FFT

poniedziałek, 17 czerwca 2024 09:48

Problem: mnożenie wielomianów

Dane: $a_0 \dots\dots a_{n-1}$ – współczynniki wielomianu $A(x)$

$b_0 \dots\dots b_{n-1}$ – współczynniki wielomianu $B(x)$

Założenie: $n = 2^k$

Wynik: $c_0, c_1, \dots, c_{2n-2}$ t. że $c_j = \sum_{i=0}^{j} a_i b_{j-i}$

$c_0 = a_0 b_0$

$c_1 = a_0 b_1 + a_1 b_0$

$\vdots$

aido

$c_{2n-2} = a_0 b_{2n-2} + a_1 b_{2n-3} + \dots +$

bo mnożąc dwa wielomiany x^2 i x^2 dostaniemy wielomian x^4 cyli potrzebujemy już 5 punktów by go określić jednoznacznie

jaki wielomiany mają mały stopień, to jeden wypełniamy zerami współczynniki

Podejście I

Naiwnie (klasycznie) – $O(n^2)$

Reprezentuje wielomiany:

jednoznacznie

- współczynnikowa (w)
- zbiór wartości w ustalonych punktach (z)

Operacje:	(w)	(z)
dodawanie	$O(n)$	$O(n)$
obliczenie wartości w punkcie	$O(n)$	przykre
mnożenie	$O(n^2)$	$O(n)$ o ile mamy wystarczającą reprezentację punktową

bo potrzebujemy więcej punktów bo stopień wzrośnie

Pomysł:

A, B w reprezentacji (w) $\qquad$ C w reprezentacji (w)

(1) $O(n^2)$? można zejść do $n\log n$ $\qquad$ (2) $O(n^2)$? Lagrange numeryki

bo obl. wart. w punkcie to $O(n)$ i robimy to dla n punktów razy 2

A, B w reprezentacji (z) $\xrightarrow[O(n)]{}$ $C = A \cdot B$ w reprezentacji (z)

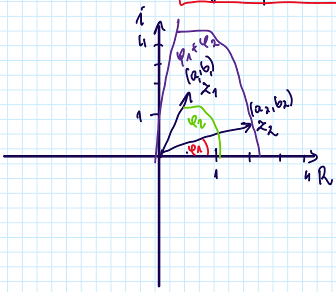
nie prowadzi do lepszego efektu niż mnożenie

→ $n\log n$ tylko trzeba dobrać dobre punkty, w których liczymy wartości wielomianu

Przejścia (1) i (2) dają się szybko wykonać, gdy liczymy wartości wielomianów w pewnych pierwiastkach z jedności

→ Co to?

takie liczby, które podniesione do potęgi n dają 1: $\omega^n = 1$



$a i + b$

Jak mnożymy dwie liczby zespolone, to liczymy ich długości wektor będący sumą ich długości, a kąt jest ich sumą kątów

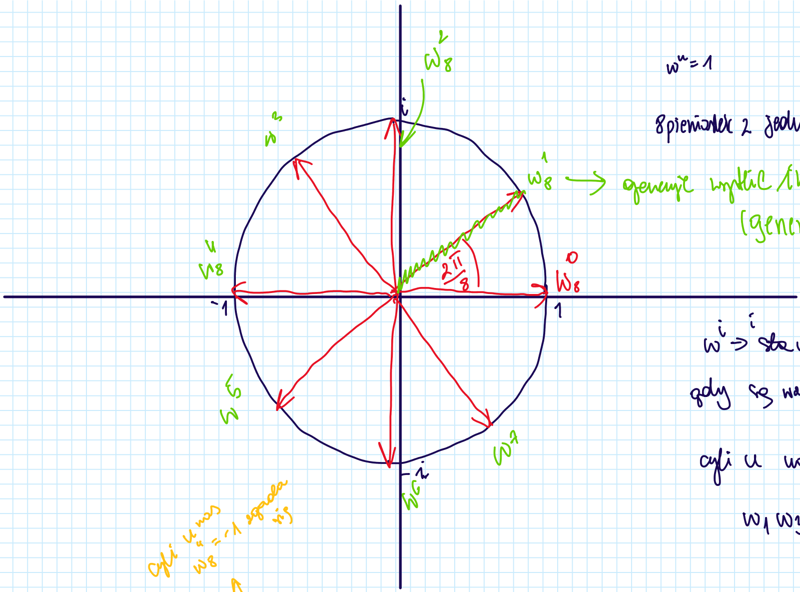
jeśli $\omega \in \mathbb{N}$ to jest tylko jedno takie $\omega = 1$

$\omega \in \mathbb{Z}$ to $\omega = -1 \vee \omega = 1$

gdy przejdziemy do liczb zespolonych, to tych pierwiastków robi się więcej

czyli będziemy potrzebować tyle pierwiastków, ile wynika ze stopni wielomianów

$\wedge i$



$w^n=1$

8 pierwiastek z jedności

w_8^1 → generuje wszystkie inne (generator)

w^i → stanowią zbiór generatorów gdy są względnie pierwsze z liczbą

czyli u nas to by było $w_1\, w_3\, w_5\, w_7$ z 8

Oznaczenie na pierwiastek z jedności: $w_n = e^{\frac{2\pi i k}{n}}$ dla $k=0,1,\dots,n-1$

