Interpolace

Matěj Doležálek

Abstrakt. Dozvíme-li se několik bodů, jimiž prochází graf neznámého polynomu, co z toho o něm můžeme vyvodit? Ukážeme si, že celkem dost.

Věta. (Lagrangeova interpolace) *Mějme navzájem různá $x_0, x_1, \dots, x_n \in \mathbb{R}$ a libovolná $y_0, y_1, \dots, y_n \in \mathbb{R}$. Pak mezi polynomy s koeficienty z $\mathbb{R}$ stupně nanejvýš n existuje právě jeden, který splňuje $f(x_i) = y_i$ pro $i \in \{0, 1, \dots, n\}$, a je to konkrétně*

$$f(x) = \sum_{i=0}^{n} y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}. \qquad (\heartsuit)$$

Úmluva. Polynom na pravé straně v $(\heartsuit)$ budeme nazývat *(Lagrangeovým) interpolačním polynomem* (skrz body $(x_0, y_0), (x_1, x_2), \dots, (x_n, y_n)$).

Cvičení. Na reálných číslech není nic speciálního – rozmyslete si, že interpolace funguje i nad $\mathbb{Q}$, nad $\mathbb{C}$ nebo nad konečnými tělesy $\mathbb{Z}_p$ pro prvočísla p. (Obecně bychom ji tedy mohli zformulovat nad obecným *tělesem*.)

Hodnoty v bodech

Cvičení. Všimněte si, že $\prod_{j \in \{0,1,\dots,n\} \setminus \{k\}} \frac{n+1-j}{k-j} = (-1)^{n-k} \binom{n+1}{k}$.

Věta. (Binomická) *Pro nezáporné celé číslo n platí $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$.*

Úloha 1. Reálný polynom f stupně nanejvýš n splňuje $f(k) = 2^k$ pro všechna $k = 0, 1, \dots, n$. Spočtěte $f(n+1)$.

Úloha 2. Reálný polynom f stupně nanejvýš n splňuje $f(k) = \frac{1}{\binom{n+1}{k}}$ pro všechna $k = 0, 1, \dots, n$. Určete $f(n+1)$.

Úloha 3. (těžká) Ať F_i značí i-té Fibonacciho číslo, tedy $F_0 = 0$, $F_1 = 1$ a dále $F_{n+1} = F_n + F_{n-1}$. Pokud polynom f stupně 990 splňuje $f(k) = F_k$ pro $k \in \{992, \dots, 1982\}$, dokažte, že $f(1983) = F_{1983} - 1$. (IMO SL 1983)

Koncepčnější pohled, aneb modulení polynomů

Pokusme se okopírovat principy modulární aritmetiky na počítání s polynomy. Pro jednoduchost uvažujme jako modulo nějaký monický lineární polynom $x - a$ a pracujme nad $\mathbb{R}$. Je-li dán reálný polynom f, co se s ním stane modulo $x - a$? Inu, ta nejprvotnější kongruence, co by modulo $x-a$ měla platit, je $x-a \equiv 0$, neboli $x \equiv a$. Jelikož polynom je jen výraz poskládaný ze sčítání a násobení, kteréžto operace by modulární aritmetika měla respektovat, dostaneme $f = f(x) \equiv f(a)$. Jinými slovy, modulo $x - a$ je polynom f kongruentní své hodnotě $f(a)$, takže v Lagrangeově interpolaci můžeme každou podmínku $f(x_i) = y_i$ přeložit jako $f \equiv y_i \pmod{x - x_i}$.

