Separacija korijena polinoma

Andrej Dujella

Matematički odsjek Prirodoslovno-matematički fakultet Sveučilište u Zagrebu e-mail: duje@math.hr

URL: https://web.math.pmf.unizg.hr/~duje/

Zajednički rad s Yannom Bugeaudom, Tomislavom Pejkovićem i Brunom Salvyjem

Istraživanje podržano od Znanstvenog centra izvrsnosti QuantiXLie Pitanje: Koliko bliska mogu biti dva različita korijena polinoma P(X) stupnja d s cjelobrojnim koeficijentima?

Usporedit ćemo udaljenost između dva različita korijena od P(X) s njegovom visinom H(P), definiranom kao maksimum apsolutnih vrijednosti njegovih koeficijenata.

Razmotrit ćemo također i apsolutnu varijantu ovog problema, gdje se pitamo za minimalnu ne-nul udaljenost između apsolutnih vrijednosti korijena.

Napomena: Vrijeme izvršavanja algoritama za izoliranje korijena polinoma P ovisi o minimalnoj udaljenosti između njegovih korijena.

Kompleksnost različitih algoritama za linearne rekurzije ovisi o udaljenosti između apsolutnih vrijednosti dva dominantna korijena (korijena s najvećom apsolutnom vrijednošću).

Primjer 1: Polinom $14x^3+17x^2-13x+2$ ima korijene $\alpha_1\approx 0.2807764064$, $\alpha_2\approx 0.2857142857$, $\alpha_3\approx -1.780776406$, i vrijedi

$$|\alpha_1 - \alpha_2| \approx 0.0049378793.$$

Primjer 2: Polinom $17x^3-9x^2-7x+8$ ima korijene $\beta_1 \approx -0.7778140159$, $\beta_2 \approx 0.6536128903 + 0.4216681370 i$, $\beta_3 \approx 0.6536128903 - 0.4216681370 i$, i vrijedi

$$||\beta_1| - |\beta_2|| \approx 0.0000123324.$$

Mahler (1964): $|\alpha - \beta| \gg H(P)^{-d+1}$

za svaka dva različita korijena α i β cjelobrojnog polinoma P(X) stupnja d (konstanta implicitno sadržana u oznaci \gg je eksplicitna konstanta koja ovisi samo o stupnju d).

Za polinom P(x) s cjelobrojnim koeficijentima stupnja $d \geq 2$ s različitim korijenima $\alpha_1, \ldots, \alpha_d$, stavimo

$$sep(P) = \min_{1 \le i < j \le d} |\alpha_i - \alpha_j|$$

i definiramo e(P) sa $sep(P) = H(P)^{-e(P)}$. Za $d \ge 2$, definiramo

$$e(d) := \limsup_{\deg(P)=d, H(P) \to +\infty} e(P).$$

Analogno definiramo $e_{irr}(d)$ tako da limsup uzmemo po svim ireducibilnim cjelobrojnim polinomima P(x) stupnja d.

Nadalje definiramo $e^*(d)$ i $e^*_{irr}(d)$ tako da se restringiramo na normirane, odnosno normirane ireducibilne cjelobrojne polinome stupnja d.

Očito je:

$$e(d) \ge e_{\mathsf{irr}}(d), \quad e^*(d) \ge e^*_{\mathsf{irr}}(d).$$

Mahler (1964): $e(d) \le d - 1$ za sve d

$$\begin{aligned} d &= 2 \\ P(X) &= aX^2 + bX + c, \\ \Delta &= b^2 - 4ac, \ \text{sep}(P) = \sqrt{|\Delta|}/a \\ e_{\text{irr}}(2) &= e(2) = 1, \ e_{\text{irr}}^*(2) = e^*(2) = 0 \\ \text{Npr. } a &= k^2 + k - 1, \ b = 2k + 1, \ c = 1, \ \Delta = 5 \end{aligned}$$

$$d = 3$$

Evertse (2004), **Schönhage** (2006):

$$e_{irr}(3) = e(3) = 2$$

Bugeaud & Mignotte (2010):

$$e_{\rm irr}^*(3) = e^*(3) \ge 3/2$$

(ovdje je jednakost ekvivalentna Hallovoj slutnji:

za svaki $\varepsilon>0$ postoji konstanta $c(\varepsilon)$ tako da za sve prirodne brojeve x,y takve da je $x^3\neq y^2$ vrijedi da je $|x^3-y^2|>c(\varepsilon)x^{1/2-\varepsilon}$, a ona je posljedica abc-slutnje)

$$d = 4$$

Bugeaud & D. (2011):

$$e_{irr}(4) \ge 13/6$$

Bugeaud & D. (2014):

$$e(4) \ge 7/3$$

Bugeaud & D. (2014):

$$e_{\rm irr}^*(4) \ge 7/4$$

Bugeaud & Mignotte (2010):

$$e^*(4) \ge 2$$

D. & Pejković (2011):

eksplicitna familija s eksponentom 2:

$$P_n(x) = (x^2 + x - 1)(x^2 + (1 + F_{n+1})x - (F_n + 1))$$

Ne postoji takva familija s koeficijentima koji rastu polinomijalno u odnosu na n, ali je moguće naći takve familije s eksponentima proizvoljno blizu 2.

 $\lim\sup e(P)=2$, gdje limsup uzimamo po svim reducibilnim normiranim cjelobrojnim polinomima P(x) stupnja 4, tj.

$$e_{\text{red}}^*(4) = 2.$$

p-adska verzija

$$sep(P)_p = \min_{1 \le i < j \le d} |\alpha_i - \alpha_j|_p,$$

Pejković (2016):

- kvadratni polinomi: $\operatorname{sep}_p(P_k) \asymp H(P_k)^{-1}$ (najbolje moguće)
- reducibilni kubni polinomi: ${\rm sep}_p(P_k) \asymp H(P_k)^{-2}$ (najbolje moguće)
- ireducibilni kubni polinomi: ${\rm sep}_p(P_k) \asymp H(P_k)^{-25/14}$

Bugeaud & Mignotte (2004,2010):

$$e(d) \ge e_{irr}(d) \ge d/2$$
, za parne $d \ge 4$,

$$e(d) \ge (d+1)/2$$
, za neparne $d \ge 5$,

$$e_{irr}(d) \ge (d+2)/4$$
, za neparne $d \ge 5$,

Beresnevich, Bernik & Götze (2010):

$$e_{irr}(d) \ge (d+1)/3$$
, za sve $d \ge 2$.

Bugeaud & Mignotte (2010):

 $e^*(d) \geq d/2$, za parne $d \geq 4$, $e^*(d) \geq (d-1)/2$, za neparne $d \geq 5$, $e^*_{\mathsf{irr}}(d) \geq (d-1)/2$, za parne $d \geq 4$, $e^*_{\mathsf{irr}}(d) \geq (d+2)/4$, za neparne $d \geq 5$,

Beresnevich, Bernik, & Götze (2010):

$$e_{\mathsf{irr}}^*(d) \geq d/3$$
, za sve $d \geq 3$.

Bugeaud & D. (2011):

$$e_{\mathsf{irr}}(d) \ge \frac{d}{2} + \frac{d-2}{4(d-1)}$$
 za sve $d \ge 4$.

Ovaj rezultat je poboljšao sve prethodno poznate donje ograde za $e_{irr}(d)$ kada je $d \ge 4$.

Neka je d=4. Za $a\geq 1$, korijeni polinoma

 $T_{4,a}(x) = (20a^4 - 2)x^4 + (16a^5 + 4a)x^3 + (16a^6 + 4a^2)x^2 + 8a^3x + 1,$ su približno jednaki:

$$r_1 = -1/4a^{-3} - 1/32a^{-7} - 1/256a^{-13} + \dots,$$

$$r_2 = -1/4a^{-3} - 1/32a^{-7} + 1/256a^{-13} + \dots,$$

$$r_3 = -2/5a + 11/100a^{-3} + 69/4000a^{-7} + 4/5ai + \dots,$$

$$r_4 = -2/5a + 11/100a^{-3} + 69/4000a^{-7} - 4/5ai + \dots$$

 $H(T_{4,a}) \approx a^6$, $sep(T_{4,a}) = |r_1 - r_2| \approx a^{-13}$, pa ako pustimo $a \to \infty$ dobivamo da je $e_{irr}(4) \ge 13/6$.

