Oblikovanje i analiza algoritama

Matej Mihelčić

Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu

matmih@math.hr

28. prosinca, 2023.

Umnožak polinoma

- Neka su:
  - $A(x) = \sum_{j=0}^{n-1} a_j x^j$
  - $B(x) = \sum_{j=0}^{n-1} b_j x^j$
- Umnožak:
  - $C(x) = A(x) \cdot B(x) = \sum_{j=0}^{2n-2} c_j x^j, \ c_k = \sum_{i=0}^{k} a_i b_{k-i}$
- Složenost:
  - $\mathcal{O}(n^2)$ $(\Theta(n^2))$
- Asimptotski brži način:
  - $A(x) = A_0(x) + A_1(x)x^{\lfloor \frac{n}{2} \rfloor}, \ B(x) = B_0(x) + B_1(x)x^{\lfloor \frac{n}{2} \rfloor}$
  - $\Theta(n^{log_2 3})$

Brza Fourierova transformacija

- Brza (diskretna) Fourierova transformacija (*FFT* - Fast Fourier Transform) je iznimno važan i korišten algoritam.
- Na njemu su bazirani mnogi brzi algoritmi u aritmetici i algebri.
- Osnovna primjena FFT-a (u kolegiju) će biti brzi algoritam za množenje kompleksnih polinoma.
- Neka je A bilo koji kompleksni polinom, stupnja najviše $n-1$, gdje je $n \in \mathbb{N}$. Taj polinom možemo zapisati u obliku $A(z) = \sum_{j=0}^{n-1} a_j z^j$, gdje:
  - $a_0, a_1, \ldots, a_{n-1} \in \mathbb{C}$ koeficijenti tog polinoma u standardnoj bazi vektorskog prostora svih polinoma stupnja najviše $n-1$ nad poljem kompleksnih brojeva.
- Dimenzija tog vektorskog prostora je točno n, pa zato kažemo da je A polinom reda n. Time izbjegavamo eksplicitno navođenje stupnja (koji može biti i manji od $n-1$).
- Prirodni izomorfizam ovog vektorskog prostora i prostora $\mathbb{C}^n$ pokazuje da je polinom A jednoznačno određen vektorom koeficijenata $\vec{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{C}^n$.

Problemi evaluacije i interpolacije

- Neka su $z_0, z_1, \ldots, z_{n-1}$ međusobno različite kompleksne točke.
- Uz oznaku $y_k = A(z_k),\ k = 0, \ldots, n-1$, polinomu A (odnosno vektoru koeficijenata $\vec{a}$, pridružili smo vektor $\vec{y} = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{C}^n$ (isti n-dimenzionalni $\mathbb{C}^n$), koji sadrži vrijednost zadanog polinoma u zadanim točkama.
- Polinom A je jednoznačno određen vektorom $\vec{y}$.
- Množenje polinoma: $C(x) = A(x) \cdot B(x)$

  Ulaz: koeficijenti polinoma A i B stupnja $n-1$
  Izlaz: koeficijenti polinoma C
- **Selekcija**
  - Odaberi međusobno različite kompleksne točke $z_0, z_1, \ldots, z_{m-1},\ m \geq 2n-1$
- **Evaluacija**
  - Izračunaj $A(z_k)$ i $B(z_k), k = 0, \ldots, m-1$
- **Množenje**
  - Izračunaj $A(z_k) \cdot B(z_k), k = 0, \ldots, m-1$

Problemi evaluacije i interpolacije

- **Interpolacija**
  - $C(x) = c_0 + c_1 x + \cdots + c_{2n-2} x^{2n-2}$
- Pridruživanje $\vec{a} \mapsto \vec{y}$ jednoznačno je određeno izborom točaka $z_0, z_1, \ldots, z_{n-1}$.
- Matrični prikaz:

$$y_k = A(z_k) = \sum_{i=0}^{n-1} a_i z_k^i, \;\; k = 0, \ldots, n-1$$

- Svaki y_k je linearna kombinacija koeficijenata a_i, što možemo matrično zapisati u obliku:

$$\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix} = V_n(z_0, z_1, \ldots, z_{n-1}) \cdot \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$$

Problem evaluacije

- $V_n(z_0, z_1, \ldots, z_{n-1})$ je Vandermondeova matrica izabranog vektora točaka $z_0, z_1, \ldots, z_{n-1}$:
$$\begin{bmatrix} z_0^0 & z_0^1 & \cdots & z_0^{n-1} \\ z_1^0 & z_1^1 & \cdots & z_1^{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ z_{n-1}^0 & z_{n-1}^1 & \cdots & z_{n-1}^{n-1} \end{bmatrix}$$
- Prvi problem – problem evaluacije (izračunavanja):
  - za zadani vektor $\vec{a}$ treba izračunati pripadni $\vec{y}$.
- Točke smatramo fiksnima.
- Problem se svodi na množenje matrice i vektora:
$$\vec{y} = V_n(z_0, z_1, \ldots, z_{n-1}) \cdot \vec{a}$$
- Standardni algoritam množenja ima složenost $\Theta(n^2)$.
- Alternativni algoritam: Hornerova shema za svaku od n točaka (identična složenost).
- Uočite da optimalnost Hornerove sheme za jednu točku ne povlači optimalnost primjene istog algoritma n puta za n točaka.

