1. Rychlá Fourierová transformácia

Budeme značiť teleso $\mathbf{T}$ a ω jeho prvok.

Veta 1.1 (o interpolácií). *Nech $\alpha_0, \alpha_1, \dots, \alpha_n$ sú po dvoch rôzne prvky telesa $\mathbf{T}[x]$. Potom pre každé $u_0, u_1, \dots, u_n \in \mathbf{T}$ existuje práve jeden polynóm $p \in \mathbf{T}[x]$ stupňa najviac n splňujúci*

$$\begin{aligned} p(\alpha_0) &= u_0 \\ p(\alpha_1) &= u_1 \\ &\vdots \\ p(\alpha_n) &= u_n. \end{aligned}$$

Definícia (modulárna reprezentácia polynómu). Zobrazenie

$$\mathbf{T}[x] \to \mathbf{T}[x]/(x - \alpha_0) \times \cdots \times \mathbf{T}[x]/(x - \alpha_n), p \mapsto (p(\alpha_0), \dots, p(\alpha_n))$$

je modulárnou reprezentáciou polynómu nad telesom $\mathbf{T}[x]$ vzhľadom k bodom $\alpha_0, \alpha_1, \dots, \alpha_n$.

Síce skutočná všeobecná definícia modulárnej reprezentácia je založená na pozorovaniach, ktoré vyplývajú z čínskej vety o zbytkoch a z vety o interpolácií polynómu, bude nám pre ďalšie účely postačovať definícia modulárnej reprezentácii polynómu vyššie, preto nebudeme zavádzať všeobecnú definíciu.

Diskrétnou Fourierovou transformáciou $\mathrm{DFT}(\omega)$ s parametrom ω rozumieme výpočet hodnôt polynómu $p \in \mathbf{T}[x]$ stupňa nejviac $n-1$ v bodoch $1, \omega, \omega^2, \dots, \omega^{n-1}$. Diskrétnu Fourierovú transformáciu môžeme chápať aj ako zobrazenie medzi vektorovými priestormi $\mathbf{T}^n \to \mathbf{T}^n$, ktoré vektoru koeficientov priradí vektor hodnôt v týchto bodoch. Teda pre polynóm $p = \sum_{i=0}^{n-1} a_i x^i$ platí

$$\mathrm{DFT}(\omega)(a_0, a_1, \dots, a_{n-1}) = (p(1), p(\omega), \dots, p(\omega^{n-1})).$$

Pretože hodnotu polynómu v ľubovoľnom bode α môžeme dostať násobením istého riadkového vektoru závislého na α a stále rovnakého stĺpcového vektoru podľe vzorca

$$p(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^i = \left(1, \alpha, \alpha^2 \dots, \alpha^{n-1}\right) \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix},$$

pre diskrétnu Fourierovu transformáciu platí vzorec

$$\mathrm{DFT}(\omega)(u) = A(\omega) \cdot u,$$

kde u je stĺpcový vektor $(a_0, a_1, \dots, a_{n-1})^T$ a $A(\omega)$ je Vandermondova matice tvaru

$$A(\omega) = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(n-1)} \\ \vdots & & & & \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \dots & \omega^{(n-1)(n-1)} \end{pmatrix}$$

Teda $\mathrm{DFT}(\omega)$ je lineárne zobrazenie. Naviac, ak sú prvky $1, \omega, \dots, \omega^{n-1}$ po dvoch rôzne, potom je toto zobrazenie bijektívne, pretože determinant Vandermondovej matice $A(\omega)$ je rovný súčinu $\prod_{i>j}(\omega^i - \omega^j)$. Za tohoto predpokladu môžeme uvažovať inverzné zobrazenie $\mathrm{DFT}(\omega)^{-1}$, ktoré sa nazýva *inverzná diskrétna Fourierová transformácia* a budeme ho značiť $\mathrm{IDFT}(\omega)$. Môžeme vidieť, že

$$\mathrm{IDFT}(\omega)(u) = A(\omega)^{-1} \cdot u.$$

IDFT je vlastne *interpolácia polynómu* z hodnôt v bodoch $1, \omega, \omega^2, \ldots, \omega^{n-1}$ a celá diskrétna Fourierová transformácia a jej inverz sú špeciálnym prípadom modulárnej reprezentácie. Jej zmysel je v tom, že pre isté ω existuje veľmi rýchly algoritmus na ich výpočet.

