notre choix

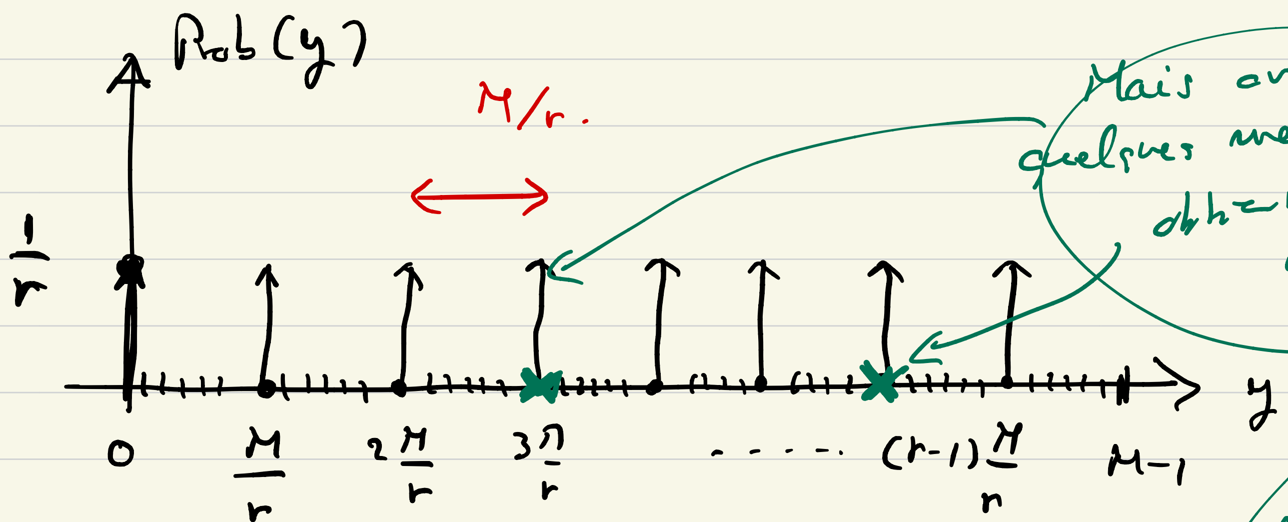
analyse mathématique plus compliquée mais les idées sont "essentiellement" les m̂.

Cas irréaliste où r divise M.

$$\text{Prob}(y) = \frac{1}{M^2}\sum_{x_0=0}^{r-1}\left|\underbrace{\sum_{j=0}^{M/r-1} e^{2\pi i \frac{jy}{M/r}}}\right|^2 .$$

$\frac{M}{r}-1$ est entier

somme géométrique de raison $\left(e^{2\pi i \frac{y}{M/r}}\right)$. calcul de la métho.



Mais avec uniquement quelques mesures on obtient quelques entiers !

pas évident d'extraire M/r et r !!!

$M \gg r$ $\quad \frac{M}{r}$ est énorme en pratique.

première remarque : si nous faisons énormément de mesures cela permettrait d'obtenir cette série de pics.
et comme M est connu grâce à $\frac{M}{r}$ → on déduit r !!!

10^{23} Molécules artificielles chacune joue le rôle d'un petit ordinateur ⇝ Manip 20 bits quantiques → ça marche 2000.
⇝ fact 15 en 21.

• En fait lors d'une mesure on obtient ici

$$y = k\frac{M}{r} \quad \text{avec} \quad k \in \{0, \dots, r-1\}$$

et avec une prob $\frac{1}{r}$.

ici remarquez que y est connu (obt par l'exp).

M est connu (notre choix).

$$\Rightarrow \underbrace{\frac{y}{M}}_{\text{rapport est connu.}} \underset{\text{on sait}}{=} \frac{k}{r}$$

comment trouver r ?

• Si vous prenez $\frac{y}{M}$ et vous la simplifiez $\rightarrow$ plusieurs candidats pour k et r.

• En pratique : on simplifie $\frac{y}{M}$ et on regarde tous les candidats k et r / on vérifie si $f(x+r) = f(x)$ ce qui est facile en général.

$\rightarrow$ on va trouver r comme cela.

