

SZYBKA TRANSFORMACJA FOURIERA (FFT)

46 Reprezentacje wielomianów

Dwie reprezentacje wielomianu A stopnia $n - 1$:

[Wsp] jako n -elementowy wektor współczynników $\langle a_0, a_1, \dots, a_{n-1} \rangle$.

[War] jako zbiór wartości w n różnych punktach $\{(x_i, y_i) : i = 0, \dots, n - 1 \text{ i } \forall_{0 \leq i \neq j \leq n-1} x_i \neq x_j \text{ i } y_i = A(x_i)\}$.

47 Podstawowe operacje na wielomianach

- dodawanie - wykonalne w czasie $O(n)$ przy obydwu reprezentacjach wielomianów,
- mnożenie - łatwe przy reprezentacji [War] (w czasie $O(n)$); trudne przy reprezentacji [Wsp] (prosta implementacja wymaga czasu $\Omega(n^2)$).
- obliczanie wartości w punkcie - łatwe przy reprezentacji [Wsp] (np. schemat Hornera - w czasie $O(n)$); trudne przy reprezentacji [War]

48 Zmiana reprezentacji wielomianu stopnia $n - 1$

[Wsp] \rightarrow [War]

Reprezentacja [War] może być wybrana na wiele różnych sposobów. Korzystając ze schematu Hornera można ją obliczyć w czasie $\Theta(n^2)$.

[War] \rightarrow [Wsp]

Twierdzenie 16 Dla każdego zbioru $\{\langle x_i, y_i \rangle \mid i = 0, \dots, n-1 \text{ oraz } \forall_{0 \leq i \neq j \leq n-1} x_i \neq x_j\}$ istnieje jednoznacznie wyznaczony wielomian A stopnia $n-1$ taki, że $\forall_{0 \leq i \leq n-1} y_i = A(x_i)$.

Współczynniki tego wielomianu można obliczyć w czasie $\Theta(n^2)$ ze wzoru Lagrange'a:

$$A(x) = \sum_{k=0}^{n-1} y_k \frac{\prod_{j \neq k} (x - x_j)}{\prod_{j \neq k} (x_k - x_j)}.$$

Jak póniej pokażemy przejścia [Wsp] \rightarrow [War] i [War] \rightarrow [Wsp], można obliczyć w czasie $O(n \log n)$.

49 Pomysł na szybkie mnożenie wielomianów w postaci [Wsp]

Niech $A(x)$ i $B(x)$ będą wielomianami stopnia $\leq n - 1$.

1. Utworzyć reprezentacje [Wsp] wielomianów A i B jako wielomianów stopnia $2n - 1$ (przez dodanie n współczynników równych 0).
2. Stosując FFT obliczyć dla tych wielomianów reprezentacje [War] o długości $2n$.
3. Obliczyć reprezentację [War] wielomianu $C(x) = A(x) \cdot B(x)$.
4. Stosując FFT obliczyć reprezentację [Wsp] wielomianu $C(x)$.

Kroki 1 i 3 można wykonać w czasie $O(n)$, a kroki 2 i 4 w czasie $O(n \log n)$.

50 Pierwiastki z jedności w ciele liczb zespolonych

Definicja 20 n -tym pierwiastkiem z jedności nazywamy liczbę ω taką, że $\omega^n = 1$.

Fakt 24 W ciele liczb zespolonych istnieje dokładnie n n -tych pierwiastków z jedności. Są nimi liczby $e^{2\pi i k/n}$ dla $i = 0, \dots, n - 1$.

Definicja 21 n -ty pierwiastek z jedności, którego potęgi generują zbiór wszystkich n -tych pierwiastków nazywamy n -tym pierwotnym pierwiastkiem z jedności.

Fakt 25 Liczba $\omega_n = e^{2\pi i/n}$ jest n -tym pierwotnym pierwiastkiem z jedności.

Fakt 26 Zbiór $\{\omega_n^j \mid j = 0, \dots, n - 1\}$ z mnożeniem tworzy grupę izomorficzną z grupą $(\mathbb{Z}_n, +_{\text{mod } n})$.

Lemat 6 (a) $\forall_{n \geq 0, k \geq 0, d > 0} \omega_{dn}^{dk} = \omega_n^k$.

