Множење полинома

Дати су полиноми $P(x)=\sum_{i=0}^{n-1} p_i x^i$ и $Q(x)=\sum_{i=0}^{n-1} q_i x^i$ над пољем реалних бројева.

Задатак је израчунати њихов производ на што ефикаснији начин.

Претпоставка је да је сваки од полинома дат низом својих коефицијената.

Уколико производ PQ рачунамо директним множењем чланова сложеност алгоритма биће $O(n^2)$.

У наставку наводимо неке чињенице које могу послужити у креирању алгоритма побољшане сложености. (алгоритма заснованог на декомпозицији).

Нека је: $P(x)=P_1(x)+x^{[\frac{n}{2}]}P_2(x)$ и $Q(x)=Q_1(x)+x^{[\frac{n}{2}]}Q_2(x)$
где је

$$P_1(x)=p_0+p_1x+\dots+p_{[\frac{n}{2}]-1}x^{[\frac{n}{2}]-1},$$

$$P_2(x)=p_{[\frac{n}{2}]}+p_{[\frac{n}{2}]+1}x+\dots+p_{n-1}x^{[\frac{n}{2}]-1},$$

$$Q_1(x)=q_0+q_1x+\dots+q_{[\frac{n}{2}]-1}x^{[\frac{n}{2}]-1},$$

$$Q_2(x)=q_{[\frac{n}{2}]}+q_{[\frac{n}{2}]+1}x+\dots+q_{n-1}x^{[\frac{n}{2}]-1}.$$

$$P(x)\cdot Q(x)=\left(P_1(x)+x^{[\frac{n}{2}]}P_2(x)\right)\left(Q_1(x)+x^{[\frac{n}{2}]}Q_2(x)\right)$$
$$=P_1(x)Q_1(x)+\left(P_1(x)Q_2(x)+P_2(x)Q_1(x)\right)x^{[\frac{n}{2}]}+P_2(x)Q_2(x)x^n$$

Означимо са: $A(x)=P_1(x)\cdot Q_1(x)$, $B(x)=P_1(x)Q_2(x)$, $C(x)=P_2(x)Q_1(x)$, $D(x)=P_2(x)Q_2(x)$

Приметимо да нам приликом множења полинома нису потребни $B(x)$ и $C(x)$ појединачно, већ збир $B(x)+C(x)$, односно:

$$P(x)\cdot Q(x) = A(x) + (B(x)+C(x))\cdot x^{[\frac{n}{2}]} + D(x)x^{n}$$

Ако је $E(x) = (P_1(x)+P_2(x))(Q_1(x)+Q_2(x))$ онда је

$$B(x)+C(x) = E(x) - A(x) - D(x).$$

Другим речима, довољно је израчунати само три производа мањих полинома $A(x)$, $D(x)$ и $E(x)$. Све остало су сабирања и одузимања полинома. (што ће бити урачунато у слободан члан $O(n)$ рекурентне једначине сложености)

Рекурентна једначина за сложеност побољшаног алгоритма је:

$$T(n) = \underbrace{3T\left(\frac{n}{2}\right)} + O(n).$$

$\hookrightarrow$ сабирања и одузимања

проблем
производа
полинома степена $n-1$
разбијен је на 3 множења
полинома дупло мањег
степена који се опет рачунају
декомпозицијом на дупло мање
степене...

Како бисмо проценили сложеност алгоритма решићемо претходну рекурентну једначину.

$$T(n) = 3T\left(\frac{n}{2}\right) + O(n)$$
$$= 3\left(3T\left(\frac{n}{4}\right) + O\left(n+\frac{n}{2}\right)\right)$$
$$= \dots$$
$$= 3^{\log_2 n}\,T(1) + O\left(n+\frac{n}{2}+\frac{n}{4}+\dots+2\right)$$

па је $T(n) = 3^{\log_2 n} + O(n)$.

Како је $\log_2 n = \dfrac{\log_3 n}{\log_3 2}$, следи да је

$$3^{\log_2 n} = \left(3^{\log_3 n}\right)^{\frac{1}{\log_3 2}} = n^{\frac{1}{\log_3 2}} = n^{\log_2 3}.$$

Дакле, $T(n) = O(n^{\log_2 3}) = O(n^{1,59})$, па ово јесте ефикаснији алгоритам од алгоритма сложености $O(n^2)$.

