Sedme vaje APS2: Diskretna Fourierova transformacija

1 Koeficientna in vrednostna predstavitev

Koeficientna predstavitev polinoma $a(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}$ je vektor $[a_0, a_1, \ldots, a_{n-1}]^T$. Vrednostna predstavitev je vektor $[a(x_0), a(x_1), \ldots, a(x_{n-1})]$ v n izbranih medsebojno različnih točkah. Predstavitvi sta enakovredni: za pretvorbo iz koeficientne v vrednostno predstavitev potrebujemo n izvedb Hornerjevega algoritma ($O(n^2)$), za obratno predstavitev pa rešimo sistem n linearnih enačb z n neznankami ($O(n^3)$).

2 Množenje polinomov

V koeficientni predstavitvi lahko polinome množimo v času $O(n^2)$, v vrednostni pa v času $O(n)$: vektorja, ki pripadata isti množici točk $\{x_0, \ldots, x_{n-1}\}$, enostavno zmnožimo po komponentah. Izkaže se (to bomo videli na naslednjih vajah), da lahko pri točno določeni množici točk $\{x_0, \ldots, x_{n-1}\}$ iz koeficientne v vrednostno predstavitev in obratno prehajamo v času $O(n \log n)$, kar pomeni, da skupni čas množenja postane $O(n \log n)$.

Oglejmo si primer. Zmnožimo polinoma $a(x) = 3 + x + 2x^2$ in $b(x) = 1 + 4x$ s prehodom na vrednostno predstavitev. Ker bo zmnožek imel štiri koeficiente, potrebujemo štiri medsebojno različne točke. Vzemimo točke $\{-1, 0, 1, 2\}$. Dobimo $y_a = [4, 3, 6, 13]$ in $y_b = [-3, 1, 5, 9]$. Vektorja zmnožimo po komponentah: $y_c = [-12, 3, 30, 117]$. Koeficiente polinoma $c(x) = a(x)b(x)$ dobimo tako, da rešimo sistem štirih enačb s štirimi neznankami (v nastavek $c(x) = c_0 + c_1x + c_2x^2 + c_3x^3$ zaporedoma vstavimo točke -1, 0, 1 in 2):

$$\begin{aligned} c_0 - c_1 + c_2 - c_3 &= -12 \\ c_0 &= 3 \\ c_0 + c_1 + c_2 + c_3 &= 30 \\ c_0 + 2c_1 + 4c_2 + 8c_3 &= 117 \end{aligned}$$

Rešitev sistema je $c_0 = 3$, $c_1 = 13$, $c_2 = 6$, $c_3 = 8$.

3 n-ti primitivni koren enote

Iz koeficientne predstavitve v vrednostno lahko učinkovito prehajamo, če za točke $x_0, \ldots, x_{n-1}$ vzamemo potence *n-tega primitivnega korena enote*. To je število ω z lastnostma $\omega^n = 1$ in $\omega^k \neq 1$ za vse $k \in \{1, \ldots, n-1\}$. V $\mathbb{Z}$ in $\mathbb{R}$ obstaja primitivni koren enote samo za $n = 1$ ($\omega = 1$) in $n = 2$ ($\omega = -1$), veliko več možnosti pa imamo v obsegu kompleksnih števil ($\mathbb{C}$) in v modulskih celoštevilskih kolobarjih ($\mathbb{Z}_p$, kjer je p praštevilo).

V obsegu kompleksnih števil je n-ti primitivni koren enote enak $\omega = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$. Vrednosti ω^0, ω^1, $\ldots$, ω^{n-1} so enakomerno razmaknjene točke na enotskem krogu v kompleksnem koordinatnem sistemu. Na primer, pri $n = 4$ imamo $\omega^0 = \omega^4 = 1$, $\omega^1 = i$, $\omega^2 = -1$ in $\omega^3 = -i$.

Pri celoštevilskih modulskih kolobarjih so razmere nekoliko bolj zapletene, saj ni nujno, da obstaja ω za vsak $n \in \{2, \ldots, p-1\}$. Na primer, v $\mathbb{Z}_5$ imamo PKE za $n = 2$ ($\omega = 4$) in $n = 4$ ($\omega = 2$ ali $\omega = 3$), nimamo pa PKE za $n = 3$. V $\mathbb{Z}_7$ obstajajo PKE za $n = 2$ ($\omega = 6$), $n = 3$ ($\omega = 2$ ali $\omega = 4$) in $n = 6$ ($\omega = 3$ ali $\omega = 5$).

4 Diskretna Fourierova transformacija

Diskretna Fourierova transformacija (DFT) je izračun vrednostne predstavitve polinoma v točkah ω^0, ω^1, $\ldots$, ω^{n-1}. DFT lahko izračunamo z množenjem *Vandermondove matrike* z vektorjem koeficientov. Vandermondova matrika F je matrika $n \times n$, v kateri je element F_{pq} (za $p, q \in \{0, \ldots, n-1\}$) enak ω^{pq}. Na primer, pri obsegu $\mathbb{C}$ in $n = 4$ imamo $\omega = i$, Vandermondova matrika pa izgleda takole:

$$F = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \begin{matrix} (i^{0k} \text{ za } k = 0,1,2,3) \\ (i^{1k} \text{ za } k = 0,1,2,3) \\ (i^{2k} \text{ za } k = 0,1,2,3) \\ (i^{3k} \text{ za } k = 0,1,2,3) \end{matrix}$$

Pri kolobarju $\mathbb{Z}_{\not 7}$ in $n = 6$ imamo $\omega = 3$ (lahko bi vzeli tudi $\omega = 5$), pripadajoča Vandermondova matrika pa je takšna:

$$F = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix}$$

Vrednostno predstavitev polinoma v točkah ω^0, $\ldots$, ω^{n-1} lahko torej izračunamo z množenjem Vandermondove matrike z vektorjem koeficientov.