(b) $\forall_{\text{parzystego } n > 0} \omega_n^{n/2} = \omega_2 = -1$.

(c) $\forall_{\text{parzystego } n > 0} \{(\omega_n^j)^2 \mid j = 0, \dots, n - 1\} = \{\omega_{n/2}^l \mid l = 0, \dots, \frac{n}{2} - 1\}$.

(d) $\forall_{n \geq 1, k \geq 0 \text{ takiego, że } n \nmid k} \sum_{j=0}^{n-1} (\omega_n^k)^j = 0$.

51 Dyskretna Transformacja Fouriera (DFT).

Definicja 22 Niech $\mathbf{a} = a_0, \dots, a_{n-1}$. Wektor $\mathbf{y} = y_0, \dots, y_{n-1}$ taki, że $y_k = \sum_{j=0}^{n-1} a_j \omega_n^{kj}$ (dla $k = 0, \dots, n - 1$) nazywamy Dyskretną Transformacją Fouriera wektora \mathbf{a} .

Jeśli \mathbf{a} jest wektorem współczynników wielomianu $A(x)$, to \mathbf{y} jest wektorem wartości tego wielomianu w punktach $\omega_n^0, \omega_n^1, \dots, \omega_n^{n-1}$.

52 FFT - szybki algorytm obliczania DFT

- Idea algorytmu.

Niech

$A^{[0]}(z) = a_0 + a_2z + a_4z^2 \dots + a_{n-2}z^{n/2-1}$ i $A^{[1]}(z) = a_1 + a_3z + a_5z^2 \dots + a_{n-1}z^{n/2-1}$.
Wówczas $A(x) = A^{[0]}(x^2) + xA^{[1]}(x^2)$.

Tak więc problem obliczenia wartości wielomianu A stopnia $n - 1$ w n punktach: $\omega_n^0, \omega_n^1, \dots, \omega_n^{n-1}$, redukuje się do problemu obliczenia wartości dwóch wielomianów $A^{[0]}$ i $A^{[1]}$ stopnia $\frac{n}{2} - 1$ w $\frac{n}{2}$ punktach: $\omega_{n/2}^0, \omega_{n/2}^1, \dots, \omega_{n/2}^{(n/2)-1}$.

```

procedure Recursive - FFT(a)
   $n \leftarrow \text{length}(\mathbf{a})$ 
  if  $n = 1$  then return (a)
   $\omega_n \leftarrow e^{2\pi i/n}$ 
   $\omega \leftarrow 1$ 
   $\mathbf{a}^{[0]} \leftarrow \langle a_0, a_2, \dots, a_{n-2} \rangle$ 
   $\mathbf{a}^{[1]} \leftarrow \langle a_1, a_3, \dots, a_{n-1} \rangle$ 
   $\mathbf{y}^{[0]} \leftarrow \text{Recursive - FFT}(\mathbf{a}^{[0]})$ 
   $\mathbf{y}^{[1]} \leftarrow \text{Recursive - FFT}(\mathbf{a}^{[1]})$ 
  for  $k \leftarrow 0$  to  $n/2 - 1$  do
     $y_k \leftarrow y_k^{[0]} + \omega y_k^{[1]}$ 
     $y_{k+(n/2)} \leftarrow y_k^{[0]} - \omega y_k^{[1]}$ 
     $\omega \leftarrow \omega \omega_n$ 
  return  $\mathbf{y}$ 

```

- Złożoność algorytmu: $T(n) = 2T(\frac{n}{2}) + \Theta(n) = \Theta(n \log n)$.

Definicja 23 Splotem wektorów $\mathbf{a} = \langle a_0, \dots, a_{n-1} \rangle$ i $\mathbf{b} = \langle b_0, \dots, b_{n-1} \rangle$ nazywamy wektor $\mathbf{c} = \langle c_0, \dots, c_{2n-1} \rangle$ taki, że $\forall_{0 \leq i \leq 2n-1} c_i = \sum_{j=0}^i a_j b_{i-j}$ i oznaczamy go $\mathbf{c} = \mathbf{a} \otimes \mathbf{b}$.

Tak więc splot $\mathbf{a} \otimes \mathbf{b}$ jest reprezentacją [Wsp] iloczynu wielomianów o reprezentacjach [Wsp] \mathbf{a} i \mathbf{b} .