Máme tedy neznámou f, o které máme jen nějaké informace v několika různých modulech – bystří mohou větřit Čínskou zbytkovou větu. V okruhu $\mathbb{R}[x]$ polynomů nad $\mathbb{R}$ jsou naštěstí polynomy $x - a$, $x - a'$ pro $a \neq a'$ nesoudělné, takže v duchu Čínské zbytkové věty se sada podmínek v nesoudělných modulech $x - x_i$ má přeložit do jedné podmínky modulo $(x-x_0)\cdots(x-x_n)$. Už zbývá jen zpozorovat, že v každé takové zbytkové třídě je právě jeden polynom stupně nanejvýš n. Základní forma Lagrangeovy interpolace pak jen říká, že když má polynom splňující tyto podmínky navíc ještě malý stupeň, musí se jednat o tohoto unikátního reprezentanta. Nic nám však nebrání si ponechat volnější výsledek i pro f libovolného stupně:

Věta. (Lagrangeova interpolace trochu obecněji) *Jsou-li $x_0, x_1, \ldots, x_n \in \mathbb{R}$ navzájem různá a $y_0, y_1, \ldots, y_n \in \mathbb{R}$ libovolná a g je Lagrangeův interpolační polynom skrz body $(x_0, y_0), (x_1, x_2), \ldots, (x_n, y_n)$, pak libovolný reálný polynom f (bez omezení stupně) splňuje $f(x_i) = y_i$ pro všechna $i \in \{0, 1, \ldots, n\}$, právě když*

$$f = g + q \cdot \prod_{i=0}^{n} (x - x_i)$$

pro nějaký reálný polynom q.

Koeficienty

Tvrzení. *Je-li f polynom stupně nanejvýš n a $x_0, x_1, \ldots, x_n \in \mathbb{R}$ navzájem různá, pak je*

$$\sum_{i=0}^{n} \frac{f(x_i)}{\prod_{j \neq i} (x_i - x_j)}$$

rovno koeficientu u x^n v f.

Úloha 4. Buď a_n koeficient u x^n v reálném polynomu f stupně nanejvýš n. Dokažte, že potom platí

$$\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} f(i) = n! a_n.$$

Úloha 5. Buď f polynom s celočíselnými koeficienty stupně d a buď p prvočíslo. Dokažte, že pokud $f(0) = 0$, $f(1) = 1$ a pro každé $n \in \mathbb{N}$ dává $f(n)$ po dělení p zbytek 0 nebo 1, potom $d \geq p - 1$. (IMO SL 1997)

Nerovnosti

Idea. Vezmeme libovolný „Lagrangeovský výraz“, který se dosud objevil v příspěvku, a plácneme na něj absolutní hodnoty a trojúhelníkovou nerovnost.

Úloha 6. Reálný polynom f stupně nanejvýš n splňuje na intervalu $\langle 0, 1\rangle$ nerovnost $|f(x)| \leq 1$. Dokažte, že $|f(-1/n)| \leq 2^{n+1} - 1$.

Úloha 7. Je dán monický reálný polynom f a celá čísla $x_0 < x_1 < \cdots < x_n$. Dokažte, že pro nějaké $0 \leq i \leq n$ nastane $|f(x_i)| \geq \frac{n!}{2^n}$. (Crux Mathematicorum)

Úlohy na procvičení

Úloha 8. Buď $F : \mathbb{Z}_p \to \mathbb{Z}_p$ zcela libovolná funkce. Nahlédněte, že ji lze zapsat polynomem s koeficienty ze $\mathbb{Z}_p$.

Úloha 9. (sdílení tajemství) Voldemutovým nejstřeženějším tajemstvím je reálné číslo r. Chtěl by navrhnout systém, ve kterém každému ze svých n smrtijedomutů sdělí nějakou informaci tak, aby

(i) dovedlo libovolných 7 smrtijedomutů spojit své informace a zjistit z nich r,
(ii) ale libovolných 6 nebo méně smrtijedomutů nedovedlo ze svých informací zjistit o r vůbec nic (např. ani žádný omezený interval, v němž musí r ležet).

Poraďte Voldemutovi, jak toho docílit. Dovede ve vašem systému Voldemut přidávat nové smrtijedomuty, aniž by cokoliv nového říkal starším smrtijedomutům?

Úloha 10. Reálný polynom f stupně nanejvýš n nabývá celočíselných hodnot v bodech $0, 1, \ldots, n$. Nahlédněte, že potom už musí nabývat celočíselných hodnot na celém $\mathbb{Z}$.

