

Kwantowa Transformata Fouriera i jej zastosowanie

1. Wstęp

Algorytm Shora (1993)

Redukuje liczbę n bitowej no. cyfrowej prędkości
w czasie n^3

Klasyczny problem bitowy ale jednocześnie
bitowy (RSA).

Jeśli N liczbę n bitowa $N < 2^n$

nieznaną metodą:

- sprawdzanie cyfrylicji się przez wszystkie liczby
mniejsze od N (w zakresie \sqrt{N})

można $\sim 2^{\frac{n}{2}}$ operacji

Czas obliczeń rośnie wykładniczo.

- Nieefektywny algorytm klasyczny można
skrócić:

$\sim 2^{\sqrt{n}}$ symboli nie dających ułamek

Algorytm jest skomplikowany, ale przedstawia
@Utwórca to kwantowa transformata Fouriera

2. Transformata Fouriera klasycznie

• Klasyczne dyskretna transformacja Fouriera

$$x_0, \dots, x_{N-1}$$

↓ \mathcal{F}

$$y_k = \frac{1}{\sqrt{N}} \sum_j e^{\frac{2\pi i j k}{N}} x_j$$

$$y_0, \dots, y_{N-1}$$

Liczba operacji: N^2 , inaczej 2^{2n}
(jeśli N liczb n bitów)

FFT ma trochę przyspieszy $N \log N = 2^n n$
wciąż wykorzystano 2 liczby bitów mniejszych dane

3. Kwantowa transformacja Fouriera

definiujemy operację unitarną U_F na stanach n qubitów

$$|j\rangle \xrightarrow{U_F} \frac{1}{\sqrt{N}} \sum_k e^{\frac{2\pi i j k}{N}} |k\rangle \quad N=2^n$$

Można sprawdzić że jest unitarna.

Jeśli rozpięty nasz dane jak poniżej:

$$\begin{aligned} \sum_j x_j |j\rangle &\xrightarrow{U_F} \sum_j \frac{1}{\sqrt{N}} \sum_k x_j e^{\frac{2\pi i j k}{N}} |k\rangle = \\ &= \sum_k y_k |k\rangle \end{aligned}$$

gdzie $y_k = \frac{1}{\sqrt{N}} \sum_j x_j e^{\frac{2\pi i j k}{N}}$ to liczy

można mieć ciekawą transformację Fouriera.

Waga i $\frac{p}{a}$

- nie chodzi o 2 macierze odwrotne, występuje jak na razie, czyli ten law. parabolizm może być sprytnie użyć dalej (chociaż się to może nie udać w alg. Shora

- V_F trzy funkcje zbudować z 2 el formuł kwantowych i pytanie jak to się składa z n , chociaż się nie b. dobrze bo n^2

Czyli mamy myśl w parawanu 2. Wersyjami FFT jak n^2 do $n^2 \ln$

Wykni, duży, zysk,

4. Co ma trans. Fouriera do redukcji na cyfry przewide?

Transf. Fouriera pozwala znajdować okres funkcji!

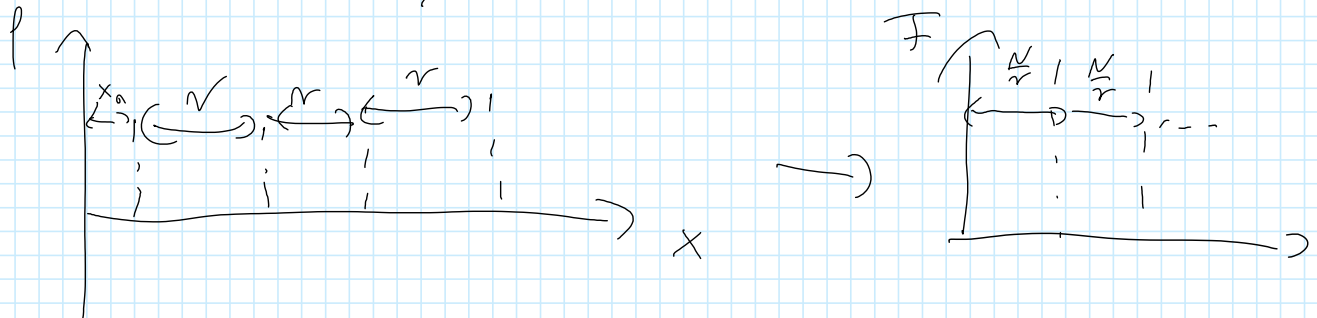
Rozwój funkcje $f: \mathbb{Z}_N \rightarrow \mathbb{Z}$

\uparrow
 cyfrowe mod N

Szukam jest okresu $f(x+r) = f(x)$ {symmetryczna na okresie

Liczmy dla wyjątków argumentów

$$|p\rangle = \frac{1}{\sqrt{N}} \sum_{x=c}^{N-1} |x\rangle |f(x)\rangle$$



Miemy drugi rejestr jest wyrażone y_0

$$\rightarrow N = k \cdot r, \quad \frac{1}{\sqrt{k}} \sum_{k=0}^{k-1} |x_0 + kr\rangle |y_0\rangle, \quad f(x_0) = y_0$$