Definícia (n-tá odmocnina z jednej)**.** Povieme, že prvok $\omega \in \mathbf{T}$ je *primitívna n-tá odmocnina z jednej* v telese $\mathbf{T}$, ak platí

(1) $\omega^n = 1$,
(2) $\omega^i \neq 1$ pre všetky $i = 1, 2, \ldots, n-1$.

Inými slovami, ak je rád prvku ω v grupe $\mathbf{T}^*$ rovný n.

Príklad (n-té odmocniny z jednej)**.**

(1) V telese $\mathbb{C}$ je $\omega = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$ primitívnou n-tou odmocninou z jednej, ako sa dá ukázať, keď si nakreslíte jej mocniny v komplexnej rovine (tvorí vrcholy pravidelného n-uholníka)
(2) V telese $\mathbb{Z}_5$ je $\omega = 2$ primitívnou štvrtou odmocninou z jednej, pretože $2^2 = 4$, $2^3 = 3$ a $2^4 = 1$. Všeobecne, každý generátor grupy $\mathbb{Z}_p^*$ je primitívnou $p-1$-tou odmocninou z jednej v telese $\mathbb{Z}_p$.

Všimnime si, že ak je ω primitívna n-tá odmocnina z jednej, tak potom je matica $A(\omega)$ regulárna.

Tvrdenie 1.2. *Ak je ω primitívna n-tá odmocnina z jednej v telese $\mathbf{T}$ a*

$$A(\omega) = \left(\omega^{ij}\right)_{i,j=0}^{n-1},$$

potom

$$A(\omega)^{-1} = \frac{1}{n} \cdot \left(\omega^{-ij}\right)_{i,j=0}^{n-1}.$$

Inými slovami,

$$\mathrm{IDFT}(\omega) = \frac{1}{n} \cdot \mathrm{DFT}(\omega^{-1}).$$

Proof. Dokážeme, že súčin týchto dvoch matíc je jednotková matica (z toho vyplýva, že sú navzájom inverzné). Podľa vzorca pre súčin matíc platí

$$\left(\omega^{ij}\right)_{i,j=0}^{n-1} \cdot \frac{1}{n} \cdot \left(\omega^{-ij}\right)_{i,j=0}^{n-1} = \frac{1}{n} \cdot \Big(\sum_{k=0}^{n-1} \omega^{ik}\omega^{-kj}\Big)_{i,j=0}^{n-1}.$$

Pritom pre $i = j$ máme

$$\frac{1}{n} \cdot \sum_{k=0}^{n-1} \omega^{ik}\omega^{-ki} = \frac{1}{n} \cdot \sum_{k=0}^{n-1} 1 = \frac{1}{n} \cdot (n \cdot 1) = 1.$$

Naopak, pre $i \neq j$

$$\sum_{k=0}^{n-1} \omega^{ik}\omega^{-kj} = \sum_{k=0}^{n-1} \omega^{k(i-j)} = \sum_{k=0}^{n-1} (\omega^{i-j})^k,$$

dostali sme geometrickú radu. Pretože ω je *primitívna* odmocnina, máme $\omega^{i-j} \neq 1$ a môžeme použiť známy vzorec, ktorý hovorí, že

$$\sum_{k=0}^{n-1} (\omega^{i-j})^k = \frac{(\omega^{i-j})^n - 1}{\omega^{i-j} - 1}.$$

Zároveň však $\omega^n = 1$, a teda $(\omega^{i-j})^n = (\omega^n)^{i-j} = 1^{i-j} = 1$. Máme výsledek a ten je 0.

Dokázali sme, že na diagonále súčinu týchto dvoch matíc sú jednotky a mimo diagonálu nuly. Súčinom je teda jednotková matica. □

Nemusíme sa teda zaoberať výpočtom IDFT, pretože ten môžeme urobiť rovnako ako DFT, len s iným parametrom.