Úloha 11. Dokažte, že pro navzájem různá $x_0, x_1, \ldots, x_n \in \mathbb{R}$ platí

$$\sum_{i=0}^{n} \frac{x_i^{n+1}}{\prod_{j \neq i}(x_i - x_j)} = \sum_{i=0}^{n} x_i.$$

Úloha 12. Dokažte, že každý monický reálný polynom stupně n lze zapsat jako aritmetický průměr dvou reálných polynomů stupně n, z nichž každý má n různých reálných kořenů. (USAMO 2002)

Úloha 13. Mějme celé číslo $n \geq 3$ a reálné polynomy f, g takové, že body $(f(i), g(i))$ pro $i = 1, \ldots, n$ jsou vrcholy pravidelného n-úhelníku v rovině (čtené v kladném směru). Dokažte, že alespoň jeden z f, g má stupeň alespoň $n - 1$.

(Putnam 2008)

Úloha 14. Dokažte, že platí $\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^{n+1} = \frac{(n+1)!n}{2}$.

Úloha 15. (těžká) Dokažte, že pro každý monický polynom f s komplexními koeficienty existuje komplexní číslo z splňující $|z| = 1$ a zároveň $|f(z)| \geq 1$.

Úloha 16. (těžká) Reálný polynom f stupně nanejvýš 2020 splňuje $f(k^2) = k$ pro $k = 0, 1, \ldots, 2020$. Určete $f(2021^2)$. (HMMT 2020)

Návody

1. Dosaď do interpolačního polynomu a uprav směrem k binomické větě.

2. V interpolačním polynomu zmizí kombinační čísla.

3. Využij, že $F_n = \frac{1}{\sqrt{5}}\big(\varphi^n - (\overline{\varphi})^n\big)$, kde $\varphi = \frac{1+\sqrt{5}}{2}$, $\overline{\varphi} = \frac{1-\sqrt{5}}{2}$. Rozděl sumu, ke které se prointerpoluješ, na část s φ a $\overline{\varphi}$.

4. Hodnoty f v kterých bodech se tu objevují? Takže skrz co asi chceš interpolovat?

5. Interpoluj nad $\mathbb{Z}_p$ a vyjádři koeficient u x^{p-1}.

6. Interpoluj skrz $x_i = \frac{i}{n}$.

7. Využij celočíselnost k odhadu $\prod_{i\neq j}|x_i - x_j|$.

8. Interpoluj skrz všechny body.

9. Sděl smrtijedomutům hodnoty polynomu v bodech.

10. Interpretuj každý člen v interpolačním polynomu pomocí kombinačních čísel.

11. Čteš koeficient, ale stupeň je moc velký – zmodul.

12. Jeden polynom zinterpoluj tak, aby byl hooodně rozkmitaný, druhý dopočítej tak, aby vyšel průměr.

13. Interpoluj jeden komplexní polynom. Vhodné BÚNO situaci zjednoduší.

14. Interpoluj $f(x) = x^n$, ale dívej se na koeficient u x^{n-1}.

15. Použij kořeny $x^{n+1} - 1$. Výraz $\prod_{i\neq j}(x_i - x_j)$ je hodnota derivace v kořenu!

16. Interpolace dá děsivou sumu, ale jde to ubít. $\sum_{k=0}^{m}(-1)^k\binom{n}{k}$ jde spočítat!

Literatura a zdroje

Tento příspěvek je z většiny založen na *i*KSkové přednášce Kuy Löwita, kterému tímto děkuji. Dále jsem některé úlohy přezval z obecnějších příspěvků o polynomech.

[1] Jakub Löwit: *Lagrangeova interpolace*, sborník *i*KS, 2018.
[2] Titu Andreescu, Gabriel Dospinescu: *Problems from the Book*, XYZ Press, 2008.
[3] Filip Sládek: *Aritmetické vlastnosti polynómov*, sborník *i*KS, 2013.
[4] Martin „E.T.“ Sýkora: *Polynomy bez Viètových vztahů*, Hojsova Stráž, 2016.