Пример: Нека је $n=4$, $P(x) = 1 - x + 2x^2 - x^3$ и $Q(x) = 2 + x - x^2 + 2x^3$.

$$P(x) = \underbrace{1 - x}_{P_1(x)} + x^2 \underbrace{(2 - x)}_{P_2(x)}$$

$$Q(x) = \underbrace{2 + x}_{Q_1(x)} + x^2 \underbrace{(-1 + 2x)}_{Q_2(x)}$$

Линеарне полиноме множимо, такође, рекурзивно множећи полиноме степена 0 (коефицијенте). Дакле,

$$A(x) = P_1(x)Q_1(x) = (1-x)(2+x)$$
$$= 1\cdot 2 + x\left((1+2)\cdot(-1+1) - 1\cdot 2 - (-1)\cdot 1\right) + x^2\cdot(-1)\cdot 1$$
$$= 2 - x - x^2$$

$$D(x) = P_2(x)Q_2(x) = (2-x)(-1+2x)$$
$$= 2\cdot(-1) + x\left((2+(-1))(-1+2) - 2\cdot(-1) - (-1)\cdot 2\right) + x^2\cdot(-1)\cdot 2$$
$$= -2 + 5x - 2x^2$$

$$E(x) = (P_1(x) + P_2(x))(Q_1(x) + Q_2(x)) = (3-2x)(1+3x)$$
$$= 3\cdot 1 + x\left((3+1)(-2+3) - 3\cdot 1 - (-2)\cdot 3\right) + x^2\cdot(-2)\cdot 3$$
$$= 3 + 6x - 6x^2$$

На основу $A(x)$, $D(x)$ и $E(x)$ израчунава се $B(x) + C(x) = E(x) - A(x) - D(x)$

па је

$$B(x)+C(x)=3+3x-3x^2$$

Сада је $P(x)Q(x)=A(x)+(B(x)+C(x))x^2+D(x)x^4$, односно

$$P(x)Q(x)=(2-x-x^2)+(3+3x-3x^2)x^2+(-2+5x-2x^2)x^4$$
$$=2-x+2x^2+3x^3-5x^4+5x^5-2x^6$$

Укупан број различитих множења је:

3 множења: $1\cdot 2$, $(1+2)\cdot(-1+1)$, $(-1)\cdot 1$ при рачунању $A(x)$
3 множења: $2\cdot(-1)$, $(2+(-1))\cdot(-1+2)$, $(-1)\cdot 2$ при рачунању $D(x)$
3 множења: $3\cdot 1$, $(3+1)\cdot(-2+3)$, $(-2)\cdot 3$ при рачунању $E(x)$

односно 9 множења, насупрот 16 множења код наивног алгоритма. Из овог видимо да је уштеда броја множења велика чак и за мало n.

У наставку дајемо још ефикаснији алгоритам, алгоритам сложености $O(n\log n)$.

Брза Фуријеова трансформација

скраћено FFT (од fast Fourier transform)

Полином степена $n-1$ потпуно је одређен вредностима у n различитих тачака.

Дакле, осим низом коефицијената, полином степена $n-1$ можемо представити и вредностима у n различитих тачака.

Израчунавање вредности полинома $p(x) = p_0 + p_1 x + \dots + p_{n-1} x^{n-1}$ у тачки a могуће је извршити помоћу $n-1$ множења и $n-1$ сабирања (Хорнеров метод):

$$p(a) = (\dots(((p_{n-1} \cdot a + p_{n-2}) \cdot a + p_{n-3}) \cdot a + p_{n-4}) a + \dots) a + p_0$$

нпр. вредност полинома $p(x) = 1 + 2x + 3x^2$ у тачки 4 рачунамо као

$$p(4) = (3 \cdot 4 + 2) \cdot 4 + 1 = 57$$

и користимо 2 множења и 2 сабирања.

Дакле, рачунање вредности полинома $p(x)$ и n различитих тачака изводљиво је помоћу n^2 множења.