Princípom rýchleho algoritmu na výpočet DFT je metóda *rozdeľ a panuj*. Ak je n nepárne, môžeme počítať hodnotu polynómu $p = \sum_{i=0}^{n-1} a_i x^i$ v bode α rekurzívne takto:

$$p(\alpha) = \underbrace{(a_0 + a_2\alpha^2 + a_4\alpha^4 + \ldots + a_{n-2}\alpha^{n-2})}_{q(\alpha^2)} + \underbrace{(a_1\alpha + a_3\alpha^3 + \ldots + a_{n-1}\alpha^{n-1})}_{\alpha r(\alpha^2)},$$

tj.

$$p(\alpha) = q(\alpha^2) + \alpha r(\alpha^2),$$

pričom q, r sú polynómy definované

$$q(x) = \sum_{i=0}^{\frac{n}{2}-1} a_{2i} x^i \quad \text{a} \quad r(x) = \sum_{i=0}^{\frac{n}{2}-1} a_{2i+1} x^i.$$

Teda úlohu dosadenia hodnoty α do polynómu s n koeficientmi sme rozdelili na dve úlohy dosadenia hodnoty α^2 do polynómov polovičnej veľkosti.

Aby sme mohli úlohu deliť na polovičnú vo všetkých krokoch, predpokladajme naďalej, že n je mocninou dvojky.

Algoritmus 1.3 (Rýchla Fourierová transformácia)**.** `FFT`(ω)

`VSTUP:` $a_0, a_1, \ldots, a_{n-1}$.
`VÝSTUP:` $\mathrm{DFT}(\omega)(a_0, a_1, \ldots, a_{n-1})$.
`0.` `IF` $n = 1$ `THEN RETURN` a_0, `STOP`.
`1.` $(b_0, \ldots, b_{\frac{n}{2}-1}) := \mathtt{FFT}(\omega^2)(a_0, a_2, \ldots, a_{n-2})$,
$(c_0, \ldots, c_{\frac{n}{2}-1}) := \mathtt{FFT}(\omega^2)(a_1, a_3, \ldots, a_{n-1})$.
`2.` Pro $i = 0, \ldots, \frac{n}{2} - 1$ polož $d_i := b_i + \omega^i c_i$, $d_{i+\frac{n}{2}} := b_i - \omega^i c_i$,
`RETURN` $(d_0, \ldots, d_{n-1})$.

Tvrdenie 1.4. *Ak je n mocnina dvojky a ω primitívna n-tá odmocnina z jednej v telese $\mathbf{T}$, potom Algoritmus 1.3 funguje.*

Proof. Dôkaz predvedieme indukciou podľa n. Pre $n = 1$ je $\mathrm{DFT}(\omega)$ dosadenie do konštantného polynómu s koeficientom a_0, teda výsledok je a_0. Prevedieme indukční krok. Nech $p = \sum_{i=0}^{n} a_i x^i$ a definujeme polynómy q, r ako vyššie. Podľa indukčného predpokladu

$$(b_0, \ldots, b_{\frac{n}{2}-1}) = (q(1), q(\omega^2), q(\omega^4), \ldots, q(\omega^{n-2}))$$

a

$$(c_0, \ldots, c_{\frac{n}{2}-1}) = (r(1), r(\omega^2), r(\omega^4), \ldots, r(\omega^{n-2})).$$

Chceme dokázať, že pre $i = 0, 1, \ldots, \frac{n}{2} - 1$ platí

$$d_i = p(\omega^i) \quad \text{a} \quad d_{i+\frac{n}{2}} = p(\omega^{i+n/2}).$$

Prvý vzťah plynie priamo zo vzorca odvodeného vyššie:

$$p(\omega^i) = q(\omega^{2i}) + \omega^i r(\omega^{2i}) = b_i + \omega^i c_i = d_i.$$

Podobne odvodíme aj druhý vzťah:

$$p(\omega^{i+n/2}) = q(\omega^{2i+n}) + \omega^{i+n/2} r(\omega^{2i+n}) = b_i - \omega^i c_i = d_{i+\frac{n}{2}}.$$

Na tomto mieste využívame jednoduché pozorovanie, že $\omega^{2i+n} = \omega^{2i}\omega^n = \omega^{2i}$ a že $\omega^{i+n/2} = \omega^i \omega^{n/2} = -\omega^i$. Pritom $\omega^{n/2} = -1$, pretože to je druhá odmocnina z jednej, a tie sú len dve: 1 (tá to nie je, pretože ω je *primitívna* odmocnina) a -1.