$|\Psi_{x_0, r}\rangle$

Mając stan $|\Psi_{x_0, r}\rangle$ chcemy stworzyć funkcję
 jest $r \geq 2$. Mianem x nie może być odległości
 $x_0 + kr$ i nie może być więcej, ale

możemy zrobić transformację

$$\begin{aligned} F(|\Psi_{x_0, r}\rangle) &= \frac{1}{\sqrt{N}} \frac{1}{\sqrt{k}} \sum_{k=0}^{k-1} \sum_{l=0}^{N-1} e^{\frac{2\pi i l (x_0 + kr)}{N}} |l\rangle = \\ &= \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} e^{\frac{2\pi i l x_0}{N}} |l\rangle \cdot \frac{1}{\sqrt{k}} \sum_{k=0}^{k-1} e^{\frac{2\pi i l r \cdot k}{N}} = \end{aligned}$$

$$\sqrt{k} \quad \text{jeśli } l \cdot r = s \cdot N$$

$$l = s \cdot \frac{N}{r}$$

$$= \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{\frac{2\pi i s x_0}{r}} \left| s \cdot \frac{N}{r} \right\rangle$$

Teoria miernymy i dostajemy

$$\lambda = s \cdot \frac{N}{r} \quad \text{dla pewnego } s = 0, \dots, r-1$$

Czy stałoby nam się wymiarować r ?

Jeśli $\text{GCD}(s, r) = 1$ to tak bo i.

$$\frac{\lambda}{N} = \frac{s}{r} \quad \text{wtedy sprawdzamy } \frac{\lambda}{N} \text{ to}$$

niezmienną wartość postaci $\frac{s}{r}$.

Jeśli nie to nie możemy. Ale to jest mało prawdopodobne, czyli możemy wymiarować r .

Fakt 2 twierdzenie: lub:

prawdop. że dwie duże przypadkowe liczby są względnie pierwsze:

$$\prod_{p=2}^{\infty} \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2} \approx 0,6$$

prawdop., że nie
dzieli się przez p

5. Co ma wymiarowanie charakteru funkcji?
de wartości ma wymiarowanie pierwsze?

N - liczba, której wymiarowanie pierwszych sum
Liczby $a < N$ i sprawdzamy

$GCD(a, N) \stackrel{!}{>} 1$ jeśli $GCD > 1$ to już mamy czynnik!

Jeśli $GCD(a, N) = 1$ (mamy resztę) to:

Wtedy z Tw Eulera \rightarrow istnieje r :

$$a^r = 1 \pmod{N} \quad (r = \text{mod } a)$$

Jeśli r jest parzyste:

$$a^r - 1 = 0 \pmod{N}$$

$$\underbrace{(a^{\frac{r}{2}} - 1)}_{\alpha} \underbrace{(a^{\frac{r}{2}} + 1)}_{\beta} = k \cdot N \quad \alpha \cdot \beta = k \cdot N$$

Czyli α lub β muszą mieć wspólny dzielnik z N
(choćby i α, β - wielokrotności N)

Fakt 2 teorii liczb: Dla $a < N$, t.j. $GCD(a, N) = 1$
wybierając losowo r mod r ($a^r = 1 \pmod{N}$)
jest parzysty i $a^{\frac{r}{2} \pm 1}$ nie są wielokrotnościami $N \geq \frac{r}{2}$

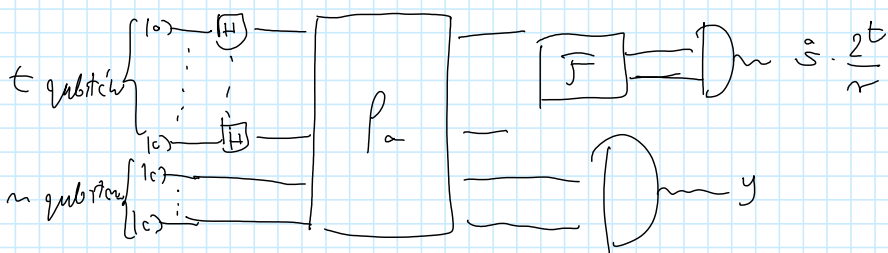
Liwny $GCD(\alpha, N)$, $GCD(\beta, N)$ dostajemy czynnik pierwszy N

Zauważmy, że mitm-dmijal jest wyznacznie r .

Metoda $f(x) = a^x \pmod{N}$

Czynnik jest mod $r \neq$ Określenie funkcji: f

$$f(x+r) = a^x \cdot a^r \pmod{N} = a^x \pmod{N}$$



$$N < 2^n$$

$$N < 2^t$$

$$f_a: |x\rangle |0\rangle = |x\rangle |a^x \pmod N\rangle \quad \left\{ \begin{array}{l} \text{wymaga } m^3 \\ \text{bramek} \end{array} \right.$$

\uparrow \uparrow
 linia t bitów linia m bitów

$$|0\rangle |a\rangle \xrightarrow{O(m^3)} \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle |a^x \pmod N\rangle$$

$\underbrace{0 \dots 0}_t$ $\underbrace{a \dots a}_m$

nie istnieje

$$\xrightarrow{\text{wymy } y_0} \sum_{x=0}^{2^t-1} |x\rangle |y_0\rangle = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} |x_0 + k \cdot r\rangle |y_0\rangle$$

$a^x \pmod N = y_0$

mrok bity t (i znowy jest) i
 2t mi jest wielokrotność
 r więc $K = \left\lfloor \frac{2^t}{r} \right\rfloor + 1$

$$F(O(m^2)) \xrightarrow{\sim} \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{\frac{2\pi i x_0 s}{r}} \left| \frac{2^t}{r} \right\rangle$$

otrymujemy

przybliżeń t bitowe ułamka $\frac{s}{r}$, jeśli t
 odpowiednio duże (chcąc się że $t \approx 2m$) to
 wystarczy użyć algorytmu N. (continued fraction algorithm)

Uwaga: Wzima jest ta implementacja funkcji f_a ,
 poprzez elem. bramki CNOTowe. No szczerze to
 ta jest $O(m^3)$

Czyli cały proces ma być $O(m^3)$