Уколико полиноме преведемо у репрезентацију дату вредностима у тачкама онда лако може бити израчунат производ $P(x) \cdot Q(x)$. Полином $P(x) Q(x)$ је полином степена $2n-2$ па је одређен вредностима у $2n-1$ тачки. Ако претпоставимо да су вредности полинома-чинилаца дате у $2n-1$ тачки, тада се вредност производа полинома израчунава помоћу $2n-1$ множења (по једно множење за сваку тачку јер је $P \cdot Q(a) = P(a) \cdot Q(a)$) односно, потребно је $O(n)$ множења.

Нажалост, представљање полинома вредностима у тачкама није увек погодно за примену. На пример, у том случају није лако израчунати вредност у неким (другим) тачкама. Међутим, уколико би се помоћу неких алгоритама лако прелазило из једне репрезентације у другу добио би се одличан алгоритам за множење полинома. То се постиже помоћу FFT.

Прелаз са репрезентације полинома вредностима у тачкама на репрезентацију коефицијентима назива се интерполација.

Брзина интерполације зависи од избора тачака. Брза Фуријеова трансформација користи специјалан скуп тачака, тако да се и интерполација и израчунавање вредности полинома могу ефикасно извршити.

Ако је $P(x) = \sum_{i=0}^{n-1} p_i x^i$, тада је

$$P(x) = P_e(x^2) + x P_o(x^2),$$

где је $P_e(x) = \sum_{j=0}^{n/2-1} p_{2j} x^j$ и $P_o(x) = \sum_{j=0}^{n/2-1} p_{2j+1} x^j$.

Ако је a нека тачка, тада је

$$P(a) = P_e(a^2) + a P_o(a^2)$$
$$P(-a) = P_e(a^2) + (-a) P_o(a^2).$$

Према томе, израчунавање вредности полинома $P(x)$ у n тачака $a_0, a_2, \ldots, a_{n-1}$ сводимо на израчунавање вредности полинома $P_o(x^2)$ и $P_e(x^2)$ (два полинома степена $\frac{n}{2}-1$) у $\frac{n}{2}$ тачака a_i, $i=0,\ldots,\frac{n}{2}-1$, ако тачке бирамо тако да је $a_{\frac{n}{2}+j} = -a_j$, за $j=0,1,\ldots,n/2-1$.

При рачунању $P(a_i)$ и $P(-a_i)$ имамо потпроблеме величине $\frac{n}{2}$ (што су $P_e(a_i^2)$ и $P_o(a_i^2)$), $\frac{n}{2}$ допунских сабирања и $\frac{n}{2}$ допунских множења. Дакле, имамо два потпроблема величине $\frac{n}{2}$ и $O(n)$ допунских операција.

Ако би се наставило рекурзивно на исти начин, дошли бисмо до рекурентне једначине $T(n) = 2T(\frac{n}{2}) + O(n)$

чије је решење $T(n) = O(n\log n)$. (погледати сложеност алгоритама).

Ако бисмо желели да наставимо даље са редукцијом дошли бисмо до следећег проблема:

вредности x у $P(x)$ могу се произвољно бирати али вредности x^2 у $P_0(x^2)$ могу бити само позитивне јер су квадрати реалних бројева увек позитивни.

Нпр. желимо да је $(a_0)^2 = -(a_{\frac{n}{4}})^2$ ако хоћемо да наставимо са рекурзијом. Генерално, желимо да је

$$(a_j)^2 = -(a_{\frac{n}{4}+j})^2, \quad j = 0, 1, \ldots, \frac{n}{4}-1.$$

Ово можемо постићи ако "напустимо" поље реалних бројева и пређемо у поље комплексних бројева, односно ако је

$$a_{\frac{n}{4}+j} = i a_j, \quad \text{за } j = 0, 1, \ldots, \frac{n}{4}-1.$$

Ако наставимо са разбијањем на потпроблеме долазимо до захтева

$$(a_j)^4 = -(a_{\frac{n}{8}+j})^4, \quad \text{за } j = 0, 1, \ldots, \frac{n}{8}-1$$

