Notatka z AiSD 28 czerwca 2022

Szybka transformacja Fouriera (FFT)

IIUWr. II rok informatyki.

1 Reprezentacje wielomianów

Dwie reprezentacje wielomianu A stopnia $n-1$:

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

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

2 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]`

3 Zmiana reprezentacji wielomianu stopnia $n-1$

`[Wsp]` $\rightarrow$`[War]`

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

`[War]` $\rightarrow$`[Wsp]`

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

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

4 Pomysł na szybkie mnożenie wielomianów w postaci `[Wsp]`

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

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 $O(n \log n)$.

5 Pierwiastki z jedności w ciele liczb zespolonych

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

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

Definicja 2 *n-ty pierwiastek z jedności, którego potęgi generują zbiór wszystkich n-tych pierwiastków nazywamy* n-tym pierwotnym pierwiastkiem z jedności.

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

Fakt 3 *Zbiór* $\{\omega_n^j \mid j = 0, \ldots, n-1\}$ *z mnożeniem tworzy grupę izomorficzną z grupą* $(\mathcal{Z}_n, +_{mod\ n})$.

Lemat 1 *(a)* $\forall_{n\geq 0, k\geq 0, d>0}\ \omega_{dn}^{dk} = \omega_n^k$.

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

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

(d) $\forall_{n\geq 1, k\geq 0 takiego, że\ n \not| k}\ \sum_{j=0}^{n-1} (\omega_n^k)^j = 0$.

6 Dyskretna Transformacja Fouriera (DFT).

Definicja 3 *Niech* $\mathbf{a} = a_0, \ldots, a_{n-1}$. *Wektor* $\mathbf{y} = y_0, \ldots, y_{n-1}$ *taki, że* $y_k = \sum_{j=0}^{n-1} a_j \omega_n^{kj}$ *(dla* $k = 0, \ldots, n-1$*) 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 $\omega_n^0, \omega_n^1, \ldots, \omega_n^{n-1}$.

7 FFT - szybki algorytm obliczania DFT

Idea algorytmu Niech

$$A^{[0]}(z) = a_0 + a_2 z + a_4 z^2 \ldots + a_{n-2} z^{n/2-1} \text{ i}$$
$$A^{[1]}(z) = a_1 + a_3 z + a_5 z^2 \ldots + a_{n-1} z^{n/2-1}.$$

Wówczas $A(x) = A^{[0]}(x^2) + xA^{[0]}(x^2)$.

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

Pseudokod

```
procedure Recursive-FFT(a)
    n ← length(a)
    if n = 1 then return (a)
    ω_n ← e^{2πi/n}
    ω ← 1
    a^[0] ← ⟨a_0, a_2, ..., a_{n-2}⟩
    a^[1] ← ⟨a_1, a_3, ..., a_{n-1}⟩
    y^[0] ← Recursive-FFT(a^[0])
    y^[1] ← Recursive-FFT(a^[1])
    for k ← 0 to n/2 − 1 do
        y_k ← y_k^[0] + ω y_k^[1]
        y_{k+(n/2)} ← y_k^[0] − ω y_k^[1]
        ω ← ω ω_n
    return y
```

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

Definicja 4 Splotem *wektorów* $\mathbf{a} = \langle a_0, \ldots, a_{n-1} \rangle$ *i* $\mathbf{b} = \langle b_0, \ldots, b_{n-1} \rangle$ *nazywamy wektor* $\mathbf{c} = \langle c_0, \ldots, c_{2n-1} \rangle$ *taki, że* $\forall_{0 \le i \le 2n-1}\ c_i = \sum_{j=0}^{i}\ a_j b_{i-j}$ *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]` **a** i **b**.

8 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 4 *Dla* $j, k = 0, \ldots, n-1$ *wyraz* (j,k)*-ty macierzy* V_n^{-1} *równa się* ω_n^{-jk}/n.

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

Dalej nie czytać.

9 Efektywna implementacja FFT

```
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 ← 2^s
            ω_m ← e^{2πi/m}
            ω ← 1
            for j ← 0 to m/2 − 1 do
                    for k ← j to n − 1 step m do
                            t ← ωA[k + m/2]
                            u ← A[k]
                            A[k] ← u + t
                            A[k + m/2] ← u − t
                    ω ← ωω_m
    return A

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

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

Definicja 5 *(a)* Splotem *wektorów* $\mathbf{a} = \langle a_0, \ldots, a_{n-1} \rangle$ *i* $\mathbf{b} = \langle b_0, \ldots, b_{n-1} \rangle$ *nazywamy wektor* $\mathbf{c} = \langle c_0, \ldots, c_{2n-1} \rangle$ *taki, że* $\forall_{0 \le i \le 2n-1}\ c_i = \sum_{j=0}^{i}\ a_j b_{i-j}$ *i oznaczamy go* $\mathbf{c} = \mathbf{a} \otimes \mathbf{b}$.

(b) Negatywnym splotem zwiniętym *wektorów* **a** *i* **b** *nazywamy wektor* $\mathbf{d} = \langle d_0, \ldots, d_{n-1} \rangle$, *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]` **a** i **b** i, jak pokazaliśmy, może być obliczony przy użyciu transformacji Fouriera.

Fakt 5 *Niech* **a**, **b** *i* **d** *jak w powyższej definicji. Niech* ψ *będzie pierwiastkiem z jedności stopnia* $2n$. *Oznaczmy przez* $\hat{\mathbf{a}}$, $\hat{\mathbf{b}}$ *i* $\hat{\mathbf{d}}$ *wektory* $\langle a_0, \psi a_1, \ldots, \psi^{n-1} a_{n-1} \rangle$, $\langle b_0, \psi b_1, \ldots, \psi^{n-1} b_{n-1} \rangle$ *i* $\langle d_0, \psi d_1, \ldots, \psi^{n-1} d_{n-1} \rangle$. *Wówczas* $DFT(\hat{\mathbf{d}}) = DFT(\hat{\mathbf{a}}) \cdot DFT(\hat{\mathbf{b}})$.

Aby uniknąć kłopotów związanych z niedokładną reprezentacją zespolonych pierwiastków z jedności, można transformację Fouriera wykonywać nad jakimś ciałem skończonym lub pierścieniem R_m liczb całkowitych modulo m posiadającym n-ty pierwotny pierwiastek z jedności, który spełnia Lemat 1 (w istocie chodzi nam o to, by spełniał własność (d) tego lematu, ponieważ pozostałe są w oczywisty sposób spełnione przez każdy, nie tylko zespolony, n-ty pierwotny pierwiastek z jedności).

Fakt 6 *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 jedności spełniającym Lemat 1.*

Pewnym mankamentem jest to, że liczba m - modulo, którą wykonywane byłyby obliczenia jest duża (ma $\Omega(n)$ cyfr).

Fakt 7 *Niech n będzie potęgą liczby 2, a k niech będzie najmniejszą liczbą taką, że $p = kn+1$ jest liczbą pierwszą. Wówczas FFT możemy obliczać modulo p przyjmując za pierwotny pierwiastek z jedności liczbę $w = g^k \mod p$, gdzie g jest generatorem $\mathcal{Z}_*$.*