Nb d'op à faire $\approx$ Nb max de simplifications

$$\approx (\log_2 M .) \approx (\log_2 r .) \approx (\log_2 N).$$

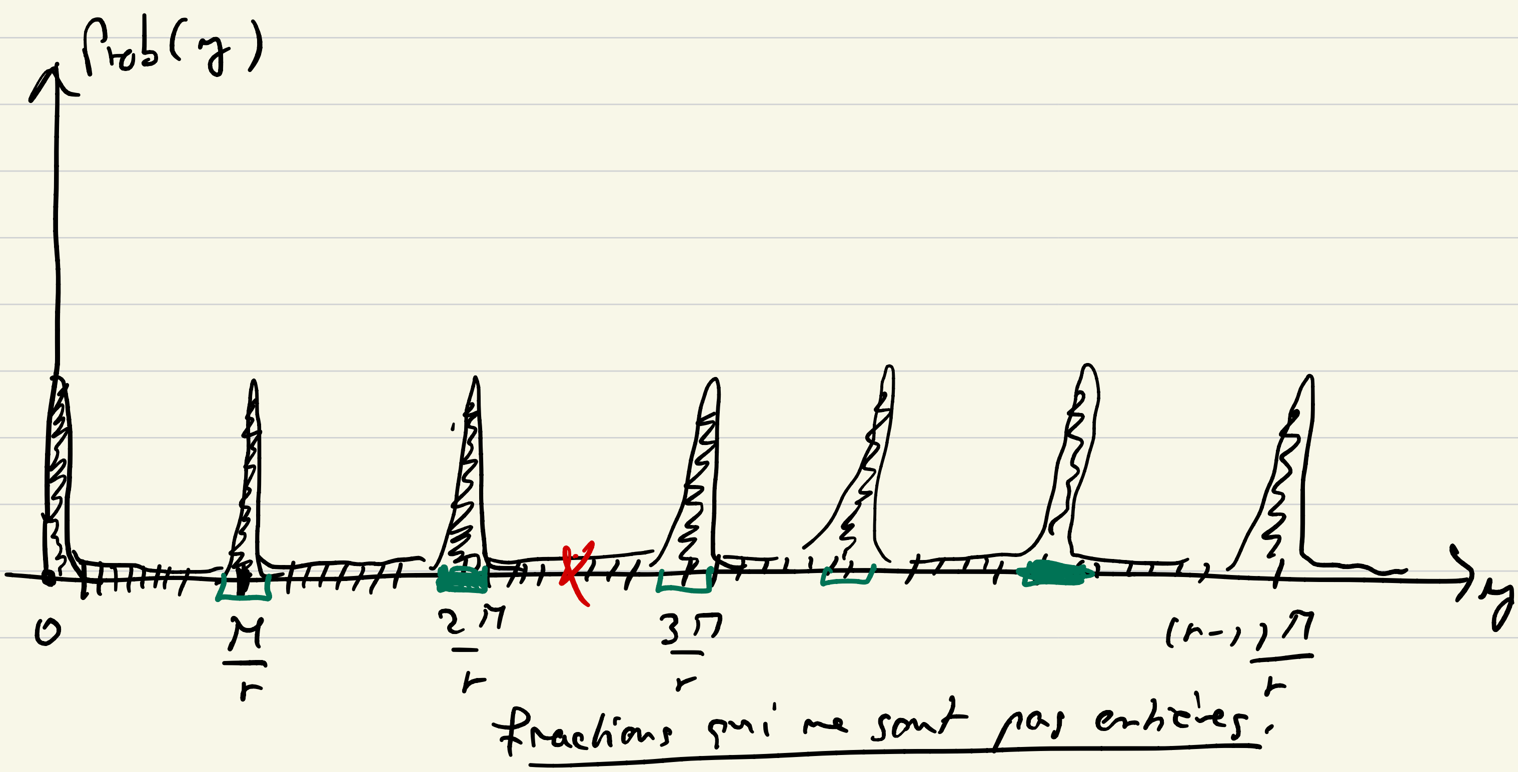
complexité polynomiale de la longueur de M.

• **Cas réaliste où r ne divise pas M.**

Prob(y) est plus compliquée car $j_{max}(x_0) \neq \frac{M}{r} - 1.$

$\uparrow$

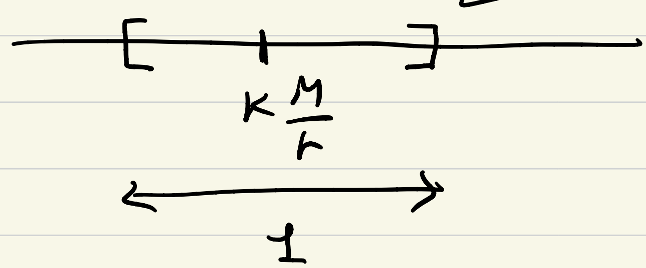
difficile à calculer.



Lemme :

Soit $I = \bigcup_{k=0}^{r-1} I_k$.

avec $I_k = \left[\underbrace{k \frac{M}{r}} - \frac{1}{2} \,,\, \underbrace{\frac{kM}{r}} + \frac{1}{2} \right]$



alors $\text{Prob}\left(y \in \bigcup_{k=0}^{r-1} I_k\right) = \text{Prob}(y \in I)$

$$\geqslant \frac{2}{5}$$

$\square$

- On a beaucoup de prob de trouver $y \approx \underbrace{k \frac{M}{r}}_{\text{pas un entier.}}$

  entier

- Plus précisément $\frac{kM}{r} - \frac{1}{2} \leq y \leq \frac{kM}{r} + \frac{1}{2}$

$\iff$ $\left| y - k\frac{M}{r} \right| \leq \frac{1}{2}$ . .

