Sklené

Sborník, podzim 2019

Filip Čermák
Matěj Doležálek
Verča Hladíková
Lenka Kopfová
Daniil Koževnikov
Anna Mlezivová
Viki Němeček
Radek Olšák
Terka Poláková
Marian Poljak
Hedvika Ranošová
Martin Raška
Rado van Švarc
Michal Töpfer

Autoři: Filip Čermák, Matěj Doležálek, Verča Hladíková, Lenka Kopfová, Danil Koževnikov, Anna Mlezivová, Viki Němeček, Radek Olšák, Terka Poláková, Marian Poljak, Hedvika Ranošová, Martin Raška, Rado van Švarc, Michal Töpfer
Editor: Viki Němeček, Michal Töpfer
vydání první, náklad 45 výtisků
září 2019
Díky za pomoc všem, kterým je za co děkovat.

Algebraické triky neboli... fígle

Filip Čermák

Abstrakt. Příspěvek obsahuje řadu algebraických triků, které se hodí při řešení příkladů nebo jejich částí. Velkým zdrojem triků, které člověk více či méně často použije, bývají nerovnosti a velkým zdrojem k řešení nerovností je zase seriál MKS od Michala Rolínka a Pavla Šaloma, který najdete na našich stránkách[1]. Ten tedy doporučuji přečíst každému, kdo má pocit, že se potřebuje v algebraických manipulacích zlepšit.

Úmluva. Úlohy jsou v tomto příspěvku označeny slovem **Příklad**, pokud patří mezi ty snazší, a slovem **Úloha**, pokud patří mezi ty náročnější.

Poznámka. (Symetrie a cykličnost) Výraz v několika proměnných je symetrický, pokud se nezmění prohozením libovolných dvou z nich. Pak můžeme BÚNO předpokládat, že proměnné jsou v námi vybraném pořadí (např. od největší po nejmenší).

Výraz je cyklický, pokud se nezmění po cyklické záměně (např. x za y, y za z a zároveň z za x). Poté můžeme BÚNO předpokládat například to, že jedna z proměnných je největší. Tyto úvahy často zkrátí sepisování řešení alespoň na polovinu.

Dosazení

Máme-li soustavu rovnic, často stačí jednu proměnnou vyjádřit a dosadit.

Příklad 1. Součin reálných čísel x, y, z je jedna. Určete všechny možné hodnoty výrazu

$$\frac{1}{1+x+xy}+\frac{1}{1+y+yz}+\frac{1}{1+z+zx}.$$

Příklad 2. Pro nenulová reálná čísla a, b, c platí

$$a^2-b^2=bc, \qquad b^2-c^2=ca.$$

Ukažte, že pak platí i $a^2-c^2=ab$.

Rozklady na součin

Mají-li se v úloze najít všechna prvočísla určitého tvaru, zpravidla se snažíme příslušný výraz rozložit na součin, protože pak je snadné říci, kdy půjde o prvočísla (jen jeden z činitelů je různý od ± 1). Ale umět rozkládat na součin se hodí i jindy.

[1] *http://mks.mff.cuni.cz/archive/29/9.pdf*

Příklad 3. Najděte dvě čtyřmístná čísla, jejichž součinem je $4^8 + 6^8 + 9^8$.

Příklad 4. Najděte všechna celá čísla n, pro něž je $n^4 - 3n^2 + 9$ prvočíslo. (MO 61-III-1)

Úloha 5. Dokažte, že existuje nekonečně mnoho kladných celých čísel a takových, že pro žádné $n \in \mathbb{N}$ není $n^4 + a$ prvočíslo. (IMO 1969)

Úloha 6. Najděte nejmenší trojciferné číslo n, pro nějž má soustava

$$\begin{aligned} x^3 + y^3 + x^2y + xy^2 &= n \\ x^2 + y^2 + x + y &= n + 1 \end{aligned}$$

pouze celočíselná řešení.

Substituce $xyz = 1$

Máme-li na proměnné podmínku $xyz = 1$, často pomůže substituce

$$x = \frac{a}{b}, \quad y = \frac{b}{c}, \quad z = \frac{c}{a}.$$

Cvičení. Rozmyslete si, že tuto substituci opravdu můžeme použít, tedy že pro každá x, y, z splňující tuto podmínku existují vhodná a, b, c.

Příklad 7. Opět vyřešte Příklad 1.

Příklad 8. Kladná čísla a, b, c splňují $abc = 1$. Dokažte

$$\frac{1 + a^2c}{c(b + c)} + \frac{1 + b^2a}{a(c + a)} + \frac{1 + c^2b}{b(a + b)} \geq 3.$$

Úloha 9. Pro kladná a, b, c splňující $abc = 1$ dokažte

$$\frac{a}{b} + \frac{b}{c} + \frac{c}{a} \geq a + b + c.$$

(MO 52-III-6)

Substituce $x' = x + c$

Ještě jednodušší substituce je pouhý posun všech proměnných o konstantu, často ale vyřeší celou úlohu.

Příklad 10. Najděte všechna reálná x splňující

$$(x^2 + 3x + 2)(x^2 - 2x - 1)(x^2 - 7x + 12) + 24 = 0.$$

V následujícím příkladu budeme využívat jedno zajímavé tvrzení o polynomech (jinak ale pro naši přednášku nedůležité).

Věta. (Eisensteinovo kritérium) *Mějme polynom* $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *s celočíselnými koeficienty a prvočíslo* p *tak, že*

(i) $p \nmid a_n$,
(ii) $p \mid a_i, \forall i \in \{0, \ldots, n-1\}$,
(iii) $p^2 \nmid a_0$.

Potom je polynom $P(x)$ *ireducibilní nad* $\mathbb{Q}$ *(tedy neexistují nekonstantní polynomy s racionálními koeficienty, jejichž součin by byl rovný* P*).*

Příklad 11. Nechť p je prvočíslo. S pomocí Eisensteinova kritéria dokažte, že polynom $P(x) = x^{p-1} + x^{p-2} + \cdots + 1$ je ireducibilní nad $\mathbb{Q}$.

Úloha 12. Jsou dána reálná čísla x, y, z, která splňují

$$x + y + z = 12, \qquad x^2 + y^2 + z^2 = 54.$$

Ukažte, že alespoň jedno z čísel x, y, z je nejvýše rovno třem a alespoň jedno je větší nebo rovno pěti. (MO 60-III-3)

Linearita proměnné

Máme-li výraz, který je v některé proměnné lineární, pak bude nabývat svých extrémů pro její krajní hodnoty. To úlohu mnohdy velmi zjednoduší nebo úplně vyřeší.

Příklad 13. Jsou dána čísla a, b, c z intervalu $\langle 0, 1\rangle$. Ukažte nerovnosti

$$6 \geq 3abc + 4(1-a)(1-b)(1-c) + a + b + c \geq 1.$$

(MKS 28-7-6)

Příklad 14. Nalezněte minimum a maximum výrazu

$$a(1-b) + b(1-c) + c(1-a),$$

v němž a, b, c jsou z intervalu $\langle 0, 1\rangle$.

Příklad 15. Pro $x, y \in \mathbb{R}$ a $z \in \langle -2, 2\rangle$ ukažte nerovnost

$$x^2 + y^2 \geq xyz.$$

Příklad 16. Nechť $n \geq 2, 0 \leq x_i \leq 1, i = 1, 2, \ldots, n$. Dokažte nerovnost

$$\sum_{i=1}^{n} x_i - \sum_{i=1}^{n} x_i x_{i+1} \leq \left\lfloor \frac{n}{2} \right\rfloor,$$

kde $x_{n+1} = x_1$. (Výběrové soustředění 2016)

Homogenita

Definice. (Homogenita) Výraz $V(a,b,c)$ nazveme homogenní stupně α, pokud existuje $\alpha \in \mathbb{R}$ takové, že pro každé $t > 0$ platí

$$V(ta,tb,tc) = t^{\alpha} V(a,b,c).$$

Máme-li homogenní nerovnost, můžeme si pomoci tím, že si přidáme nějakou podmínku (jejíž splnění můžeme zaručit právě pomocí t v předchozí definici).