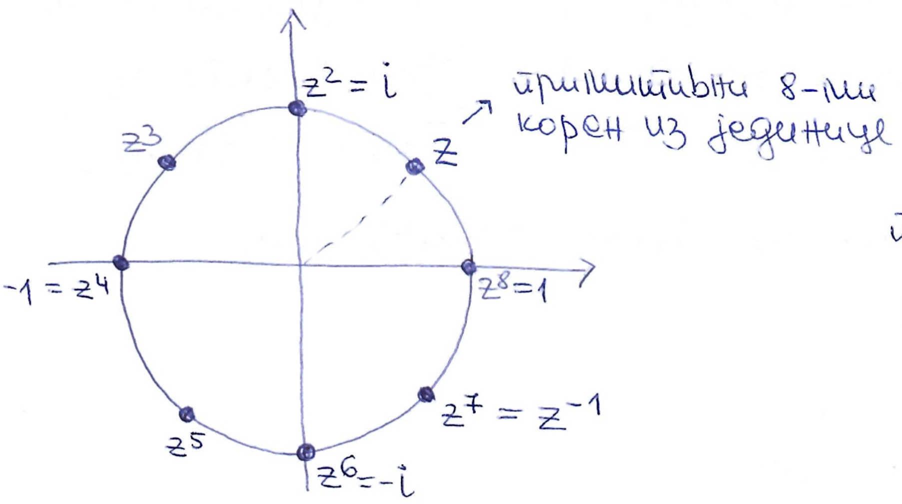
што ће бити испуњено ако је

$$a_{\frac{n}{8}+j} = z a_j, \quad \text{за } j = 0, 1, \ldots, \frac{n}{8}-1,$$

где је z примитивни 8-ми корен из јединице (тј. $z^8 = 1$ и $z^j \neq 0$ за све $0 < j < 8$).

Генерално, потребан нам је n-ти примитивни корен из јединице, означићемо га са ω. Број ω задовољава следеће услове:

$$\omega^n = 1, \quad \omega^j \neq 1 \text{ за } 0 < j < n.$$



приметимо да је $z^4 = -1$
и $z^2 = -1$

Генерално, важи да је $\omega^{\frac{n}{2}} = -1$.

На основу претходне анализе, за n тачака $a_0, a_1, \ldots, a_{n-1}$ бирамо комплексне бројеве $1, \omega, \omega^2, \ldots, \omega^{n-1}$ што нам гарантује да су различити (размисли-важи). Приметимо да

$$a_{\frac{n}{2}+j} = \omega^{\frac{n}{2}+j} = \underbrace{\omega^{\frac{n}{2}}}_{=-1} \cdot \omega^j = -\omega^j = -a_j, \quad j = 0, 1, \ldots, \tfrac{n}{2}-1.$$

Ако је $P(x) = \sum_{j=0}^{n-1} p_j x^j$, прелазак са вектора

$$(p_0, p_1, \ldots, p_{n-1})$$

на вектор

$$(P(1), P(\omega), \ldots, P(\omega^{n-1}))$$

називамо Фуријеова трансформација.

Претходним разматрањима решили смо само део проблема множења полинома: вредности полинома $P(x)$ и $Q(x)$ могу се ефикасно израчунати у тачкама $1, \omega, \ldots, \omega^{n-1}$, изможити парови добијених вредности и тако наћи вредност полинома у наведеним тачкама.

Остаје проблем интерполације, односно одређивања коефицијената производа на основу вредности у тачкама. Показује се да је проблем интерполације врло сличан проблему израчунавања вредности.

Ако је

$$V(\omega) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \omega^{n-1} & \cdots & \omega^{(n-1)(n-1)} \end{pmatrix}$$

$$p = \begin{pmatrix} p_0 \\ p_1 \\ \vdots \\ p_{n-1} \end{pmatrix}, \quad v = \begin{pmatrix} P(1) \\ P(\omega) \\ \vdots \\ P(\omega^{n-1}) \end{pmatrix}$$

онда важи $V(\omega)p = v$ па је

$$\underbrace{V^{-1}(\omega)V(\omega)}_{E}\, p = V^{-1}(\omega)\, v.$$

Дакле, лако се добија да је вектор коефицијената

$$p = V^{-1}(\omega)\, v.$$

Како је $V^{-1}(\omega) = \frac{1}{n} V(\omega^{-1})$, вектор p се може израчунати применом брзе Фуријеове трансформације, заменом ω са ω^{-1}. Ова трансформација се назива инверзна Фуријеова трансформација.