• Supposons que $y \in I_k$; $k = \{0, \dots, r-1\}$

$$\boxed{\left| \frac{y}{M} - \frac{k}{r} \right|} \leq \frac{1}{2M} \boxed{\leq \frac{1}{2r^2}} .$$

en pratique

$M \sim N^2$ factorisable.

et $\underbrace{r < N}$

• Les théoriciens des nombres connaissent bien ce genre d'inégalités :

$$\boxed{\begin{array}{l}\text{Théorie des fractions Continues :}\\ \text{Si le } PGCD(k, r) = 1 \text{ alors toutes les solutions } (k, r) \text{ de } \left| \frac{y}{M} - \frac{k}{r} \right| \leq \frac{1}{2r^2}\\ \text{sont données par les convergents de } \frac{y}{M} \text{. et on peut les calculer par un alg d'Euclide.}\end{array}}$$

<u>Théorie des fractions Continues :</u>

Si le $PGCD(k, r) = 1$ alors toutes les solutions de $\left| \underbrace{\frac{y}{M}}_{\text{connu}} - \frac{k}{r} \right| \leq \frac{1}{2r^2}$

(k, r) inconnu.

sont données par les <u>convergents</u> <u>de</u> $\frac{y}{M}$. et on peut les calculer par un alg d'Euclide.

Petite incursion dans la théorie des nombres.

$$\frac{y}{M} = \frac{185}{263}.$$

(Théorie des fractions continues).

→ Sur un exemple de la fraction $\frac{263}{189}$.

→ Représentation en fraction continue :

PGCD (263, 189). par l'alg d'Euclide :

$$\left.\begin{aligned} 263 &= 1 \cdot 189 + 74 \\ 189 &= 2 \cdot 74 + 41 \\ 74 &= 1 \cdot 41 + 33 \\ 41 &= 1 \cdot 33 + 8 \\ 33 &= 4 \cdot 8 + 1 \end{aligned}\right\} \Rightarrow$$

$$\frac{263}{189} = 1 + \frac{74}{189}$$

$$= 1 + \cfrac{1}{\cfrac{189}{74}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{41}{74}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{\cfrac{74}{41}}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{33}{41}}}$$

$$= \ldots$$

combien de div ? $(\log N)$

chaque div $(\log N)^2$

compl totale de l'alg d'Euclide

$O((\log N)^3)$

→

Finalement

$$\frac{263}{189} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{8}}}}}$$

$$= [1 ; 2 ; 1 ; 1 ; 4 ; 8]$$

$$\frac{189}{263} = 0 + \frac{1}{\cdots\cdots}$$

$$= [0 ; 1 ; 2 ; 1 ; 1 ; 4 ; 8].$$

Par définition les "convergents" sont les fractions continues tronquées :

$[0 ; 1]$ $[0, 1, 2]$ $[0, 1, 2, 1]$ $[0, 1, 2, 1, 1]$

$[0, 1, 2, 1, 1, 4]$ $[0, 1, 2, 1, 1, 4, 8]$.

Chaque convergent est une meilleure approx de $\frac{189}{263}$.

Théorème en th des nbs :

Si $\left| \frac{y}{M} - \frac{k}{r} \right| \leqslant \frac{1}{2r^2}$ et si $PGCD(k,r)=1$

alors $\frac{k}{r}$ est nécessairement un convergent de $\frac{y}{M}$, et

en plus toute sol (k, r) est un convergent de $\frac{y}{M}$.

#

Revenons à notre problème : il suffit à partir

de y obs et M choisit de calculer tous les

convergents de $\frac{y}{M}$. $\longrightarrow (k, r)$.

et on vérifie si r est une période. $f(x+r)=f(x)$

#.

Quelle est la prob de succès de cette procédure

- succès correspond à la réunion

① $y \in I = \bigcup_k I_k$

$$\left| y - k\frac{n}{r} \right| \leq \frac{1}{2}.$$

prob $\geq \frac{2}{5}$. (Lemme)

② $PGCD(k, r) = 1$. pour appliquer la théorie des convergents.

$$\text{prob}\,(\,PGCD(k,r) = 1\,) = \;?$$

- Ici $k \in \{0, 1, \ldots, r-1\}$. on tire k aléatoirement unif avec prob $\frac{1}{r}$.

- Lemme de Th des nombres: $\text{Prob}\,(PGCD(k,r) = 1) \geq \frac{1}{5\ln(\ln r)}$

"pas si faible que ça". $\longrightarrow$

- La prob totale de succès lorsqu'une exp :

$$\text{Prob}\left(\text{bon ordre } y \in I_k \text{ avec } PGCD(k,r)=1\right)$$

$$\geq \frac{2}{5} \cdot \frac{1}{4 \,\underbrace{\ln(\ln r)}}.$$

- En pratique cette prob peut être amplifiée en faisant plusieurs exp. (T exp.).

Pour l'amplification à $(1-\epsilon)$:

$$T \approx O\left(|\ln \epsilon| \underbrace{\ln(\ln r)}\right).$$

$$T \approx O\left(|\ln \epsilon| \ln(\ln N)\right).$$

d'exp pas si grand que ça pour N ← 400 décimal

- Finalement complexité de l'algo est celle de l'alg d'Euclide pour trouver les convergents

$\longrightarrow O\left((\ln N)^3\right)$

suite et fin dans la prochaine semaine.