Příklad 17. Pro $a,b \geq 0$ a $s \geq r$ dokažte

$$(a^r + b^r)^{\frac{1}{r}} \geq (a^s + b^s)^{\frac{1}{s}}.$$

Příklad 18. Pro $a,b > 0$ ukažte

$$a^4 + 2b^4 \geq a^2b^2 + 2ab^3.$$

Úloha 19. Dokažte Cauchy-Schwarzovu nerovnost: $n \in \mathbb{N}$, dále $u_1, u_2, \ldots, u_n \in \mathbb{R}$ a $v_1, v_2, \ldots, v_n \in \mathbb{R}$. Pak

$$(u_1^2 + u_2^2 + \cdots + u_n^2)(v_1^2 + v_2^2 + \cdots + v_n^2) \geq (u_1v_1 + u_2v_2 + \cdots + u_nv_n)^2.$$

(Ne)rovnost

Máme-li nějakou rovnici nebo soustavu rovnic, můžeme si někdy pomoci tím, že ukážeme, že jedna strana je větší než druhá, a využijeme, že víme, kdy v námi použité nerovnosti nastává rovnost.

Úloha 20. V oboru reálných čísel řešte soustavu rovnic

$$\begin{aligned} x^4 + y^2 + 4 &= 5yz, \\ y^4 + z^2 + 4 &= 5zx, \\ z^4 + x^2 + 4 &= 5xy. \end{aligned}$$

(MO 61-III-6)

Úloha 21. Určete všechny trojice (a,b,c) kladných reálných čísel, které jsou řešeními soustavy rovnic

$$\begin{aligned} a\sqrt{b} - c &= a, \\ b\sqrt{c} - a &= b, \\ c\sqrt{a} - b &= c. \end{aligned}$$

(ČPS 2010)

Polynomy

Příklad 22. Mějme reálná čísla x, y, z, pro která platí

$$x+y+z=0,$$
$$xy+yz+zx=0.$$

Dokažte, že $x=y=z=0$.

Příklad 23. Ukažte, že pokud pro nenulová reálná čísla a, b, c platí rovnost

$$\frac{a-b}{c}+\frac{b-c}{a}+\frac{c-a}{b}=0,$$

tak se dvě z těchto tří čísel rovnají.

Příklad 24. Jakých hodnot může nabývat výraz

$$\frac{(a+b-c)^2}{(a-c)(b-c)}+\frac{(b+c-a)^2}{(b-a)(c-a)}+\frac{(c+a-b)^2}{(a-b)(c-b)}$$

pro všechny možné trojice po dvou různých reálných čísel a, b, c?

(Výběrové soustředění 2013)

Úloha 25. Nechť a, b, c, d, e, f jsou přirozená čísla. Označme $S=a+b+c+d+e+f$. Platí, že S dělí výrazy $abc+def$ a $ab+bc+ca-de-ef-fd$. Dokažte, že S je složené. (IMO shortlist 2005)

Algebra? Ne, geometrie!

Úloha 26. Dvojice nekonečných posloupností celých čísel a_1, a_2, … a b_1, b_2, … splňuje pro $n \geq 3$ vztah

$$(a_n-a_{n-1})(a_n-a_{n-2})+(b_n-b_{n-1})(b_n-b_{n-2})=0.$$

Ukažte, že existuje přirozené k takové, že $a_k=a_{k+2016}$. (iKS 5. ročník, A5)

Úloha 27. Vyřešte úlohu 12, tentokrát geometricky.

Trikové úpravy

Úloha 28. Celá čísla x, y, z splňují vztah

$$(x-y)^2+(y-z)^2+(z-x)^2=xyz.$$

Dokažte, že výraz $x^3+y^3+z^3$ je dělitelný $x+y+z+6$.

Úloha 29. Nechť existuje $n > 0$ reálných čísel $x_1, x_2, \ldots, x_n$, která pro každé $i = 1, \ldots, n$ splňují

$$x_i = \frac{1}{x_i - x_1} + \frac{1}{x_i - x_2} + \cdots + \frac{1}{x_i - x_{i-1}} + \frac{1}{x_i - x_{i+1}} + \cdots + \frac{1}{x_i - x_n}.$$

Navíc platí $x_1^2 + x_2^2 + \cdots + x_n^2 = 45$. Určete n. (MKS 27-1-8)

Úloha 30. Pro libovolná nezáporná reálná čísla a a b dokažte nerovnost

$$\frac{a}{\sqrt{b^2+1}} + \frac{b}{\sqrt{a^2+1}} \geq \frac{a+b}{\sqrt{ab+1}}$$

a zjistěte, kdy nastane rovnost. (MO 63-III-6)

Návody

1. Dosaďte $z = \frac{1}{xy}$ a zlomky zjednodušte a sečtěte.

2. Z první rovnice dosaďte za c do druhé a třetí. Nyní má z druhé rovnice plynout třetí. Všimněte si, že druhou rovnici lze vydělit a, a potom ji vytkněte ze třetí rovnice.

3. Přičtěte 6^8, abyste mohli využít vzorečku, a pak ho opět odečtěte a využijte jiného vzorečku. Ověřte čtyřmístnost obou čísel.

4. Přičtěte a odečtěte $9n^2$ a s pomocí dvou vzorečků rozložte na součin.

5. Zvolte $a = 4m^4$ pro $m > 1$ a rozložte na součin.

6. Označte $a = x^2 + y^2, b = x + y$, odvoďte $a = n, b = 1$, Vyřešte kvadratickou rovnici a odvoďte v jakém tvaru musí být n. Výsledek by měl být 113.

7. Tady se fakt nedá nic nového radit :D. Udělejte substituci a upravte (sečtěte zlomky).

8. Udělejte substituci a použijte AG-nerovnost (jde to i rovnou bez substituce, ale po substituci je to lépe vidět).

9. Po substituci nerovnost vynásobte třemi a rozložte ji na součet tří cyklických AG-nerovností.

10. Rozložte kvadratické trojčleny na součin, zvolte $y = x - 1$ a následně $z = y^2$. Vyřešte kubickou rovnici v z natipováním kořenů.

11. Polynom sečtěte na $P(x) = \frac{x^p-1}{x-1}$, uvažte polynom $Q(x) = P(x+1)$ a dokažte, že je ireducibilní. Uvědomte si, že P je pak také nutně ireducibilní.

12. Pro první část uvažme $x = a + 3$, $y = b + 3$, $z = c + 3$. Pro druhou $x = 5 - a$ atd.. Potom už stačí říct, že je jedno z a, b, c nekladné.

13. Stačí rozebrat osm možností, kdy $a, b, c \in \{0, 1\}$. Díky symetrii výrazu můžete navíc předpokládat $a \geq b \geq c$ a rozebírat jen čtyři možnosti.

15. Díky linearitě v proměnné z stačí rozebrat případy $z = \pm 2$.

16. Využijte linearitu a představte si n kuliček na kružnici, kde některé jsou černé a některé bílé. Co počítá výraz na levé straně?