Za $i \geq 0$, s c_i označimo i-ti Catalanov broj definiran s

$$c_i = \frac{1}{i+1} {2i \choose i}.$$

Početni dio niza Catalanovih brojeva $(c_i)_{i>0}$ izgleda ovako:

$$1, 1, 2, 5, 14, 42, 132, 429, 1430, \ldots$$

Niz zadovoljava rekurziju

$$c_{i+1} = \sum_{k=0}^{i} c_k c_{i-k}, \quad \text{za } i \ge 0.$$

Za prirodne brojeve $d \geq 3$ i $a \geq 1$, promotrimo polinom

$$T_{d,a}(x) = (2c_0ax^{d-1} + 2c_1a^2x^{d-2} + \dots + 2c_{d-2}a^{d-1}x)^2 - (4c_1a^2x^{2d-2} + 4c_2a^3x^{2d-3} + \dots + 4c_{d-2}a^{d-1}x^{d+1}) + (4c_1a^2x^{d-2} + 4c_2a^3x^{d-3} + \dots + 4c_{d-2}a^{d-1}x) + 4ax^{d-1} - 2x^d + 1,$$

koji predstavlja poopćenje polinoma $T_{4,a}(x)$.

Iz rekurzije slijedi da $T_{d,a}(x)$ ima stupanj točno d, a ne 2d-2, kako bi moglo izgledati na prvi pogled. Nadalje, visina od $T_{d,a}(x)$ je dana s koeficijentom uz x^2 , tj.

$$H(T_{d,a}) = 4c_{d-2}^2a^{2d-2} + 4c_{d-3}a^{d-2}.$$

Primjenom Eisensteinovog kriterija za prosti broj 2 na recipročni polinom $x^dT_{d,a}(1/x)$, zaključujemo da je polinom $T_{d,a}(x)$ ireducibilan. Zaista, svi koeficijenti od $T_{d,a}(x)$ osim slobodnog člana su parni, ali njegov vodeći koeficijent, koji je jednak $4c_{d-1}a^d-2$, nije djeljiv sa 4.

Bugeaud & D. (2014):

$$e(d) \ge \frac{2d}{3} - \frac{1}{3}$$
 za sve $d \ge 4$.

Ovo je prvi rezultat oblika $e(d) \ge C \cdot d$ uz $C > \frac{1}{2}$.

Bugeaud & D. (2014):

$$e^*(d) \ge \frac{2d}{3} - 1$$
 za parne $d \ge 6$

$$e^*(d) \ge \frac{2d}{3} - \frac{5}{3}$$
 za neparne $d \ge 7$

Bugeaud & D. (2014):

$$e_{\mathsf{irr}}^*(d) \geq \frac{d}{2} - \frac{1}{4}$$
 za sve $d \geq 4$.

Teorem 1:
$$e(d) \ge \frac{2d}{3} - \frac{1}{3}$$
 za sve $d \ge 4$.

Želimo konstruirati jednoparametarski niz cjelobrojnih polinoma $p_{d,n}(x)$ stupnja d koji imaju jedan korijen vrlo blizu racionalnog broja $x_n=(n+2)/(n^2+3n+1)$. Tada će polinomi

$$P_{d,n}(x) = ((n^2 + 3n + 1)x - (n + 2))p_{d-1,n}(x)$$

imati dva bliska korijena. Definiramo niz $p_{d,n}(x)$ rekurzivno s

$$p_{0,n}(x) = -1, \quad p_{1,n}(x) = (n+1)x - 1,$$

$$p_{d,n}(x) = (1+x)p_{d-1,n}(x) + x^2p_{d-2,n}(x).$$

Tada vrijedi

$$p_{d,n}\left(\frac{n+2}{n^2+3n+1}\right) = \frac{(-1)^{d-1}}{(n^2+3n+1)^d}.$$

Pomoću ovoga možemo dokazati da za dovoljno veliki n polinom $p_{d,n}(x)$ ima korijen između x_n i

$$z_{d,n} = x_n + \frac{(-1)^d}{n(n^2 + 3n + 1)^d}.$$

Stoga polinom $P_{d,n}(x)$ ima dva bliska korijena: x_n i $y_{d,n}$, koji je između x_n i $z_{d-1,n}$. Zaključujemo da je

$$sep(P_{d,n}) \le |x_n - y_{d,n}| \le \frac{1}{n(n^2 + 3n + 1)^{d-1}} \le \frac{1}{n^{2d-1}},$$

za dovoljno veliki n. Budući da je visina od $P_{d,n}(x)$ omeđena odozgo s n^3 (pomnoženo s brojem koji ovisi samo o d), pustivši $n\to\infty$, dobivamo

$$e(d) \geq \frac{2d-1}{3}.$$

Teorem 2:
$$e^*(d) \ge \frac{2d}{3} - 1$$
 za parne $d \ge 6$,
$$e^*(d) \ge \frac{2d}{3} - \frac{5}{3}$$
 za neparne $d \ge 7$.