$e^{\pi i}=-1$, więc $e^{2\pi i}=1$

czyli u nas $w_8^4=-1$ zgadza się

Lemat:

a) $w_n^{\frac{n}{2}} = -1$ dla każdego n parzystego

b) $\forall$ parzystego $n>0$ $\left\{ (w_n^j)^2 \mid j=0,\dots,n-1 \right\} = \left\{ w_{\frac{n}{2}}^l \mid l=0,\dots,\frac{n}{2}-1 \right\}$

$\{w_8^1, w_8^2, w_8^3, w_8^4, w_8^5, w_8^6, w_8^7, w_8^8\}$

do kwadratu

$\{w_8^2, w_8^4, w_8^6, w_8^8, w_8^{10}, w_8^{12}, w_8^{14}, w_8^{16}\}$

$w_8^8 = 1$, $w_8^{16} = 1$, $w_8^{10} = w_8^8 \cdot w_8^2$

$$w_{dn}^{dk} = w_n^k$$

c) $\forall_{\substack{n\geq 1\\ k\geq 0\\ n\nmid k}} \sum_{j=0}^{k-1} (w_n^k)^j = 0$

1)

W → Z

$x = w_n, w_n^2, \dots, w_n^n$

$A(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$

Definiujemy sobie dwa wielomiany

są stopnia $\frac{n}{2}$

$A^{(0)}(x) = a_0 + a_2x + a_4x^2 + \dots + a_{n-2}x^{\frac{n}{2}-1}$

$A^{(1)}(x) = a_1 + a_3x + a_5x^2 + \dots + a_{n-1}x^{\frac{n}{2}-1}$

Zatem $A(x)$ jest równy:

$$A(x) = A^{(0)}(x^2) + x\cdot A^{(1)}(x^2)$$

n — $\frac{n}{2}$ — $\frac{n}{2}$ z w $\frac{n}{2}$ pkt.

w $\frac{n}{2}$ pkt

czyli mamy pełną redukcję

redukujemy również liczbę punktów, ponieważ wiemy, że w kwadracie punktów jest tylko $\frac{n}{2}$ pierwiastków z jedności

to koszt całego

Algorytm 1)

FFT($\vec{a}$)
Niech n - długość $\vec{a}$
if ($n=1$) then return $\vec{a}$
$w_n \leftarrow e^{\frac{2\pi i}{n}}$
$w \leftarrow 1$
$a^0 \leftarrow \langle a_0, a_2, \dots, a_{n-2}\rangle$
$a^1 \leftarrow \langle a_1, a_3, \dots, a_{n-1}\rangle$
$y^{(0)} \leftarrow FFT(\vec{a}^{(0)})$
$y^{(1)} \leftarrow FFT(\vec{a}^{(1)})$
for $k=0$ to $\frac{n}{2}-1$ do
  $y_k \leftarrow \vec{y}_k^{(0)} + w\cdot \vec{y}_k^{(1)}$
  $y_{k+\frac{n}{2}} \leftarrow \vec{y}_k^{(0)} - w\cdot \vec{y}_k^{(1)}$
  $w \leftarrow w\cdot w_n$
return $\vec{y}$

realn... powo... punktów

Czyli $T(n)=2T\left(\frac{n}{2}\right)+\Theta(n)$ bo koszt całego

Zatem rozwiązaniem równania będzie $T(n)=O(n\log n)$

2) teraz mamy zbiór wartości w punktach i chcemy przejść do zapisu współczynnikowego

$$\underbrace{\begin{bmatrix} (w_n^0)^0 & (w_n^0)^1 & \cdots & (w_n^0)^{n-1} \\ (w_n^1)^0 & (w_n^1)^1 & \cdots & (w_n^1)^{n-1} \\ \vdots & \vdots & & \vdots \\ (w_n^{n-1})^0 & (w_n^{n-1})^1 & \cdots & (w_n^{n-1})^{n-1} \end{bmatrix}}_{V_n} \cdot \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix} \begin{matrix} = A(w_n^0) \\ = A(w_n^1) \\ \vdots \\ = A(w_n^{n-1}) \end{matrix}$$

wartości wielomianu w pierwiastku w_n^0

Musimy policzyć tę wartość w konkretnym punkcie

$a_0\cdot w_n^0 + a_1\cdot(w_n^0)^1 + a_2\,(w_n^0)^2+\ldots+a_{n-1}\cdot(w_n^0)^{n-1}$

$A(x)=a_0\cdot x^0+a_1\cdot x^1+a_2\cdot x^2$

tu we pozycji (j,k) jest wartość w_n^{jk}

współczynniki niewiadomy → oryginalny wartości pierwiastka z jedności

Czyli $V_n\cdot\vec{a}=\vec{y}$

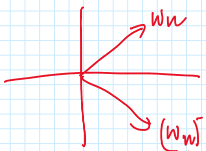
$V_n^{-1}\cdot\vec{y}=\vec{a}$

macierz odwrotna istnieje, bo V_n jest nieosobliwa, bo to macierz Vandermonda

W macierzy V_n^{-1} na pozycji (j,k) jest wartość $\frac{w_n^{-j\cdot k}}{n}$

$\frac{1}{n}\cdot[\quad]\cdot\vec{y}$

$w_n^{-jk}=(w_n^{-1})^{jk}$



jest też pierwiastkiem generatorem

Czyli możemy przeprowadzić taką samą transformację jak poprzednio

więc obliczenie tego iloczynu możemy wykonać poprzez FFT

Zamiast liczb zespolonych można użyć innych ciał.