17. BÚNO předpokládejte $a^r + b^r = 1$. Pak $1 \geq a, b \geq 0$, a tedy $a^r \geq a^s$ a $b^r \geq b^s$.

18. BÚNO předpokládejte $b = 1$ a polynom rozložte na součin tipováním kořenů.

19. Nejprve využijte homogennost v $u_1, \ldots, u_n$ a BÚNO předpokládejte $u_1^2 + \cdots + u_n^2 = 1$ a pak ještě stejnou úvahu zopakujte pro $v_1, \ldots, v_n$. Nakonec využijte odhady $\frac{1}{2}u_i^2 + \frac{1}{2}v_i^2 \geq u_i v_i \geq -\left(\frac{1}{2}u_i^2 + \frac{1}{2}v_i^2\right)$.

20. Využijte odhad $4x^2 \leq x^4 + 4$ a jeho cyklické záměny a získané nerovnosti sečtěte.

21. BÚNO předpokládejte, že a je největší a dokažte postupně $b \leq 4, c \geq 4$ a $c \leq b$.

22. Uvažte polynom třetího stupně s kořeny x, y, z a pomocí Vietových vztahů odvoďte, že je tvaru $t^3 + c = 0$.

23. Vynásobte abc a uvažujte jako polynom v a. Dokažte, že se rovná polynomu $(b-c)(a-b)(a-c)$.

24. Označte výraz ze zadání jako výraz $V(a)$ v neznámé a s parametry b, c. Uvažte polynom $P(a) = V(a)(a-b)(b-c)(c-a)$, ukažte, že je druhého stupně a b i c jsou jeho kořeny (pozor, to není jasné, protože $V(a)$ není polynom!). Stejně jako v předchozím příkladu rozložte polynom $P(a)$, když znáte jeho kořeny.

25. Uvažte polynom $P(x) = (x+a)(x+b)(x+c) - (x-d)(x-e)(x-f)$.

26. Uvažujte body v rovině $X_n = (a_n, b_n)$. Rozmyslete si, že trojúhelník X_n, X_{n-1}, X_{n-2} má pravý úhel u vrcholu X_n. Z Pythagorovy věty odvoďte, že vzdálenosti mezi po sobě jdoucími body se nezvětšují, a využijte celočíselnosti.

27. Uvědomte si, že soustava rovnic definuje kružnici v prostoru. Tu rozdělte na šest částí (vždy získáte dva body při průniku kružnice s rovinou danou dvěma osami) a pro každou část si rozmyslete, jakých hodnot v ní nabývají jednotlivé souřadnice.

28. Využijte vzoreček $a^3 + b^3 + c^3 - 3abc = (a+b+c)(a^2+b^2+c^2-ab-bc-ca)$.

29. V součtu druhých mocnin nahraďte vždy jedno x_i pomocí vztahu v zadání.

30. Roznásobte, upravte, aby na obou stranách byl rozdíl odmocnin, a netradičním způsobem využijte vztah $x^2 - y^2 = (x-y)(x+y)$.

Literatura a zdroje

Obrovský dík patří *Štěpánu Šimsovi* od něhož byl příspěvek (skoro beze změn) převzat.

[1] Štěpán Šimsa: *Algebrické triky*, Lipová-lázně, 2016.
[2] Michal „Kenny“ Rolínek: *Algebraické legrácky*, Blansko-Obůrka, 2011.
[3] Michal „Kenny“ Rolínek, Pavel Šalom: *Zdolávání nerovností*, *http://mks.mff.cuni.cz/archive/29/9.pdf*
[4] Martina Vaváčková: *Rozklady na součin*, Hojsova Stráž, 2011.

Zbytky a mocnění

Filip Čermák

Abstrakt. Příspěvek obsahuje návod na řešení olympiádních úloh pomocí kongruencí a také uvádí základní věty z teorie čísel: malou Fermatovu větu, Wilsonovu větu a Eulerovu větu. Je zde také spousta příkladů na procvičení.

Úmluva. Není-li řečeno jinak, pracujeme s celými čísly.

Definice. Skutečnost, že $a = bk$, tedy a je násobek b, zapisujeme $b \mid a$ a říkáme „*b dělí a*“.

Definice. Skutečnost, že $n \mid a - b$, značíme $a \equiv b \pmod{n}$ a říkáme „*a* je *kongruentní s b modulo n*“.

Tvrzení. *Mějme a nesoudělné s n, dále mějme čísla b a c, pak* $ab \equiv ac \pmod{n}$ *je ekvivalentní* $b \equiv c \pmod{n}$.

Definice. Množinu čísel nazýváme *úplnou sadou zbytků modulo n*, pokud každý zbytek modulo n je kongruentní s alespoň jedním prvkem z dané množiny.

Tvrzení. *Platí rovnost množin* $\{0, 1, \ldots, p-1\} = \{a \cdot 0, a \cdot 1, \ldots, a \cdot (p-1)\}$ *pro* $a \not\equiv 0 \pmod{p}$.

Věta. *(Malá Fermatova) Buď p prvočíslo a a číslo s ním nesoudělné, potom*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Věta. *(Wilsonova) Přirozené číslo p je prvočíslo právě tehdy, když*

$$(p-1)! \equiv -1 \pmod{p}.$$

Věta. *(Eulerova) Buď a nesoudělné s n a* $\varphi(n)$ *počet čísel menších než n nesoudělných s n. Potom*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Tvrzení. *Eulerovu funkci* $\varphi(n)$ *lze spočítat následovně: pokud* $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, *pak* $\varphi(n) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdots (p_k - 1)p_k^{\alpha_k - 1}$.

Definice. *Řád čísla a modulo n* nazveme nejmenší nenulové číslo r takové, že $a^r \equiv 1 \pmod{n}$.

Tvrzení. *Z Eulerovy věty plyne, že řád dělí $\varphi(n)$.*

Definice. Zaveďme množinu $\mathbb{Z}_n^*$ obsahující všechny zbytky modulo n nesoudělné s n. Její velikost je tedy rovna $\varphi(n)$.

Tvrzení. *(Bezoutovo lemma) Nechť jsou a a b celá čísla, jejichž největší společný dělitel je d. Pak existují celá čísla x a y, tak zvané Bezoutovy koeficienty, taková, že $ax + by = d$. Tyto koeficienty lze nalézt pomocí Euklidova algoritmu.*

Tvrzení. *(Existence inverzu) Pro každé a nesoudělné s n existuje inverzní prvek x, tedy z definice číslo splňující $ax \equiv 1 \pmod{n}$, ekvivalentně $ax + yn = 1$. Z Bezoutova lemmatu a nesoudělnosti n a a plyne, že taková x, y existují, navíc je také x nesoudělné s n, takže také patří do $\mathbb{Z}_n^*$.*

Poznámka. Inverzní prvek k a v $\mathbb{Z}_n^*$ budeme značit $\frac{1}{a}$.

Tvrzení. *Existenci $\frac{1}{a}$ můžeme nahlédnout z Eulerovy věty, protože jde o prvek $a^{\varphi(n)-1}$. Konkrétně pokud je n prvočíslo, pak je prvek a^{n-2} jeho inverzem. S těmito zlomky můžeme pracovat obdobně jako s normálními racionálními čísly: jsou-li b a d nesoudělná s n, pak v $\mathbb{Z}_n^*$ platí*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = (ad + bc)\frac{1}{bd}.$$

Úlohy

Úloha 1. Najděte pro n větší než 1 a celé číslo x všechna řešení $(n-1)! \equiv x \pmod{n}$.

Úloha 2. V závislosti na a určete zbytek $\binom{p-1}{a}$ modulo p.