Da bi dobili familiju normiranih polinoma sa sličnim separacijskim svojstvima poput familije $P_{d,n}(x)$, zamijenit ćemo linearni ne-normirani polinom $L_n(x) = (n^2 + 3n + 1)x - (n+2)$ s kvadratnim normiranim polinomom

$$K_n(x) = x^2 - (n^2 + 3n + 1)x + (n + 2).$$

Želimo konstruirati niz cjelobrojnih polinoma $q_{d,n}(x)$ stupnja d koji imaju jedan korijen vrlo blizu korijenu $y_n = 1/n + O(1/n^2)$ od $K_n(x)$. Tada će polinom

$$Q_{d,n}(x) = (x^2 - (n^2 + 3n + 1)x + (n + 2))q_{d-2,n}(x)$$
imati dva vrlo bliska korijena.

Za parni $d \ge 0$, definiramo rekurzivno niz $q_{d,n}(x)$:

$$q_{0,n}(x) = 1$$
, $q_{2,n}(x) = x^2 - (n+1)x + 1$,

$$q_{d,n}(x) = (2x^2 + x + 1)q_{d-2,n}(x) - x^4q_{d-4,n}(x).$$

Tada je $q_{d,n}(x)-q_{d-2,n}(x)q_{2,n}(x)$ djeljivo s $K_n(x)$, što povlači da je

$$q_{d,n}(y_n) = q_{d-2,n}(y_n)q_{2,n}(y_n) = (q_{2,n}(y_n))^{d/2},$$

za parni $d \geq 2$. Iz

$$y_n=1/n-1/n^2+2/n^3-4/n^4+8/n^5+O(1/n^6),$$
dobivamo $q_{2,n}(y_n)=1/n^4+O(1/n^5)$ pa je
$$q_{d,n}(y_n)=1/n^{2d}+O(1/n^{2d+1}).$$

Može se pokazati da za dovoljno veliki n polinom $q_{d,n}(x)$ ima korijen između y_n i $w_{d,n}=y_n+\frac{2}{n^{2d+1}}$. Stoga polinom $Q_{d,n}(x)$ ima dva bliska korijena: y_n i $v_{d,n}$, koji je između y_n i $w_{d-2,n}$. Tako dobivamo

$$\operatorname{sep}(Q_{d,n}) \le \frac{2}{n^{2d-3}},$$

pa budući da je $H(Q_{d,n}) \asymp n^3$, puštajući $n \to \infty$ zaključujemo da je

$$e^*(d) \ge \frac{2d-3}{3}.$$

Neka je sada d neparan. Tada definiramo

$$Q_{d,n}(x) = x(x^2 - (n^2 + 3n + 1)x + (n + 2))q_{d-3,n}(x).$$

Ovaj polinom ima dva bliska korijena: y_n i korijen koji leži između y_n i $w_{d-3,n}$. Tako dobivamo da je

$$\operatorname{sep}(Q_{d,n}) \le \frac{2}{n^{2d-5}},$$

za dovoljno veliki n, pa je

$$e^*(d) \ge \frac{2d-5}{3}.$$

D. & Pejković (2017):

$$7/3 \le e^*(5) \le 3$$
, $17/5 \le e^*(7) \le 5$, $31/7 \le e^*(9) \le 7$

$$T_{5,n} = (x^2 + n^2x - n)(x^3 + nx - 1)$$

bliski korijeni: $1/n - 1/n^4 + (2,3)/n^7 + \cdots$

$$T_{7,n} = (x^2 + n^3x - n)(x^5 + nx^3 + n^2x - 1)$$

korijeni: $1/n^2 - 1/n^7 + 2/n^{12} + (-4, -5)/n^{17} + \cdots$

$$T_{9,n} = (x^2 + n^4x - n)(x^7 + nx^5 + n^2x^3 + n^3x - 1)$$

korijeni: $1/n^3 - 1/n^{10} + 2/n^{17} - 5/n^{24} + (14, 15)/n^{31} + \cdots$

Može se poopćiti na $(d^2-2d-1)/(2d-4) \le e^*(d) \le d-2$; ova donja ograda je asimptotski slabija od one iz Teorema 2.