Пример: Израчунати брзу Фуријеову трансформацију вектора $P(x) = 1+2x+3x^2+4x^3$.

Полином $P(x)$ дат је листом (вектором) коефицијената $(1,2,3,4)$.

Означимо са $P_{j_0,j_1,\dots,j_k}(a_0,a_1,\dots,a_k)$ проблем одређивања вредности полинома $j_0+j_1x+\dots+j_kx^k$ у тачкама $a_0,a_1,\dots,a_k$. Дакле, $j_0,j_1,\dots,j_k$ означавају коефицијенте полинома, а $a_0,\dots,a_k$ су тачке у којима се израчунава вредност тог полинома.

Према томе, наш задатак се своди на решавање

$$P_{1,2,3,4}(1,\omega,\omega^2,\omega^3),$$

где је ω 4-ти корен (примитивни) из јединице, тј. важи $\omega^4=1$ и $\omega^2=-1$.

Дрво рекурзије изгледа овако:

$$\begin{tikzcd}[column sep=small]
 & & & P_{1,2,3,4}(1,\omega,\omega^2,\omega^3) \arrow[dll, no head] \arrow[drr, no head] & & & \\
 & P_{1,3}(1,\omega^2) \arrow[dl, no head] \arrow[dr, no head] & & & & P_{2,4}(1,\omega^2) \arrow[dl, no head] \arrow[dr, no head] & \\
\underbrace{P_1(1)}_{=1} & & \underbrace{P_3(1)}_{=3} & & \underbrace{P_2(1)}_{=2} & & \underbrace{P_4(1)}_{=4}
\end{tikzcd}$$

У првом кораку смо проблем $P_{1,2,3,4}(1,\omega,\omega^2,\omega^3)$ свели на два потпроблема $P_{1,3}(1,\omega^2)$ и $P_{2,4}(1,\omega^2)$, које у наредним корацима сводимо на мање потпроблеме $P_1(1)$ и $P_3(1)$, односно $P_2(1)$ и $P_4(1)$.

Kako je $P(x)=P_e(x^2)+xP_o(x^2)$ dobijamo:

$$P_{1,3}(1)=P_1(1^2)+1\cdot P_3(1^2)=P_1(1)+P_3(1)=1+3=4$$

$$P_{1,3}(\omega^2)=P_1(\underbrace{\omega^4}_{=1})+\omega^2 P_3(\underbrace{\omega^4}_{=1})=P_1(1)+\underbrace{\omega^2}_{=-1}P_3(1)=1-3=-2$$

$$\Longrightarrow \quad P_{1,3}(1,\omega^2)=(4,-2)$$

$$P_{2,4}(1)=P_2(1^2)+1\cdot P_4(1^2)=P_2(1)+P_4(1)=2+4=6$$

$$P_{2,4}(\omega^2)=P_2(\underbrace{\omega^4}_{=1})+\underbrace{\omega^2}_{=-1}\cdot P_4(\underbrace{\omega^4}_{=1})=P_2(1)-P_4(1)=2-4=-2$$

$$\Longrightarrow \quad P_{2,4}(1,\omega^2)=(6,-2)$$

$$P_{1,2,3,4}(1)=P_{1,3}(1^2)+1\cdot P_{2,4}(1^2)=P_{1,3}(1)+P_{2,4}(1)=4+6=10$$

$$P_{1,2,3,4}(\omega)=P_{1,3}(\omega^2)+\omega\, P_{2,4}(\omega^2)=-2+\omega\,(-2)=-2-2\omega$$

$$P_{1,2,3,4}(\omega^2)=P_{1,3}(\underbrace{\omega^4}_{=1})+\underbrace{\omega^2}_{=-1}P_{2,4}(\underbrace{\omega^4}_{=1})=4+(-1)\cdot 6=-2$$

$$P_{1,2,3,4}(\omega^3)=P_{1,3}(\underbrace{\omega^6}_{=\omega^2})+\underbrace{\omega^3}_{=-\omega}P_{2,4}(\underbrace{\omega^6}_{=\omega^2})=P_{1,3}(\omega^2)-\omega P_{2,4}(\omega^2)$$

$$=-2-\omega\cdot(-2)=-2+2\omega$$

Dakle,

$$P_{1,2,3,4}(1,\omega,\omega^2,\omega^3)=(10,-2-2\omega,-2,-2+2\omega).$$

Пример: Израчунати инверзну Фуријеову трансформацију вектора $(10, -2-2\omega, -2, -2+2\omega)$.