Úloha 3. Nechť $P(x) = 5x^{13} + 13x^5 + 9ax$. Najděte nejmenší a takové, že $P(x)$ je dělitelné 65 pro každé x. (Irsko 2000)

Úloha 4. Najděte všechna kladná n, pro která je $n! + 5$ čtverec.

Úloha 5. Nechť $p > 5$ je prvočíslo a číslo a je tvořeno $p - 1$ jedničkami v soustavě o základu $p + 6$. Dokažte, že $p \mid a$.

Úloha 6. Najděte všechna prvočísla p a q taková, že $p + q = (p - q)^3$. (Rusko 2001)

Úloha 7. Dokažte, že existují právě tři nejvýše n-ciferná přirozená čísla a taková, že $a^2 \equiv a \pmod{10^n}$. (MKS–24–5–5)

Úloha 8. Ukažte, že pro různá prvočísla p a q platí

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Úloha 9. Nechť p a q jsou prvočísla. Dokažte, že $p^{p(q-1)} - 1$ není dělitelné číslem $(p^{q-1} - 1)q$.

Úloha 10. Zjistěte, pro která přirozená n platí, že $n \mid 3^{n!} - 2^{n!}$.
(MKS 17–7–4)

Úloha 11. Uvažujme posloupnost $a_1, a_2, \ldots$ definovanou vztahem $a_n = 6^n + 3^n + {+}2^n - 1$. Určete všechna přirozená čísla, která jsou nesoudělná s každým členem této posloupnosti. (IMO 2005)

Úloha 12. Dokažte, že pro každé x a každá y, z, w lichá platí $17 \mid x^{y^{z^w}} - x^{y^z}$.
(Irsko 2005)

Úloha 13. Najděte všechna prvočísla p, pro která je výraz

$$\binom{p}{1}^2 + \binom{p}{2}^2 + \ldots + \binom{p}{p-1}^2$$

dělitelný p^3. (CPS 2008–3)

Úloha 14. Pro liché prvočíslo p dokažte

$$1^{p-2} + 2^{p-2} + \ldots + \left(\frac{p-1}{2}\right)^{p-2} \equiv \frac{2 - 2^p}{p} \pmod{p}.$$

(iKS 2012/N3)

Úloha 15. Dokažte, že pro každé sudé přirozené n platí, že $n^2 - 1$ dělí $2^{n!} - 1$.

Úloha 16. Dokažte, že pokud je $4^n + 2^n + 1$ prvočíslo, potom je n mocnina tří.

Úloha 17. Určete hodnotu výrazu $1 \cdot 2^{-1} + 2 \cdot 3^{-1} + \ldots + (p-2) \cdot (p-1)^{-1} \pmod{p}$ pro libovolné p. (MKS 24–5–7)

Úloha 18. Existuje přirozené číslo n s právě 2015 prvočíselnými děliteli takové, že $n \mid 2^n + 1$? (IMO 2000)

Úloha 19. Definujme $a_1 = 2$, $a_n = 2^{a_{n-1}}$. Dokažte, že pro všechna $n > 1$ platí $n \mid a_n - a_{n-1}$. (iKS 2012/N5)

Úloha 20. Nechť je a liché přirozené číslo. Dokažte, že jsou $a^{2^n} + 2^{2^n}$ a $a^{2^m} + 2^{2^m}$ pro všechna přirozená $n \neq m$ nesoudělná.

Návody

7. Pro $n = 1$ máme 1, 5, 6. První krok máme, co takhle pokračovat indukcí?

9. Zkuste ten levý výraz rozložit.

10. Podívejme se, jak vypadá Eulerova funkce.

11. Jelikož n může být libovolné přirozené číslo, co kdyby to bylo třeba $p - 2$ pro prvočíslo p.

13. Důležité je, že všechny členy jsou dělitelné p^2, pak už stačí dokázat jen dělitelnost p, navíc $(p-k)! \equiv (-1)^{p-k}k(k+1)\cdots p$.

14. Kde jen už jsme to a^{p-2} viděli? Taky je docela fajn umět sčítat $1+1=2$, pak se to dá hezky rozložit binomickou větou.

15. Asi zase ta Eulerova funkce.

16. $x^2 + x + 1 \mid x^{2n} + x^n + 1$, pokud $3 \nmid n$.

17. Můžou být nějaké dva členy toho součtu stejné modulo p?

18. Pro $n = 9$ to platí, pak můžete zase zkusit nějakou indukci. Pokud totiž $n \mid 2^n + 1$, $p \mid 2^n + 1$ a zároveň $p \nmid n$, pak $np \mid 2^{np} + 1$, např $p_1 = 19$ vypadá, že funguje.

20. Pro spor jsou soudělná a jejich společný dělitel obsahuje prvočíslo p. Potom tedy chceme zkoumat řád $\frac{a}{2} \pmod p$.

Literatura a zdroje

[1] Kuba Svoboda: *Zbytky a mocnění*, Staré Město, 2015.
[2] *AoPS*, *http:/artofproblemsolving.com/community*
[3] Staré ročníky *i*KS, *http:/iksko.org/problems.php*

Pellova rovnice a kvadratické okruhy

Matěj Doležálek

Abstrakt. Příspěvek se zabývá slavnou Pellovou rovnicí a souvisejícími (reálnými) kvadratickými okruhy. Ukážeme si důkaz existence jejích netriviálních řešeních vycházející z tzv. diofantických aproximací, popíšeme grupovou strukturu jednotek v reálném kvadratickém okruhu a projdeme některé zajímavé úlohy a aplikace.

Pod přívlastkem „Pellova“ je známa diofantická rovnice[1]

$$x^2 - dy^2 = 1,$$

kde d je přirozené číslo, které není čtvercem celého čísla. V teorii čísel si vysloužila výjimečné postavení, neboť se za jejím jednoduchým zadáním skrývá velmi zajímavá struktura a spousta souvislostí s mnoha zajímavými oblastmi matematiky.

Okamžitě jsou vidět dvě řešení Pellovy rovnice: $(x, y) = (\pm 1, 0)$. Tato dvě řešení budeme nazývat triviálními a většinu času se o ně nebudeme moc zajímat. Dokážeme následující: Pellova rovnice má vždy nekonečně mnoho netriviálních řešení, z nichž všechna jsou generována[2] jediným z nich.

Kvadratické okruhy

Definice. *Kvadratickým okruhem* rozumíme množinu

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\},$$

kde $d \in \mathbb{Z}$ není čtvercem celého čísla, opatřenou operacemi sčítání a násobení obvyklým způsobem. Množina $\mathbb{Z}[\sqrt{d}]$ tedy obsahuje všechny výrazy tvaru $a + b\sqrt{d}$ pro a, b celá čísla.

Pokud $d > 0$, nazýváme $\mathbb{Z}[\sqrt{d}]$ *reálným* kvadratickým okruhem, pokud $d < 0$, nazýváme jej *komplexním* kvadratickým okruhem. Pokud v této definici všude napíšeme $\mathbb{Q}$ namísto $\mathbb{Z}$, dostaneme *kvadratické těleso* $\mathbb{Q}(\sqrt{d})$.

Obecně *komutativním okruhem* rozumíme množinu R, ve které umíme sčítat, odčítat a násobit podle všech obvyklých pravidel (a výsledky těchto operací jsou

[1] To značí, že hledáme pouze celočíselná řešení.

[2] Co přesně je tímto slovíčkem míněno, nalezneš dále v příspěvku.

opět prvky R). *Tělesem* pak rozumíme takový komutativní okruh, ve kterém navíc umíme dělit každým prvkem kromě nuly.

Cvičení. Rozmyslete si, že kvadratický okruh je komutativní okruh.

Cvičení. Co se stane, když $d = m^2$ pro nějaké $m \in \mathbb{Z}$?