53 Interpolacja w n -tych pierwiastkach z jedności

Jeśli $\mathbf{y} = DFT(\mathbf{a})$, to $\mathbf{y} = V_n \cdot \mathbf{a}$, gdzie V_n jest macierzą $n \times n$, której wyraz (j, k) -ty równa się ω_n^{jk} .

Fakt 27 Dla $j, k = 0, \dots, n-1$ wyraz (j, k) -ty macierzy V_n^{-1} równa się ω_n^{-jk}/n .

Powyższy fakt pozwala na obliczenie \mathbf{a} z danego \mathbf{y} przez zastosowanie FFT (należy ω_n zastąpić przez ω_n^{-1})

```

procedure Iterative – FFT(a)
  Bit – Reverse – Copy(a, A)
  n ← length(a)                                { n jest potęgą 2-ki }
  for s ← 1 to log n do
    m ← 2s
     $\omega_m \leftarrow e^{2\pi i/m}$ 
     $\omega \leftarrow 1$ 
    for j ← 0 to m/2 – 1 do
      for k ← j to n – 1 step m do
        t ←  $\omega A[k + m/2]$ 
        u ← A[k]
        A[k] ← u + t
        A[k + m/2] ← u – t
       $\omega \leftarrow \omega \omega_m$ 
  return A

procedure Bit – Reverse – Copy(a, A)
  n ← length(a)
  for k ← 0 to n – 1 do A[rev(k)] ← ak

```

$rev(k)$ oznacza tutaj n -bitową liczbę powstałą przez zapisanie n -bitowego rozwinięcia binarnego liczby k od prawej do lewej strony.

Definicja 24 (a) Splotem wektorów $\mathbf{a} = \langle a_0, \dots, a_{n-1} \rangle$ i $\mathbf{b} = \langle b_0, \dots, b_{n-1} \rangle$ nazywamy wektor $\mathbf{c} = \langle c_0, \dots, c_{2n-1} \rangle$ taki, że $\forall_{0 \leq i \leq 2n-1} c_i = \sum_{j=0}^i a_j b_{i-j}$ i oznaczamy go $\mathbf{c} = \mathbf{a} \otimes \mathbf{b}$.

(b) Negatywnym splotem zwiniętym wektorów \mathbf{a} i \mathbf{b} nazywamy wektor $\mathbf{d} = \langle d_0, \dots, d_{n-1} \rangle$, taki że $d_i = \sum_{j=0}^i a_j b_{i-j} - \sum_{j=i+1}^{n-1} a_j b_{n+i-j}$.

Tak więc splot $\mathbf{a} \otimes \mathbf{b}$ jest reprezentacją [Wsp] iloczynu wielomianów o reprezentacjach [Wsp] \mathbf{a} i \mathbf{b} i, jak pokazaliśmy, może być obliczony przy użyciu transformacji Fouriera.

Fakt 28 Niech \mathbf{a} , \mathbf{b} i \mathbf{d} jak w powyższej definicji. Niech ψ będzie pierwiastkiem z jednościi stopnia $2n$. Oznaczmy przez $\hat{\mathbf{a}}$, $\hat{\mathbf{b}}$ i $\hat{\mathbf{d}}$ wektory $\langle a_0, \psi a_1, \dots, \psi^{n-1} a_{n-1} \rangle$, $\langle b_0, \psi b_1, \dots, \psi^{n-1} b_{n-1} \rangle$ i $\langle d_0, \psi d_1, \dots, \psi^{n-1} d_{n-1} \rangle$. Wówczas $DFT(\hat{\mathbf{d}}) = DFT(\hat{\mathbf{a}}) \cdot DFT(\hat{\mathbf{b}})$.

Aby uniknąć kłopotów związanych z niedokładną reprezentacją zespolonych pierwiastków z jednościi, można transformację Fouriera wykonywać nad jakimś ciałem skończonym lub pierścieniem R_m liczb całkowitych modulo m posiadającym n -ty pierwotny pierwiastek z jednościi.

Fakt 29 Niech n i ω będą potęgami liczby 2 (różnymi od 1) oraz niech $m = \omega^{n/2} + 1$. Wówczas n i ω są odwracalne w R_m oraz ω jest n -tym pierwotnym pierwiastkiem z jednościi.