K funkčnosti algoritmu ostáva dokázať, že ω^2 je primitívna $\frac{n}{2}$-tá odmocnina z jednej. Zrejme $(\omega^2)^{n/2} = \omega^n = 1$ a ďalej pre všetky $i = 1, 2, \ldots, \frac{n}{2} - 1$ platí $(\omega^2)^i = \omega^{2i} \neq 1$, pretože $2i < n$ a ω je primitívna odmocnina. □

Tvrdenie 1.5. *Algoritmus 1.3 má časovú zložitosť $\mathcal{O}(n \log n)$ (ako jednotkovú operáciu uvažujeme akúkoľvek operáciu v telese $\mathbf{T}$).*

Proof. Budeme postupovať podľa už niekoľkokrát použitého schématu pre algoritmy rozdeľ a panuj. Predpokladajme, že $n = 2^k$. Označme $T(n)$ počet operácií v telese $\mathbf{T}$, ktoré algoritmus vykoná na vstupe dĺžky n. Všimnime si, že $T(1) = 0$ a

$$T(n) = 2T(\frac{n}{2}) + cn$$

pre istú konštantu c. Platí teda

$$\begin{aligned}
T(2^k) &= 2T(2^{k-1}) + c2^k \\
&= 2(2T(2^{k-2}) + c2^{k-1}) + c2^k = 4T(2^{k-2}) + c(2^k + 2^k) \\
&= \ldots \\
&= 2^k T(2^{k-k}) + ck2^k = 2^k T(1) + ck2^k = \mathcal{O}(k2^k).
\end{aligned}$$

Teda $T(n) = \mathcal{O}(n \log n)$. □

Príklad (FFT)**.** Uvažujme polynóm $p = 5x^3 + x + 1 \in \mathbb{Z}_{41}[x]$. Môžeme zvoliť $\omega = -9$, pretože $\omega^2 = -1$, $\omega^3 = 9$ a $\omega^4 = 1$. Spočítajme $\mathrm{DFT}(\omega)(1, 1, 0, 5)$ pomocou Rýchlej Fourierovej transformácie: $\texttt{FFT}(\omega^2)(1, 0) = (1, 1)$, $\texttt{FFT}(\omega^2)(1, 5) = (6, -4)$, výsledok teda je $(1 + \omega^0 6, 1 + \omega^1 \cdot (-4), 1 - \omega^0 6, 1 - \omega^1(-4)) = (1 + 6, 1 + (-9) \cdot (-4), 1 - 6, 1 - (-9) \cdot (-4)) = (7, -4, -5, 6)$.

Ostáva vyriešiť otázku, ako zvoliť parameter ω, tj. odkiaľ vziať v telese $\mathbf{T}$ primitívnu n-tú odmocninu z jednej. Ako už bolo povedané, v telese $\mathbb{C}$ existuje primitívna n-tá odmocnina z jednej pre každé n, napr.

$$\omega = e^{\frac{2\pi i}{n}} = \cos \frac{2\pi i}{n} + i \sin \frac{2\pi i}{n}.$$

Pre telesa $\mathbb{Z}_p$ platí nasledujúce tvrdenie:

Tvrdenie 1.6. *V telese $\mathbb{Z}_p$ existuje primitívna n-tá odmocnina z jednej práve vtedy, ak $n \mid p - 1$. V tom prípade je primitívnou n-tou odmocninou každý prvok $a^{\frac{p-1}{n}}$, kde a je generátor grupy $\mathbb{Z}_p^*$.*