Cvičení. Kdy platí $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$?

Cvičení. Rozmyslete si, že pokud pro $a_1, b_1, a_2, b_2 \in \mathbb{Q}$ platí $a_1 + b_1\sqrt{d} = a_2 + b_2\sqrt{d}$, pak už nutně $a_1 = a_2$ a zároveň $b_1 = b_2$.

V této přednášce se budeme zabývat hlavně reálnými kvadratickými okruhy, avšak intuice a motivace za uvedenou definicí je dost podobná zavedení komplexních čísel. Trápí nás kvadratická rovnice $x^2 - d = 0$, pro kterou nemáme v oboru celých (resp. racionálních) čísel řešení. No tak si ho prostě zavedeme pod jménem $\sqrt{d}$ a začneme s ním počítat. Jediné, co při tom požadujeme, je $(\sqrt{d})^2 = d$.

Definice. Pro každé číslo $\lambda = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ (resp. $\mathbb{Q}(\sqrt{d})$) definujeme jeho *sdružené číslo* jako

$$\overline{\lambda} = a - b\sqrt{d}$$

a jeho *normu* jako

$$N(\lambda) = \lambda \cdot \overline{\lambda} = a^2 - dy^2.$$

Cvičení. Rozmyslete si, že 0 je jediným prvkem $\mathbb{Q}(\sqrt{d})$ s normou 0.

Cvičení. Nechť $d \equiv 1 \pmod 4$. Rozmyslete si, že množina

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{ a + b \cdot \frac{1+\sqrt{d}}{2} \;\middle|\; a, b \in \mathbb{Z} \right\}$$

tvoří komutativní okruh, jehož prvky mají celočíselné normy.

Sdružené číslo nám dává způsob, jak z $\lambda = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ vytáhnout jeho racionální a iracionální část – platí

$$a = \frac{\lambda + \overline{\lambda}}{2}, \qquad b = \frac{\lambda - \overline{\lambda}}{2\sqrt{d}}.$$

Stejně tak nám norma pomůže rozepsat

$$\frac{1}{\lambda} = \frac{\overline{\lambda}}{N(\lambda)} = \frac{a}{a^2 - db^2} - \frac{b}{a^2 - db^2}\sqrt{d}.$$

Cvičení. Rozmyslete si, že kvadratické těleso je těleso.

Nyní už je vidět, proč jsme si zavedli kvadratické okruhy. Pokud pojmenujeme $\omega = x + y\sqrt{d}$, můžeme Pellovu rovnici jednoduše přepsat jako[3] $N(\omega) = 1$. Kvadratické okruhy nám dávají zajímavou algebraickou strukturu „pod“ Pellovou rovnicí.

[3] Triviální řešení pak odpovídají $\omega = \pm 1$

Cvičení. Rozmyslete si, že $\overline{(\alpha \cdot \beta)} = \overline{\alpha} \cdot \overline{\beta}$.

Důsledek. *Norma je úplně multiplikativní, neboli* $N(\alpha\beta) = N(\alpha)N(\beta)$.

V kvadratickém okruhu můžeme dělat většinu věcí, které můžeme dělat v celých číslech. Teď se zaměřme na dělitelnost a modulení. Pro $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ řekneme, že α *dělí* β (píšeme $\alpha \mid \beta$), pokud existuje $\gamma \in \mathbb{Z}[\sqrt{d}]$ splňující $\beta = \alpha \cdot \gamma$. Pro nenulové α je to ekvivalentní tomu, že $\frac{\beta}{\alpha} \in \mathbb{Z}[\sqrt{d}]$. Dále

$$\alpha \equiv \beta \pmod{\lambda}$$

značí, že $\lambda \mid (\alpha - \beta)$.

Cvičení. Dokažte, že v $\mathbb{Z}[\sqrt{d}]$ existuje přesně $|N(\lambda)|$ zbytkových tříd mod λ.

Lemma. *Pokud* $N(\alpha) = N(\beta) = k \neq 0$ *a zároveň* $\alpha \equiv \beta \pmod{k}$, *pak už* $\alpha \mid \beta$.

Poznámka. (stěžejní trik) Reálné kvadratické okruhy mají následující super vlastnost: jejich prvky jsou reálná čísla. Takže ač většinu času s čísly $a + b\sqrt{d}$ zacházíme jako s dvojicemi (a, b), můžeme je kdykoliv začít porovnávat či řadit jako reálná čísla. Na rozdíl od komplexních kvadratických okruhů se také $N(\lambda)$ nijak přímočaře neodvíjí od $|\lambda|$. Máme tedy dvě různé „velikosti“ čísla $\lambda \in \mathbb{Z}[\sqrt{d}]$: jednak jeho absolutní hodnotu $|\lambda|$ jakožto reálného čísla, ale taky jeho normu $N(\lambda)$, a tyto dvě „velikosti“ dávají dvě zcela odlišné informace.

To hlavní

Postupně ukážeme, že dokud $d \in \mathbb{N}$ není čtverec celého čísla, tak Pellova rovnice má netriviální řešení. Po cestě se bude hodit Dirichletův princip.

Věta. (Dirichletova o diofantických aproximacích) *Nechť je* α *reálné číslo a* t *přirozené číslo. Potom existují* $p \in \mathbb{Z}$, $q \in \{1, \ldots, t\}$ *taková, že* $|q\alpha - p| < \frac{1}{t}$.

Cvičení. Rozmyslete si, že pro nečtvercové $d \in \mathbb{N}$ je množina $\mathbb{Z}[\sqrt{d}]$ hustá v $\mathbb{R}$, tedy že mezi každými dvěma různými reálnými čísly leží nějaký prvek $\mathbb{Z}[\sqrt{d}]$.

Lemma. *Nechť je* $\alpha \in \mathbb{R}$ *iracionální. Pak existuje nekonečně mnoho zlomků* $\frac{p}{q}$ *v základním tvaru takových, že* $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

Lemma. *Nechť* $\alpha = \sqrt{d}$ *a nechť je* $\frac{p}{q}$ *zlomek popsaný v předchozím lemmatu. Potom* $|N(p + q\sqrt{d})| < 2\sqrt{d} + 1$.

Věta. *Pellova rovnice má netriviální řešení.*

Důkaz. Předchozí dvě lemmata nám dohromady vytváří nekonečně mnoho čísel $\lambda \in \mathbb{Z}[\sqrt{d}]$, z nichž každé má celočíselnou normu splňující $|N(\lambda)| < 2\sqrt{d} + 1$. Množina celých čísel v absolutní normě menších než $2\sqrt{d} + 1$ je ale konečná, takže musí existovat celé k takové, že existuje nekonečně mnoho $\lambda \in \mathbb{Z}[\sqrt{d}]$ splňujících $N(\lambda) = k$; toto k musí být nenulové, neboť jen 0 má normu 0. Stejně tak zbytkových tříd mod

k je v $\mathbb{Z}[\sqrt{d}]$ jen konečně mnoho (konkrétně k^2), takže alespoň jedna z nich obsahuje nekonečně mnoho prvků s normou k. Máme tak nekonečnou podmnožinu $\mathbb{Z}[\sqrt{d}]$, jejíž prvky mají všechny stejnou normu a jsou kongruentní modulo tato norma. Pro libovolná dvě taková λ_1, λ_2 pak tedy $\lambda_2 \mid \lambda_1$, neboli $\omega = \frac{\lambda_1}{\lambda_2} \in \mathbb{Z}[\sqrt{d}]$. Z multiplikativity normy ale nutně $N(\omega) = 1$. Když vezmeme čtyři různá $\lambda_1, \lambda_2, \lambda_3, \lambda_4$, pak jsou $\frac{\lambda_2}{\lambda_1}$, $\frac{\lambda_3}{\lambda_1}$ a $\frac{\lambda_4}{\lambda_1}$ po dvou různá, takže alespoň jedno z nich není ± 1 a představuje tak netriviální řešení Pellovy rovnice. □

S pomocí stěžejního triku svedeme dokonce dokázat, že z jediného netriviálního řešení Pellovy rovnice už umíme vygenerovat všechna řešení.