Problem interpolacije

- Drugi problem je problem interpolacije:
  - za zadani vektor $\vec{y}$ vrijednosti polinoma u zadanim točkama, treba pronaći vektor $\vec{a}$ koeficijenata tog polinoma.
  - treba pronaći polinom A koji u zadanim točkama ima zadane vrijednosti, pa je prirodno ovaj problem zvati problemom interpolacije.
- Drugi problem je obrat ili inverz prvoga.
- Matrično-vektorski gledano, treba riješiti linearni sustav:

$$\vec{y} = V_n(z_0, z_1, \ldots, z_{n-1}) \cdot \vec{a}$$

- Promotrimo kada ovaj sustav ima jedinstveno rješenje (ima ga smisla računati). Matrica sustava je Vandermondeova, pa je pripadna determinanta Vandermondeova, a za nju vrijedi:

$$det(V_n(z_0, z_1, \ldots, z_{n-1})) = \prod_{0 \leq l < k \leq n-1} (z_k - z_l)$$

Problem interpolacije

- Pretpostavka o različitosti izabranih točaka je nužan i dovoljan uvjet da matrica sustava bude regularna, tj. da sustav ima jedinstveno rješenje.
- Kolika je složenost računanja rješenja ovog linearnog sustava?
- Sasvim općenito, možemo koristiti Gaussove eliminacije (ili LU faktorizaciju), kao da je matrica sustava bilo koja regularna matrica. Taj postupak ima složenost $\Theta(n^3)$ kompleksnih aritmetičkih operacija, tj. kubnu u n, što je bitno sporije od prvog problema.
- Međutim, naš sustav ima matricu vrlo specijalne strukture (Vandermondeovu), pa očekujemo da se rješenje može naći i brže. Moguće je konstruirati algoritme koji imaju kvadratnu složenost u n (kao i za prvi problem).

Korijeni jedinice

- Neka je n prirodan broj. Osnovni ili glavni n-ti korijen iz jedinice je kompleksni broj

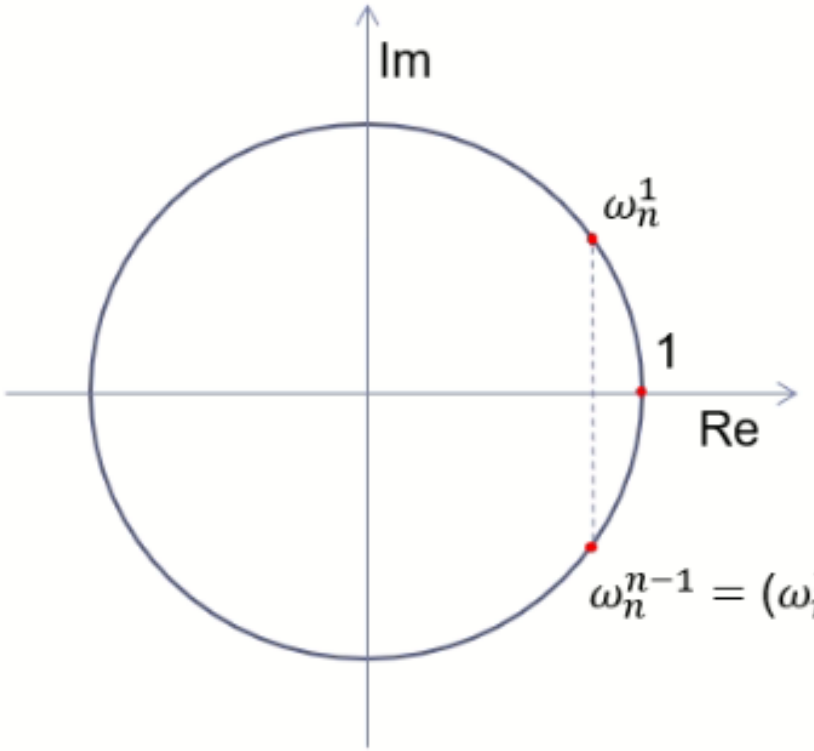
$$\omega_n = e^{2\pi i/n} = cos\frac{2\pi}{n} + i \cdot sin\frac{2\pi}{n}$$

- Svi n-ti korijeni iz jedinice su točke

$$\omega_n^k = e^{2k\pi i/n} = cos\frac{2k\pi}{n} + i \cdot sin\frac{2k\pi}{n}, k = 0, \ldots, n-1$$

- Te točke čine grupu obzirom na množenje kompleksnih brojeva. Navedena grupa je izomorfna aditivnoj grupi $(\mathbb{Z}_n, +_n)$ ostataka modulo n.
- Točke su raspoređene u vrhovima pravilnog n-terokuta na jediničnoj kružnici u kompleksnoj ravnini, s tim da je jedan od vrhova smješten na realnoj osi u točki 1.