Teorem 3:
$$e_{\text{irr}}^*(d) \ge \frac{d}{2} - \frac{1}{4}$$
 za sve $d \ge 4$.

Iskoristit ćemo polinome $p_{d,n}(x)$ za konstrukciju *ireducibilnih normiranih* polinoma s dva bliska korijena.

S F_k ćemo označiti k-ti Fibonaccijev broj. Fibonaccijevi brojevi se pojavljuju u asimptotskom razvoju od $x_n = (n+2)/(n^2+3n+1)$, jer vrijedi

$$x_n = 1/n - 1/n^2 + 2/n^3 - 5/n^4 + \dots - (-1)^k F_{2k-3}/n^k + \dots$$

Za $d \ge 0$, najprije definiramo normirane polinome $s_{d,n}(x)$ s korijenom bliskim x_n :

$$s_{d,n}(x) = (-1)^{d-1} (F_{d-1}p_{d,n}(x) - F_d x p_{d-1,n}(x)),$$

a zatim normirane polinome s dva bliska korijena:

$$r_{2d+1,n}(x) = xs_{d,n}^2(x) + F_d^2 p_{d,n}^2(x),$$

$$r_{2d,n}(x) = s_{d,n}^2(x) + F_{d-1}^2 x p_{d-1,n}^2(x).$$

Tvrdimo da su svi polinomi normirani. Dovoljno je to dokazati za $s_{d,n}(x)$. Budući da je vodeći koeficijent od $p_{d,n}(x)$ jednak $F_{d}n+F_{d-2}$, dobivamo da je vodeći koeficijent od $s_{d,n}(x)$ jednak

$$(-1)^{d-1}(F_{d-1}(F_{dn} + F_{d-2}) - F_d(F_{d-1}n + F_{d-3}))$$

$$= (-1)^{d-1}(F_{d-1}F_{d-2} - F_dF_{d-3}) = 1.$$

Vrijedi

$$r_{d,n}(x_n) = F_{\lfloor (d-1)/2 \rfloor}^2 / n^{2d-3} + O(1/n^{2d-2}).$$

Uočimo da je stupanj polinoma $r_{d,n}(x)$ jednak d dok je $H(r_{d,n}) \asymp n^2$.

Može se pokazati da $r_{d,n}(x)$ ima dva kompleksno konjugirana korijena $v_{d,n}$ i $\overline{v_{d,n}}$ bliska x_n . Ti korijeni su

$$1/n - 1/n^2 + 2/n^3 - 5/n^4 + 13/n^5 - \dots + (-1)^d F_{2d-5}/n^{d-1} \pm i/n^{(2d-1)/2} + O(1/n^d).$$

Može se pokazati da je za dovoljno velike prirodne brojeve n polinom $r_{d,n}(x)$ ireducibilan nad \mathbb{Z} . Dokaz koristi ocjene za rezultantu polinoma $R_{d,n}(x)$ i $L_n(x)$, gdje $R_{d,n}(x)$ označava ireducibilni faktor od $r_{d,n}(x)$ koji ima korijene $v_{d,n}$ i $\overline{v_{d,n}}$. Iz tih ocjena slijedi da je stupanj od $R_{d,n}(x)$ jednak ili d ili d-1, a zadnja mogućnost se može isključiti za dovoljno velike n.