Věta. (grupová struktura) *Existuje $\omega_0 \in \mathbb{Z}[\sqrt{d}]$ takové, že $\omega \in \mathbb{Z}[\sqrt{d}]$ splňuje $N(\omega) = 1$ právě tehdy, pokud $\omega = \pm\omega_0^k$ pro nějaké $k \in \mathbb{Z}$. Takové ω_0 nazýváme* fundamentálním řešením *příslušné Pellovy rovnice.*

Cvičení. Rozmyslete si, že předchozí věta platí i tehdy, pokud namísto $N(\omega)$ píšeme $|N(\omega)|$.[4]

Cvičení. Nechť $d \equiv 1 \pmod 4$. Rozmyslete si, že předchozí věta i předchozí cvičení platí i tehdy, pokud namísto $\mathbb{Z}[\sqrt{d}]$ píšeme $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Základní úlohy

Úmluva. Číslo a nazvěme *čtvercem* v množině S, pokud existuje $b \in S$ splňující $a = b^2$. Není-li řečeno jinak, mluvme o čtvercích v $\mathbb{Z}$.

Příklad 1. Řešte v celých číslech $x^2 + y^2 - 1 = 4xy$.

Definice. *Trojúhelníková čísla* definujme jako $T_n = \frac{n(n+1)}{2}$.

Příklad 2. Najděte všechna n, pro která je T_n čtverec.

Příklad 3. Najděte všechny dvojice $m, n \in \mathbb{N}$ splňující $T_n - T_m = mn$.

Příklad 4. Dokažte, že pokud $3n + 1$ a $4n + 1$ jsou čtverce, pak $56 \mid n$.

Příklad 5. Definujme posloupnost *Fibonacciho čísel* vztahy $F_0 = 0$, $F_1 = 1$ a $F_{n+2} = F_{n+1} + F_n$ pro $n \geq 0$. Dokažte, že pro $x \in \mathbb{N}$ je alespoň jedno z čísel $5x^2 \pm 4$ čtverec, právě pokud je x Fibonacciho číslo.

Jiná konstanta

Občas se nám může stát, že dostaneme rovnici

$$x^2 - dy^2 = c$$

pro jiné c než 1. Těmto rovnicím se obecně říká rovnice Pellova typu a i v jejich řešení nám pomůžou reálné kvadratické okruhy. Případ $c = -1$ (často se mu říká *záporná*

[4] Samozřejmě pak můžeme dostat odlišné ω_0.

Pellova rovnice) jsme už vlastně potkali – víme, že řešení rovnice $|N(\omega)| = 1$ mají grupovou strukturu, takže pokud záporná Pellova rovnice má nějaké nejmenší řešení ω_0, můžeme všechna další vygenerovat jako $\pm\omega_0^\ell$, kde ℓ je liché celé číslo.

Příklad 6. Najděte všechna $n \in \mathbb{N}$, pro která existuje přirozené $k < n$ splňující

$$\binom{n}{k-1} = 2\binom{n}{k} + \binom{n}{k+1}.$$

Cvičení. Rozmyslete si, že pokud je ω_0 nejmenší řešení záporné Pellovy rovnice, pak už je ω_0^2 fundamentální řešení obyčejné Pellovy rovnice.

Příklad 7. Dokažte, že pokud je $\frac{x^2+1}{y^2} + 4$ čtverec, pak už je to nutně 9.

Příklad 8. Nechť je p liché prvočíslo. Ukažte, že rovnice $x^2 - py^2 = -1$ má řešení, právě pokud $p \equiv 1 \pmod 4$.

Obecně pro všechna c můžeme z jednoho řešení dostat nekonečně mnoho dalších: pokud $N(\lambda) = c$, pak i $N(\omega^n\lambda) = c$ pro libovolné n, kde ω je fundamentální řešení Pellovy rovnice. Pozor si ale musíme dát na to, že to nemusí být všechna řešení – může existovat více takovýchto „rodinek“.

Definice. Budiž ω_0 fundamentální řešení Pellovy rovnice a pojmenujme množinu[5] $U = \{\pm\omega_0^n \mid n \in \mathbb{Z}\}$. *Orbitou* nazvěme každou množinu L, která je tvaru

$$L = U\lambda = \{\omega\lambda \mid \omega \in U\}.$$

Orbitě vždy přiřkneme (společnou) normu všech jejích prvků.

Cvičení. Rozmyslete si, že různých orbit dané normy k je jen konečně mnoho (např. určitě méně než k^2).

Příklad 9. Najděte všechna řešení rovnice $x^2 - 3y^2 = 13$.

Příklad 10. Nechť je $p \equiv 3 \pmod 4$ prvočíslo. Dokažte, že právě jedna z rovnic $x^2 - py^2 = \pm 2$ má řešení.

Cvičení. (dvojky jsou fajn) Rozmyslete si, že vždy existuje nanejvýš jedna orbita normy 2 (resp. -2). Z toho pokud je ω fundamentální řešení Pellovy rovnice, pak nejmenší řešení rovnice $N(\lambda) = 2$ (resp. $N(\lambda) = -2$) splňuje $\lambda = \omega\overline{\lambda}$ (resp. $\lambda = -\omega\overline{\lambda}$), neboli $\lambda^2 = 2\omega$ (v obou případech).

Čtverce v $\mathbb{Z}[\sqrt{d}]$

Cvičení. Pokud q je racionální číslo a zároveň čtverec v $\mathbb{Q}(\sqrt{d})$, pak je v $\mathbb{Q}$ buďto čtverec, nebo d-násobek čtverce, a to podle toho, zdali je základ tohoto čtverce ryze racionální, nebo ryze iracionální.

[5] Pro fajnšmekry grupu.

Příklad 11. Dokažte, že pokud je $m = 2+2\sqrt{28n^2+1}$ celé číslo pro nějaké $n \in \mathbb{N}$, pak už je m čtvercem celého čísla.

Příklad 12. Dokažte, že pokud je n^2 rozdílem třetích mocnin dvou po sobě jdoucích přirozených čísel, pak už je $2n-1$ čtverec v $\mathbb{Z}$.

Příklad 13. Seřaďme v rostoucí posloupnost $a_0, a_1, \ldots$ všechna nezáporná čísla a_n, pro která jsou $a_n + 1$ i $3a_n + 1$ čtverce. Dokažte, že pro libovolné přirozené n je $1 + a_{n-1}a_n$ čtverec.

Prvočísla a valuace

Věta. (binomická) *V libovolném komutativním okruhu platí*

$$(x+y)^n = x^n + nx^{n-1}y + \cdots + \binom{n}{k}x^{n-k}y^k + \cdots + y^n.$$

Cvičení. Nechť $n \in \mathbb{N}$ a prvočíslo p dělí d. Potom pokud $a + b\sqrt{d} = (x + y\sqrt{d})^n$ a zároveň $p \nmid x$, $p \mid y$, pak[6] $v_p(b) = v_p(y) + v_p(n)$.

Příklad 14. Najděte všechna n taková, že $3^n - 2$ je čtverec.

Cvičení. Budiž p prvočíslo. Dokažte, že pouze pro konečně mnoho n je $p^n - 2$ čtverec.

