12 - Algorytm Shora

4 maja 2011 19:25

Kwantowa Transformata Fouriera i jej konsekwencje

1. Wstęp

Algorytm Shora (1993)

Rozkład liczby n bitowej na czynniki pierwsze w czasie n^3

Klasyczny problem trudny ale jednocześnie bardzo ważny (RSA).

Jeśli N liczba n bitowa $N < 2^n$

naiwna metoda:

- sprawdzamy czy dzieli się przez wszystkie liczby mniejsze od N (w zasadzie $\sqrt{N}$)

mamy $\sim 2^{\frac{n}{2}}$ operacji

Czyli obliczeń rośnie wykładniczo.

- Najlepsze algorytmy klasyczne mają skalowanie:

$\sim 2^{\sqrt[3]{n}}$ szybciej niż dowolny wielomian

Algorytm dość skomplikowany, ale podstawowy element to kwantowa transformata Fouriera

2. Transformata Fouriera klasycznie

• Klasyczna dyskretna trans Fouriera

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

$\downarrow F$ $\qquad y_k = \frac{1}{\sqrt{N}} \sum_j e^{\frac{2\pi i jk}{N}} x_j$

$y_0 \ldots y_{N-1}$

Liczba operacji N^2, inaczej 2^{2n}

(jeśli N liczba n bitowa)

FFT może trochę przyspieszyć $N \log N \approx 2^n n$

wciąż wykładniczo z liczbą bitów numerujących dane

3. Kwantowa trans Fouriera

definiujemy op unitarną U_F na stanach n qubitowych

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

Można sprawdzić że jest unitarna.

Jeśli zapiszemy nasze dane jako przykład:

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

$$= \sum_k y_k |k\rangle$$

gdzie $y_k = \frac{1}{\sqrt{N}} x_j e^{\frac{2\pi i jk}{N}}$ to liczby

mamy na razie całą trans Fouriera.

Uwagi:

— nie oznacza to że można odczytać wszystkie y_k na raz, czyli ten kw. paralelizm trzeba forsować sprytnie użyć dalej (okazuje się to możliwe właśnie w alg. Shora

— U_F trzeba zbudować z Cl bramek kwantowych i pytanie jak to się skaluje z n. Okazuje się, że b. dobrze bo $\sim n^2$

Czyli mamy zysk w porównaniu z klasycznym FFT jak

$$n^2 \text{ do } n2^n \; !$$

Wykładniczy zysk.

4. Co ma trans. Fouriera do rozkładu na czynniki pierwsze?

Transf. Fouriera pozwala znajdować okres funkcji!

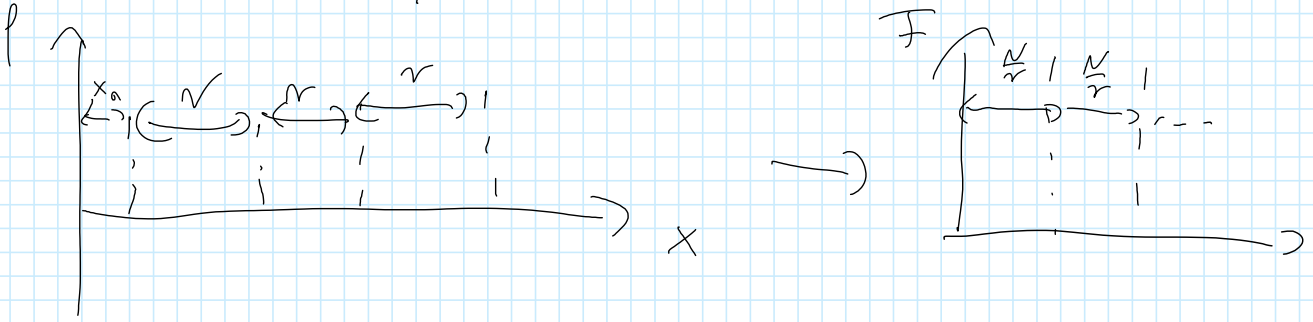
Rozważmy funkcję $f: Z_N \to Z$

(Z_N — całkowite mod N)

Szukamy jej okresu $f(x+r) = f(x)$ {niezmieniona / ma okresie}

Liczymy dla wszystkich argumentów

$$|\rho\rangle = \frac{1}{\sqrt{N}} \cdot \sum_{x=0}^{N-1} |x\rangle |\rho(x)\rangle$$



Mierzymy drugi rejestr jest wyjście y t_0

$$\rightarrow \quad N = k \cdot r \quad , \quad \underbrace{\frac{1}{\sqrt{k}} \sum_{k=0}^{k-1} |x_0 + k \cdot r\rangle}_{|\psi_{x_0,r}\rangle} |y\rangle, \quad \rho(x_0) = y_0$$