Izkaže se, da lahko na zelo podoben način izvršimo tudi obratno pretvorbo, le namesto matrike F vzamemo matriko F^{-1}. Ta matrika je skoraj enaka matriki F; njen element (p, q) je namreč $n^{-1}(\omega^{-1})^{pq}$. Matrika F^{-1} za $\mathbb{C}$ in $n = 4$ ($\omega = i$) je potemtakem videti takole:

$$F^{-1} = \frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix}$$

Zapišimo še inverzno Vandermondovo matriko za $\mathbb{Z}_7$, $n = 6$ in $\omega = 3$. Velja $6^{-1} = 6$ (ker je $6 \cdot 6 = 1$) in $3^{-1} = 5$.

$$F^{-1} = 6\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{bmatrix}$$

5 Množenje polinomov s pomočjo DFT

Sedaj imamo vse, kar potrebujemo za množenje polinomov s pomočjo DFT.

1. Izberemo vrednost n. Ta vrednost mora biti najmanj enaka $S(a) + S(b) + 1$, kjer je $S(.)$ stopnja polinoma (tj. število koeficientov minus 1). Kot bomo videli na naslednjih vajah, je za n smiselno vzeti potenco števila 2, saj lahko na ta način uporabimo algoritem za hitro računanje DFT.

2. Polinoma, zapisana z vektorjema koeficientov a in b, s pomočjo DFT pretvorimo v vektorja Fa in Fb, ki podajata vrednosti polinomov v točkah ω^0, ω^1, $\ldots$, ω^{n-1}.

3. Vektorja Fa in Fb zmnožimo po komponentah in dobimo vrednostno predstavitev produktnega polinoma c: $Fc = Fa \odot Fb$.

4. Koeficientno predstavitev produktnega polinoma izračunamo tako, da vektor Fc z leve pomnožimo z matriko F^{-1}, saj je $c = F^{-1}(Fc)$.

Oglejmo si dva primera.

5.1 Prvi primer: $a(x) = 3 + x + 2x^2$ in $b(x) = 1 + 4x$ v $\mathbb{C}$

1. Produktni polinom bo imel štiri koeficiente, zato vzamemo $n = 4$. V obsegu $\mathbb{C}$ je ω pri izbranem n enak i.

2. Izračunajmo Fa in Fb:

$$Fa = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \begin{bmatrix} 3 \\ 1 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 6 \\ 1+i \\ 4 \\ 1-i \end{bmatrix}$$

$$Fb = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \begin{bmatrix} 1 \\ 4 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 5 \\ 1+4i \\ -3 \\ 1-4i \end{bmatrix}$$

3. Zmnožimo Fa in Fb po komponentah:

$$Fc = Fa \odot Fb = \begin{bmatrix} 6 \\ 1+i \\ 4 \\ 1-i \end{bmatrix} \begin{bmatrix} 5 \\ 1+4i \\ -3 \\ 1-4i \end{bmatrix} = \begin{bmatrix} 30 \\ -3+5i \\ -12 \\ -3-5i \end{bmatrix}$$

4. Izračunamo inverzno DFT na vektorju Fc:

$$F^{-1}(Fc) = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} \begin{bmatrix} 30 \\ -3+5i \\ -12 \\ -3-5i \end{bmatrix} = \begin{bmatrix} 3 \\ 13 \\ 6 \\ 8 \end{bmatrix}$$

5. Lahko se prepričamo, da je polinom $3 + 13x + 6x^2 + 8x^3$ res zmnožek polinomov $3 + x + 2x^2$ in $1 + 4x$.

5.2 Drugi primer: $a(x) = 3 + x + 2x^2$ in $b(x) = 1 + 4x + 5x^2 + 3x^3$ v $\mathbb{Z}_{\text{ı}}$

1. Produktni polinom bo imel šest koeficientov, zato vzamemo $n = 6$. (Če bi hoteli uporabiti algoritem za hitro računanje DFT, bi vzeli $n = 8$.) Najmanjši $p \geq 6$, v katerem obstaja 6. primitivni koren enote, je enak 7. V $\mathbb{Z}_{\not{p}}$ je ω pri $n = 6$ enak 3 (lahko bi vzeli tudi $\omega = 5$).

2. Izračunajmo Fa in Fb:

$$Fa = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \\ 2 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 6 \\ 3 \\ 6 \\ 4 \\ 4 \\ 2 \end{bmatrix}$$

$$Fb = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \\ 5 \\ 3 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 6 \\ 6 \\ 4 \\ 6 \\ 2 \\ 3 \end{bmatrix}$$

3. Zmnožimo Fa in Fb po komponentah:

$$Fc = Fa \odot Fb = \begin{bmatrix} 6 \\ 3 \\ 6 \\ 4 \\ 4 \\ 2 \end{bmatrix} \begin{bmatrix} 6 \\ 6 \\ 4 \\ 6 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 1 \\ 4 \\ 3 \\ 3 \\ 1 \\ 6 \end{bmatrix}$$

4. Izračunamo inverzno DFT na vektorju Fc.

$$F^{-1}(Fc) = 6 \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \\ 3 \\ 3 \\ 1 \\ 6 \end{bmatrix} = \begin{bmatrix} 3 \\ 6 \\ 0 \\ 1 \\ 6 \\ 6 \end{bmatrix}$$

5. Zmnožek polinomov $3+x+2x^2$ in $1+4x+5x^2+3x^3$ je $3+13x+21x^2+22x^3+13x^4+6x^5$, tako da je vektor, dobljen v prejšnjem koraku, res koeficientna predstavitev produktnega polinoma po modulu 7.