Lemma. *Nechť je ω fundamentální řešení Pellovy rovnice. Potom má pro $|n| > 1$ iracionální složka ω^n prvočíselného dělitele, který nedělí d.*

Příklad 15. Najděte všechny dvojice nezáporných celých čísel (x, n), pro něž je splněna rovnice $3 \cdot 2^x + 4 = n^2$.

Příklad 16. Najděte všechna celočíselná řešení rovnice $5^a - 3^b = 2$.

Věta. (Størmerova) *Budiž P konečná množina prvočísel. Přirozené číslo nazvěme* hladkým, *pokud jsou všichni jeho prvočíselní dělitelé z P. Pak existuje pouze konečně mnoho párů po sobě jdoucích hladkých čísel.*

Cvičení. Dokažte, že existuje jen konečně mnoho párů hladkých čísel lišících se o 2.

[6] $v_p(n)$ zde značí *p-valuaci* přirozeného n, tedy největší nezáporné celé číslo splňující $p^{v_p(n)} \mid n$.

Návody

1. Substituce $z = x - 2y$, potom grupová struktura.

3. Důsledně uprav na čtverce. Obdržíš Pellovu rovnici s $d = 8$.

4. Vzorečky pro racionální a iracionální část dají $7 \mid n$. Z kvadratických zbytků mod 8 vymlať $8 \mid n$.

5. Nechť $\varphi = \frac{1+\sqrt{5}}{2}$. Indukcí dokaž vzoreček $F_n = \frac{1}{\sqrt{5}}(\varphi^n - (\overline{\varphi})^n)$ a následně využij grupové struktury jednotek v $\mathbb{Z}[\varphi]$.

7. Ekvivalentně: záporná Pellova rovnice $x^2-(m^2-4)y^2 = -1$ má řešení pouze pro $m = 3$. Rozliš dva případy podle parity, vždy odhadni z malých případů explicitní konstrukci pro nějaké řešení příslušné kladné Pellovy rovnice a zkoumej, kdy může toto řešení být čtvercem v $\mathbb{Z}[\sqrt{m^2-4}]$.

8. Vezmi fundamentální řešení kladné Pellovy rovnice a použij jeho minimalitu.

9. Ujisti se, že máš všechny orbity. Pomůže stěžejní trik.

10. Vezmi fundamentální řešení Pellovy rovnice a použij jeho minimalitu.

11. Vyjádři z grupové struktury a použij předchozí cvičení.

13. Vyjádři z Pellovy rovnice pro $d = 3$. Zatni zuby a poupravuj získaný humus na $\left(\frac{\omega^{2n}+\omega^{-2n}-8}{6}\right)^2$, kde ω je fundamentální řešení.

14. Uprav v $\mathbb{Z}[\sqrt{3}]$, porovnej 3-valuace iracionálních částí a hoď na to stěžejní trik.

16. Substitucí $x = 3^b + 1$, $y = 3^{\frac{b-1}{2}}5^{\frac{a-1}{2}}$ obdržíš Pellovu rovnici s $d = 15$. Najdi spor pomocí nežádoucího prvočísla v iracionální části.

Literatura a zdroje

[1] Anh Dung „Tonda“ Le: *Pellova rovnice*, Lipová-lázně, 2016.

[2] Edward J. Barbeau: *Pell's Equation*, Springer, 2003.

[3] Dušan Djukić: *Pell's equation*, *https://pdfs.semanticscholar.org/6079/b973581e07ff pdf*

Koulítko a rovinítko

Verča Hladíková

Abstrakt. Konstrukční úlohy trochu jinak? Místo roviny prostor, místo pravítka rovinítko, místo kružítka koulítko.

Na přednášce si procvičíme prostorovou představivost řešením konstrukčních úloh ve třech dimenzích. Oproti klasickým nástrojům rovinné geometrie budeme mít k dispozici rovinítko (umožní nám proložit rovinu třemi body, které neleží v jedné přímce) a koulítko (z daného bodu opíše sféru s určeným poloměrem).

Při řešení mnohých úloh napoví, představíš-li si podobnou konstrukci v rovině. Například hned první úloha je „stejná“ jako konstrukce rovnostranného trojúhelníka. Jen má o dimenzi víc.

Příklady

Příklad 1. Sestroj pravidelný čtyřstěn.

Řešení. Zvolíme si v prostoru dva libovolné body A a B. Úsečka AB (její délku označíme a) bude hranou našeho čtyřstěnu. Zabodneme koulítko postupně do bodů A a B a z obou opíšeme sféru o poloměru a. Průnik těchto sfér je kružnice, říkejme jí k. Kdekoliv na k si zvolíme další bod C. Z bodu C opět nakreslíme sféru o poloměru a, ta protne k ve dvou bodech. Libovolný z těchto bodů je čtvrtý vrchol našeho čtyřstěnu.

Příklad 2. Je dána přímka p a bod B, který na ní neleží. Sestroj rovinu kolmou na p a procházející bodem B.

Příklad 3. Je dána rovina σ a přímka p. Sestroj rovinu τ, která je kolmá na σ a současně v ní leží přímka p.

Příklad 4. Mějme rovinu σ a bod B mimo ni. Sestroj přímku p procházející bodem B a kolmou na σ.

Příklad 5. Sestroj přímku q rovnoběžnou s danou přímkou p a procházející daným bodem B nenáležejícím p.

Příklad 6. Sestroj sféru opsanou danému čtyřstěnu.

Příklad 7. Sestroj rovinu, která prochází daným bodem a je rovnoběžná k dané rovině.

Příklad 8. Sestroj čtyřstěn, jsou-li zadána těžiště jeho stěn.

Příklad 9. Sestroj sféru vepsanou danému čtyřstěnu.

Příklad 10. Nechť jsou dány body S, S_{AB}, S_{BD}, S_{CD}, které neleží v jedné rovině. Sestroj čtyřstěn $ABCD$ takový, že S je střed sféry jemu opsané a S_{AB}, S_{BD}, S_{CD} jsou po řadě středy hran AB, BD, CD.

Příklad 11. Sestroj sféru, která prochází danými dvěma body a dotýká se daných dvou sfér.

Příklad 12. Nechť jsou dány nekolineární body T_A, V_A, T_C, přímka p mimoběžná s přímkou T_AV_A a úsečka délky d. Sestroj čtyřstěn $ABCD$ takový, že T_A, resp. T_C, je těžiště stěny BCD, resp. ABD, V_A je pata výšky spuštěné z vrcholu A na stěnu BCD, bod B leží na přímce p a vzdálenost $|CV_A|$ je rovna d.

Příklad 13. Sestroj krychli pouze koulítkem jsou-li dány délky stěnové a tělesové úhlopříčky.

Literatura a zdroje

Celý příspěvek je bezostyšně zkopírován od *Rado vana Švarce*, který ho bezostyšně zkopíroval od *Alči Skálové*, která jej vytvořila pro soustředění v Blansku-Obůrce (2011) a které tímto děkuji.

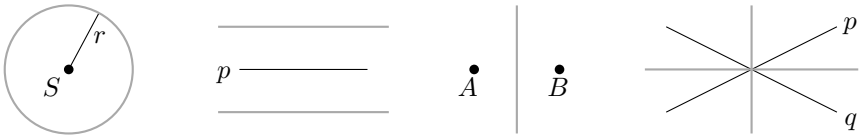
Geometrické množiny bodů

Lenka Kopfová

Abstrakt. Příspěvek shrnuje základní geometrické množiny bodů a obsahuje řadu převážně snadných úloh, k nimž jsou na konci uvedeny stručné postupy a výsledky.