Задатак је решити проблем

$$P_{10,-2-2\omega,-2,-2+2\omega}(1,\omega^{-1},\omega^{-2},\omega^{-3})$$

и на крају све помножити са $\frac{1}{n}=\frac{1}{4}$.

$$P_{10,-2-2\omega,-2,-2+2\omega}(1,\omega^{-1},\omega^{-2},\omega^{-3})$$

$$P_{10,-2}(1,\omega^{-2}) \qquad\qquad P_{-2-2\omega,-2+2\omega}(1,\omega^{-2})$$

$$\begin{array}{cccc} P_{10}(1) & P_{-2}(1) & P_{-2-2\omega}(1) & P_{-2+2\omega}(1) \\ \shortparallel & \shortparallel & \shortparallel & \shortparallel \\ 10 & -2 & -2-2\omega & -2+2\omega \end{array}$$

$$P_{10,-2}(1) = P_{10}(1^2) + 1\, P_{-2}(1^2) = 10-2 = 8$$

$$P_{10,-2}(\omega^{-2}) = P_{10}(\omega^{-4}) + \omega^{-2} P_{-2}(\omega^{-4}) = 10 + (-1)\cdot(-2) = 12$$

$$\Rightarrow \quad P_{10,-2}(1,\omega^{-2}) = (8,12)$$

$$P_{-2-2\omega,-2+2\omega}(1) = P_{-2-2\omega}(1^2) + 1\, P_{-2+2\omega}(1^2) = -2-2\omega-2+2\omega = -4$$

$$P_{-2-2\omega,-2+2\omega}(\omega^{-2}) = P_{-2-2\omega}(\omega^{-4}) + \omega^{-2} P_{-2+2\omega}(\omega^{-4})$$

$$= -2-2\omega - (-2+2\omega) = -4\omega$$

$$\Rightarrow \quad P_{-2-2\omega,-2+2\omega}(1,\omega^{-2}) = (-4,-4\omega)$$

$$P_{10,-2-2\omega,-2,-2+2\omega}(1) = P_{10,-2}(1^2) + 1\cdot P_{-2-2\omega,-2+2\omega}(1)$$

$$= 8 + 1\cdot(-4) = 4$$

$$P_{10,-2-2\omega,-2,-2+2\omega}(\omega^{-1}) = P_{10,-2}(\omega^{-2}) + \omega^{-1} P_{-2-2\omega,-2+2\omega}(\omega^{-2})$$

$$= 12 + \omega^{-1} \cdot (-4\omega) = 8$$

$$P_{10,-2-2\omega,-2,-2+2\omega}(\omega^{-2}) = P_{10,-2}(\underset{1}{\underset{\shortparallel}{\omega^{-4}}}) + \underset{-1}{\underset{\shortparallel}{\omega^{-2}}} P_{-2-2\omega,-2+2\omega}(\underset{1}{\underset{\shortparallel}{\omega^{-4}}})$$

$$= 8 + (-1)\cdot(-4) = 12$$

$$P_{10,-2-2\omega,-2,-2+2\omega}(\omega^{-3}) = P_{10,-2}(\underset{\omega^{-2}}{\underset{\shortparallel}{\omega^{-6}}}) + \omega^{-3} P_{-2-2\omega,-2+2\omega}(\underset{\omega^{-2}}{\underset{\shortparallel}{\omega^{-6}}})$$

$$= 12 + \omega^{-3} \cdot (-4\omega) = 12 - 4\underbrace{\omega^{-2}}_{=-1}$$

$$= 12 + 4 = 16$$

$$\Rightarrow P_{10,-2-2\omega,-2,-2+2\omega}(1, \omega^{-1}, \omega^{-2}, \omega^{-3}) = (4, 8, 12, 16)$$

Када се вектор $(4,8,12,16)$ помножи са $\frac{1}{4}$ добијамо решење:

$$(1,2,3,4).$$