Korijeni jedinice

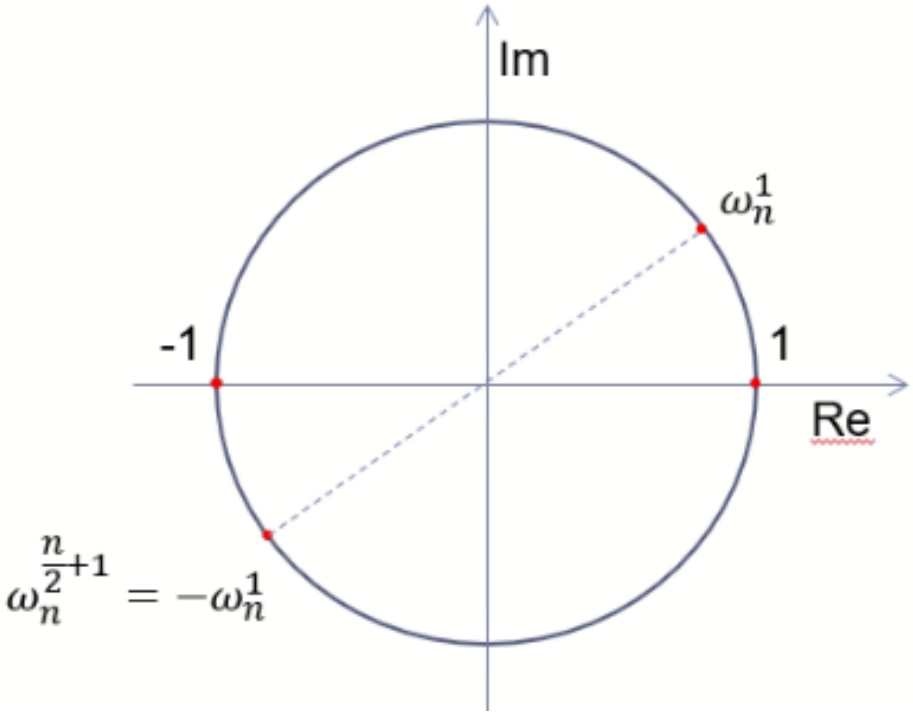


$$\begin{bmatrix} 1 & 1 & 1 & & 1 \\ 1 & \omega_n & \omega_n^2 & \cdots & \omega_n^{n-1} \\ 1 & \omega_n^2 & \omega_n^4 & & \omega_n^{2(n-1)} \\ & \vdots & & \ddots & \vdots \\ 1 & \omega_n^{(n-1)} & \omega_n^{2(n-1)} & \cdots & \omega_n^{(n-1)(n-1)} \end{bmatrix}$$

- **Zadatak**: Dokažite da su stupci matrice $V_n(\omega_n^0, \omega_n^1, \ldots, \omega_n^{n-1})$ ortogonalni (uz standardni kompleksni skalarni umnožak).
- $1 + \omega_n^{j-k} + \omega_n^{2(j-k)} + \cdots + \omega_n^{(n-1)(j-k)} = (1 - \omega_n^{n(j-k)})/(1 - \omega_n^{j-k})$

Korijeni jedinice

- Neka je n paran prirodan broj:



$$V_n := V_n(\omega_n^0, \omega_n^1, \ldots, \omega_n^{n-1})$$
$$V_n V_n^* = nI,\ V_n^{-1} = (1/n)V_n^*$$
$$V_n^* = V_n(\omega_n^0, \omega_n^{-1}, \ldots, \omega_n^{-(n-1)})$$

- **Lema** (Lema kraćenja): Za bilo koje prirodne brojeve $n, d \in \mathbb{N}$ i $k = 0, \ldots, n-1$ vrijedi $\omega_{dn}^{dk} = \omega_n^k$.

Korijeni jedinice

- **Lema** (Lema "raspolavljanja") Ako je n paran prirodan broj, onda su kvadrati svih n-tih korijena iz jedinice upravo svi $n/2$-ti korijeni iz jedinice. Preciznije, vrijedi:

$$((\omega_n^0)^2, (\omega_n^1)^2, \ldots, (\omega_n^{n-1})^2) = (\omega_{\frac{n}{2}}^0, \omega_{\frac{n}{2}}^1, \ldots, \omega_{\frac{n}{2}}^{\frac{n}{2}-1}, \omega_{\frac{n}{2}}^0, \omega_{\frac{n}{2}}^1, \ldots, \omega_{\frac{n}{2}}^{\frac{n}{2}-1})$$

  tj. vektor kvadrata n-tih korijena iz jedinice sadrži točno 2 kopije vektora $n/2$-tih korijena iz jedinice (jednu za drugom).
- **Dokaz**: $(\omega_n^j)^2 = e^{2(2\pi ij/n)} = e^{2\pi ij/(n/2)} = \omega_{\frac{n}{2}}^j$
- $(\omega_n^j)^2 = \omega_n^{2j}\omega_n^n = \omega_n^{2j+n} = (\omega_n^{j+n/2})^2$.