Proof. Pripomeňme, že primitívna n-tá odmocnina z jednej je vlastne prvok $\omega \in \mathbb{Z}_p^*$ rádu n. Vieme, že $|\mathbb{Z}_p^*| = p-1$, a teda, podľa Lagrangeovej vety, ak $n \nmid p-1$, potom žiadny prvok rádu n neexistuje. V opačnom prípade využijeme faktu, že grupa $\mathbb{Z}_p^*$ je cyklická, teda existuje prvok $a \in \mathbb{Z}_p^*$, ktorý túto grupu generuje, a teda má rád $p-1$. Zrejme $\omega = a^{\frac{p-1}{n}}$ je prvok rádu n, pretože $\omega^i = a^{i\frac{p-1}{n}} \neq 1$ pre každé $i < n$ a pritom $\omega^n = a^{p-1} = 1$ v $\mathbb{Z}_p$. □

Ako ale také a v $\mathbb{Z}_p$ nájsť? Vieme, že grupa $\mathbb{Z}_p^*$ obsahuje $\varphi(p-1)$ generátorov, kde φ značí Eulerovu funkciu. Ich hustota je teda relatívne veľká a existuje odhad (dokazovaný obvykle v teórií čísel)

$$\frac{\varphi(p-1)}{p} \sim \frac{3}{\pi^2} \doteq 0,3.$$

Nejefektívnejšia metóda je teda náhodna voľba a následne overenie, či skutočne rád náhodne zvoleného prvku je $p-1$. Spomenutý odhad Hovorí, že se trafíme do generátoru v priemere v každom treťom prípade.

Poznamenejme, že nás vlastne zaujímajú primitívne n-té odmocniny z jednej pre n rovno mocnine dvojky. Zaujímavé sú telesa $\mathbb{Z}_p$, kde $2^k \mid p-1$ pre veľmi veľké k (napr. 17, 41, atď.)

Záverom okomentujeme nepríjemnú námietku, ktorá vás už možno napadla: čo ak v našom obľúbenom telese $\mathbf{T}$ (ako napríklad v racionálnych čislach) žiadne primitívne n-té odmocniny z jednej nie sú? Potom v $\mathbf{T}$ nemôžeme robiť Rýchlu Fourierovú transormáciu. Nikto nám však nebráni si príslušnú odmocninu k $\mathbf{T}$ adjungovať a pracovať v algebraickom rozšíreni $\mathbf{T}(\omega)$. Ako $\mathbf{T}(\omega)$ si samozrejme zvolíme vhodné koreňové nadteleso polynómu $x^n - 1$. V prípade racionálnych čísel je prirodzenou voľbou $\mathbb{Q}(e^{\frac{2\pi i}{n}})$.

2. Rýchle násobenie polynómov

Princípom rýchleho algoritmu na násobenie a delenie polynómov je nasledujúcie pozorovanie: ak je

$$(c_0, \ldots, c_n)$$

modulárna reprezentácia polynómu p a

$$(d_0, \ldots, d_n)$$

modulárna reprezentácia polynómu q vzhľadom k daným bodom $\alpha_0, \ldots, \alpha_n$, a ak je naviac $n \geq \deg(p) + \deg(q)$, potom modulárna reprezentácia polynómu $p \cdot q$ vzhľadom k týmto bodom je

$$(c_0 d_0, \ldots, c_n d_n),$$

pretože $(p \cdot q)(\alpha_i) = p(\alpha_i) \cdot q(\alpha_i)$ pre ľubovoľný bod α_i. Analogicky, ak $q \mid p$, potom $\frac{p}{q}$ má modulárnu reprezentáciu

$$(\frac{c_0}{d_0}, \ldots, \frac{c_n}{d_n}).$$

Pritom k výpočtu súčinu a podielu v takejto modulárnej reprezentácii stačí $n+1$ operacií (násobení, resp. delení) v telese $\mathbf{T}$. Vzhľadem k tomu, že užívateľ obvykle vyžaduje vstup aj výstup v štandardnej reprezentácii, zložitost násobenia a delenia závisí na algoritmu pre prevod do vhodne zvolenej modulárnej bázi.

Algoritmus 2.1 (Rýchle násobenie).