Budući da je

$$sep(r_{d,n}) \simeq n^{-(d-1/2)},$$

dobivamo

$$e_{\mathsf{irr}}^*(d) \geq \frac{2d-1}{4}.$$

Apsolutna varijanta problema: minimalna udaljenost (različita od 0) između apsolutnih vrijednosti korijena:

$$abs \operatorname{sep}(P) := \min_{\substack{P(\alpha) = P(\beta) = 0, \\ |\alpha| \neq |\beta|}} |\alpha| - |\beta|$$

Gourdon & Salvy (1996), Dubickas & Sha (2015):

abs sep
$$(P) \gg H(P)^{-d(d^2+2d-1)/2}$$

Bugeaud, D., Fang, Pejković & Salvy (2019):

abs sep
$$(P) \gg H(P)^{-(d-1)(d-2)(d-3)/2}$$

Bugeaud, D., Pejković & Salvy (2017): Neka su $\alpha_1 = \alpha, \alpha_2 = \beta, \alpha_3, \dots, \alpha_d \in \mathbb{C}$ korijeni separabilnog polinoma $P(x) \in \mathbb{Z}[x]$ stupnja d takvog da je $\alpha_i + \alpha_j \neq 0$ za sve $i, j \in \{1, \dots, d\}$. Ako su α i β realni, tada je

$$||\alpha| - |\beta|| \ge 2^{(-d^2+2)/2} (d+1)^{(-d+1)/2} H(P)^{-d+1}.$$

Nadalje, ovdje je eksponent od H(P) najbolji mogući.

Familije polinoma za koje se dostiže eksponent -d + 1:

Konstrukcija započinje s polinomom Mx^2-1 koji ima dva realna korijena $\pm 1/\sqrt{M}$. Perturbirajući Mx^2-1 na odgovarajući način dobivamo polinome oblika $(Mx^2-1)u(x)+v(x)$ čiji su korijeni vrlo blizu $\pm 1/\sqrt{M}$ i čija je suma mala (po apsolutnoj vrijednosti).

Neka su $d \geq 2$ i M prirodni brojevi. Promotrimo polinome $P_{d,M}(x)$ stupnja d i visine M definirane s:

$$P_{d,M}(x) = \begin{cases} Mx^2 - x - 1 & d = 2; \\ x^3 - Mx^2 + 1 & d = 3; \\ x^d + (Mx^2 - 1)(x^{d-3} - 1) & d \ge 4 \text{ paran}; \\ x^d + x^{d-1} - (Mx^2 - 1)(x^{d-3} + x + 1) & d \ge 5 \text{ neparan}. \end{cases}$$

Kada $M \to \infty$, polinomi $P_{d,M}(x)$ imaju dva korijena $\alpha, \beta \in \mathbb{R}$ takva da je

$$0 < |\alpha| - |\beta| = \alpha + \beta \leq M^{-d+1} = H(P_{d,M})^{-d+1}.$$

Polinom $P_{3,M}$ ima dva korijena α_3,β_3 koji zadovoljavaju

$$\alpha_3 = -M^{-1/2} + \frac{1}{2}M^{-2} + O(M^{-7/2}),$$

$$\beta_3 = M^{-1/2} + \frac{1}{2}M^{-2} + O(M^{-7/2}).$$

To se može dokazati tako da se nađu dovoljno mali intervali u kojima polinomi $P_{d,M}(x)$ mijenjaju predznak:

$$P_{3,M}(-M^{-1/2} + \frac{1}{2}M^{-2} - M^{-3}) = -2M^{-5/2} + O(M^{-3}) < 0,$$

$$P_{3,M}(-M^{-1/2} + \frac{1}{2}M^{-2}) = \frac{5}{4}M^{-3} + O(M^{-4}) > 0,$$

za dovoljno velik M, a slično vrijedi i za β_3 .

Slično, za $d \geq$ 4 paran, $P_{d,M}(x)$ ima korijene

$$\alpha = -M^{-1/2} - \frac{1}{2}M^{-(d+1)/2} + \frac{1}{2}M^{-d+1} + O(M^{-(2d+1)/2}),$$

$$\beta = M^{-1/2} + \frac{1}{2}M^{-(d+1)/2} + \frac{1}{2}M^{-d+1} + O(M^{-(2d+1)/2}),$$

dok za $d \geq 5$ neparan, $P_{d,M}(x)$ ima korijene

$$\alpha = -M^{-1/2} - \frac{1}{2}M^{-d/2} + \frac{1}{2}M^{-(2d-3)/2} + \frac{1}{2}M^{-d+1} + O(M^{-(2d-1)/2}),$$

$$\beta = M^{-1/2} + \frac{1}{2}M^{-d/2} - \frac{1}{2}M^{-(2d-3)/2} + \frac{1}{2}M^{-d+1} + O(M^{-(2d-1)/2}).$$

Hvala Vam na pozornosti!