Mając stan $|\psi_{x_0,r}\rangle$ chcemy stwierdzić jakie jest r? Mamienie x nic nie da dostaniemy $x_0 + kr$ i nic nie wiemy, ale

możemy zrobić transformatę

$$\mathcal{F}|\psi_{x_0,r}\rangle = \frac{1}{\sqrt{N}} \frac{1}{\sqrt{k}} \sum_{k=0}^{k-1} \sum_{c=0}^{N} e^{\frac{2\pi i \cdot l (x_0 + kr)}{N}} |l\rangle =$$

$$= \frac{1}{\sqrt{N}} \sum_{c=0}^{N} e^{\frac{2\pi i l x_0}{N}} |l\rangle \cdot \underbrace{\frac{1}{\sqrt{k}} \sum_{k=0}^{k-1} e^{\frac{2\pi i l \cdot r \cdot k}{N}}}_{\sqrt{k} \text{ jeśli } l \cdot r = s \cdot N} =$$

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

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

Teraz mierzymy i dostajemy

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

Czy stąd możemy wywnioskować r?

Jeśli $GCD(s, r) = 1$ to tak bo wtedy

$\frac{\lambda}{N} = \frac{s}{r}$ więc sprowadzając $\frac{\lambda}{N}$ do

nieredukowalnej postaci mamy r.

Jeśli nie to niestety nie. ALE to jest

mało prawdopodobne, czyli możemy wyznaczyć r

Fakt z teorii liczb:

prawdop. że dwie duże przypadkowe liczby

są względnie pierwsze:

$$\prod_{p=2}^{\infty} \underbrace{\left(1 - \frac{1}{p^2}\right)} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2} \approx 0{,}7$$

prawdop., że nie dzielą się przez p

5. Co ma wyznaczenie okresu funkcji do rozkładu na czynniki pierwsze?

N - liczba, której czynników pierwszych szukamy

Losujemy liczbę $a < N$ i sprawdzamy

GCD(a, N) ⇑ Jeśli GCD > 1 to już mamy czynnik!

Jeśli GCD(a, N) = 1 (znacznie częściej) to:

Wtedy z Tw Eulera ⇑ istnieje r:

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

Jeśli r jest parzyste:

$$a^r - 1 = 0 \mod N$$

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

czyli α lub β muszą mieć wspólne dzielniki z N

(chyba że α, β - wielokrotności N)

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

Licząc $GCD(\alpha, N)$, $GCD(\beta, N)$ dostajemy czynniki pierwsze N

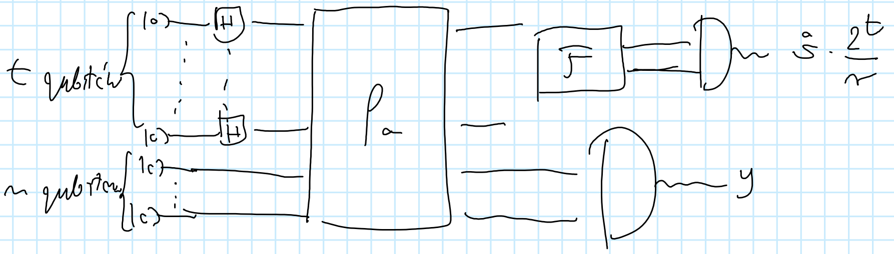
Zauważmy, że najtrudniejsze jest wyznaczenie r.

Niech

$$f(x) = a^x \mod N$$

Czym jest rząd r? Okresem funkcji f!

$$f(x + r) = a^x \cdot a^r \mod N = a^x \mod N$$



$N < 2^n$

$N < 2^n$

$$f_a: |x\rangle|0\rangle = |x\rangle|a^x \bmod N\rangle$$ } wymaga n^3 bramek

($|x\rangle$ – liczba t bitów, $|0\rangle$ – liczba n bitów)

$$|0\rangle|0\rangle \xrightarrow{H,\ f\ O(n^3)} \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|a^x \bmod N\rangle \longrightarrow$$

($|0\rangle = \underbrace{0\ldots0}_{t}$, $|0\rangle = \underbrace{0\ldots0}_{n}$)

$$\xrightarrow{\text{mierzymy } y_0} \propto \sum_{\substack{x=0 \\ a^x \bmod N = y_0}}^{2^t-1} |x\rangle \underbrace{|y_0\rangle}_{\text{nie istotne}} = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} |x_0 + k\cdot r\rangle |y_0\rangle$$

może być tak (i zwykle jest) że 2^t nie jest wielokrotnością r więc $K = \left\lfloor \frac{2^t}{r} \right\rfloor$ v $\left\lfloor \frac{2^t}{r} \right\rfloor + 1$

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

przybliżenie t bitowe ułamka $\frac{s}{r}$, jeśli t odpowiednio duże (okazuje się że $t \approx 2n$) to wystarczy żeby uzyskać r. (continued fraction algorithm)

Uwaga: Ważna jest też implementacja funkcji f_a, poprzez elem. bramki kwantowe. Na szczęście to też jest $O(n^3)$

Czyli cała procedura jest $O(n^3)$