`VSTUP:` $p = \sum_{i=0}^{n} a_i x^i, q = \sum_{i=0}^{m} b_i x^i \in \mathbf{T}[x]$.

`VÝSTUP:` $p \cdot q = \sum_{i=0}^{m+n} f_i x^i$.

`1.` Zvoľ $N = 2^k > m + n$ a nejakú primitívnu n-tú odmocninu z jednej ω v $\mathbf{T}$.

`2.` $\bar{c} := \mathrm{FFT}(\omega)(a_0, \ldots, a_n, 0, \ldots, 0)$,
$\bar{d} := \mathrm{FFT}(\omega)(b_0, \ldots, b_m, 0, \ldots, 0)$.

`3.` $\bar{e} := \bar{c} \cdot \bar{d} = (c_0 \cdot d_0, \ldots, c_{N-1} \cdot d_{N-1})$.

`4.` $\bar{f} := \frac{1}{N} \mathrm{FFT}(\omega^{-1})(e_0, \ldots, e_{N-1})$.

`5.` `RETURN` $\sum_{i=0}^{N-1} f_i x^i$.

Tvrdenie 2.2. *Predpokladajme, že ω je daná. Časová zložitosť Algoritmu 2.1 je $\mathcal{O}(n \log n)$, kde n je väčší zo stupňov p, q.*

Proof. Rozoberieme zložitosť jednotlivých krokov: `1.` je triviálny. Krok `2.` má zložitosť $2\mathcal{O}(N \log N)$. Krok `3.` má zložitosť N. Krok `4.` má zložitosť $\mathcal{O}(N \log N)$. A krok `5.` je triviálny. Pretože $N \leq 4n$, máme celkovú časovú zložitosť algoritmu $\mathcal{O}(N \log N) = \mathcal{O}(n \log n)$. □

Poznámka. Zložitosť hľadania primitívnej odmocniny z jednej sme nepočítali, pretože toto záleží na telese $\mathbf{T}$. Napríklad v prípade $\mathbb{Q}$ nemusíme nič hľadať, stačí položiť $\omega = e^{\frac{2\pi i}{N}}$ a $\omega^{-1} = e^{-\frac{2\pi i}{N}}$ a počítať v telese $\mathbb{Q}(\omega)$. V prípade $\mathbb{Z}_p$ môžeme hľadať pravdepodobnostným algoritmom popísaným v predošlej sekcii. Ak v $\mathbb{Z}_p$ žiadna primitívna N-tá odmocnina z jednej neexistuje, pracujeme v príslušnom rozšírení.

Príklad. Spočítajme súčin $(3x^3 + x^2 - 4x + 1) \cdot (x^3 + 2x^2 + 5x - 3)$ v $\mathbb{Z}_{41}$.

(1) zvoľme $N = 2^3 = 8 > 3 + 3$ a $\omega = 14$.
(2) $\bar{c} = \mathrm{FFT}(14)(1, -4, 1, 3, 0, 0, 0, 0) = (1, 9, -19, -18, 3, 16, 19, -3)$,
$\bar{d} = \mathrm{FFT}(14)(-3, 5, 2, 1, 0, 0, 0, 0) = (5, 5, 0, 14, -7, -6, -10, 16)$.
(3) $\bar{e} = (5, 4, 0, -6, 20, -14, 15, -7)$.
(4) Platí $\omega^{-1} = 3$ a $\frac{1}{N} = \frac{1}{8} = -5$. Tedy
$\bar{f} = -5 \cdot \mathrm{FFT}(3)(5, 4, 0, -6, 20, -14, 15, -7) = (-3, 17, 20, -11, 13, 7, 3, 0)$.
(5) Súčin je $-3 + 17x + 20x^2 - 11x^3 + 13x^4 + 7x^5 + 3x^6$

Poznámka. Algoritmus na rýchle delenie funguje analogicky. V kroku `1.` stačí $N = 2^k > n$ a v kroku `3.` počítame $\bar{e} = (\frac{c_0}{d_0}, \ldots, \frac{c_{N-1}}{d_{N-1}})$. Aj v tomto prípade bude časová zložitosť $\mathcal{O}(n \log n)$.