Tvrzení. *Množina bodů, které mají*

(i) *danou vzdálenost r od daného bodu S, je kružnice $k(S, r)$.*
(ii) *danou vzdálenost od dané přímky p, je dvojice přímek rovnoběžných s p.*
(iii) *stejnou vzdálenost od dvou daných bodů A, B, je osa úsečky AB.*
(iv) *stejnou vzdálenost od dvou daných přímek p, q, je dvojice přímek, které jsou osami úhlů vytvořenými přímkami p, q.*



Věta. (Věta o obvodovém úhlu) *Množina bodů, z nichž je daná úsečka AB vidět pod daným úhlem φ, je dvojice kružnicových oblouků symetrických podle přímky AB s krajními body A, B. Speciálně pro $\varphi = 90°$ je hledanou množinou kružnice nad průměrem AB.*

Lehounké úložky

Příklad 1. Jsou dány rovnoběžné přímky p, q. Najděte množinu středů úseček AB takových, že bod A leží na p a bod B na q.

Příklad 2. Je dána kružnice k a bod O. Určete množinu středů všech úseček OP, kde P probíhá kružnici k.

Příklad 3. Jsou dány body A, B. Najděte všechny přímky p, jejichž vzdálenost od A je stejná jako od B.

Příklad 4. Je dána úsečka AB. Určete množinu obrazů A' bodu A v osové souměrnosti podle libovolné přímky procházející bodem B.

Příklad 5. Uvnitř kružnice k se středem O je dán bod P. Určete množinu středů všech tětiv AB kružnice k, které procházejí bodem P. Co kdyby bod P ležel vně kružnice k?

Příklad 6. Polem vede rovná cesta, po které se rozjel autobus.

(i) Kde musí člověk stát, aby autobus dostihnul, pokud běží stejnou rychlostí, jakou autobus jede?
(ii) Co kdyby člověk vyrážel o minutu dřív?
(iii) Co kdyby byl člověk dvakrát pomalejší?

Příklad 7. Po ramenech VX, VY pravého úhlu XVY se pohybují body A, B tak, že úsečka AB má konstantní délku d. Určete množinu středů M úseček AB.

Příklad 8. Je dána úsečka AB. Uvažme všechny dvojice kružnic k, l, které se dotýkají úsečky AB postupně v bodech A, B a navíc mají samy vnější dotyk v T. Určete množinu bodů T.

Běžné příklady

Příklad 9. Jsou dány kružnice k a l, které se protínají v bodech A a B. Na kružnici k zvolíme bod C a označíme D druhý průsečík přímky BC s l. Určete množinu vepsišť trojúhelníku ACD.

Příklad 10. Na úsečce AC je dán bod B. Určete množinu druhých průsečíků X shodných kružnic, z nichž jedna prochází body A, B a druhá body B, C.

Příklad 11. Osa úhlu ABC protne stranu AC trojúhelníku ABC v bodě D. Najdeme bod E v polorovině určené přímkou BC ve které neleží bod A, tak, aby $|\sphericalangle BCE| = |\sphericalangle BAC|$ a $|CE| = |AD|$. Dokažte, že střed úsečky DE leží na BC.

Příklad 12. Určete množinu středů všech úseček AB, jejichž krajní body leží na dané půlkružnici t.

Příklad 13. Bod C probíhá pevný kružnicový oblouk nad tětivou AB. Určete množinu opsišť, těžišť, ortocenter a vepsišť všech takových trojúhelníků ABC.

Příklad 14. V rovině je dána kružnice k se středem S a bod $A \neq S$. Určete množinu opsišť trojúhelníků ABC, jejichž strana BC je průměrem kružnice k.
(MO 56–A–I–5)

Příklad 15. Je dána kružnice k s tětivou AC, jež není průměrem. Na její tečně vedené bodem A zvolíme bod $X \neq A$ a označíme D průsečík kružnice k s vnitřkem úsečky XC (pokud existuje). Trojúhelník ACD doplníme na lichoběžník $ABCD$ vepsaný kružnici k. Určete množinu průsečíků přímek BC a AD odpovídajících všem takovým lichoběžníkům. (MO 59–A–III–4)

Příklad 16. Bod C probíhá pevný kružnicový oblouk nad tětivou AB. Označme P patu kolmice vedené středem M strany BC na přímku AC. Určete množinu bodů P.

Příklad 17. Uvnitř trojúhelníka ABC je dán bod O tak, že $|\sphericalangle OBA| = |\sphericalangle OAC|$, $|\sphericalangle BAO| = |\sphericalangle OCB|$ a $|\sphericalangle BOC| = 90°$. Určete poměr $|AC| : |OC|$.

(Moskva 2011)

Příklad 18. V trojúhelníku ABC platí $|\sphericalangle ABC| = 120°$. Označme D, E, F průsečíky os vnitřních úhlů u vrcholů A, B, C s protějšími stranami. Ukažte, že $|\sphericalangle DEF| = 90°$.

Návody

1. Nakreslete přímky vodorovně. Jak vysoko leží střed? (Vyjde osa pásu určeného přímkami p, q.)

2. Stejnolehlost. (Vyjde „poloviční“ kružnice vzhledem k bodu O.)

3. Konstuujte tečny ke stejně velkým kružnicím se středy v A a B. (Vyjdou rovnoběžky s AB a přímky skrz střed AB.)

4. Ukažte, že $\triangle ABA'$ je rovnoramenný. (Vyjde kružnice o středu B a poloměru $|BA|$.)

5. Tětiva je kolmá na spojnici svého středu se středem kružnice. (Vyjde Thaletova kružnice nad OP případně její oblouk.)

6. Množina bodů, ze kterých je člověk schopen autobus dostihnout v jistém pevném bodě X, je kruh. Sjednoťte tyto kruhy přes všechny přípustné body X. (Vyjde postupně polorovina, posunutá polorovina, úhel o velikosti 60°.)

7. Vzdálenost středu přepony od vrcholu s pravým úhlem je rovna polovině délky přepony. (Vyjde čtvrtkružnice se středem V a poloměrem $\frac{1}{2}d$.)

8. Ať vnitřní společná tečna v T protne AB v M. Pak $|MA| = |MT| = |MB|$ (stejně dlouhé tečny). (Vyjde kružnice nad průměrem AB bez bodů A, B.)

9. Dokreslete švrky M a N trojúhelníků ACB a ADB. (Vyjde kružnice opsaná trojúhelníku MNB.)

10. Úhly $\sphericalangle XAB$ a $\sphericalangle BCX$ jsou obvodové k téže tětivě ze stejně velkých kružnic, takže mají stejnou velikost. (Vyjde osa usečky AC.)

11. Označme A' obraz A podle osy $\sphericalangle ABC$. Pak $A'D$ a CE jsou stejně dlouhé a svírají týž úhel s BC, tedy D je „nad“ BC přesně o tolik, o kolik je E „pod“.

12. Vyjde vnitřek půlkruhu bez půlkruhů nad průměry určenými koncovými body t a jejím středem.

13. Vyjde po řadě bod, „přitřetěný“ oblouk C ke středu strany AB, oblouk nad AB odpovídající úhlu $180° - \gamma$, oblouk odpovídající úhlu $90° + \frac{1}{2}\gamma$ (resp. oblouk posunutý tak, aby procházel A a B).

14. Mocnost S ke všem takovým kružnicím je stejná ($|SB| \cdot |SC|$), takže druhý průsečík kružnice opsané trojúhelníku ABC a AS je pevný a množina opsišť je přímka.

15. Dokreslete si bod E, průsečík tečen ke k z bodů A, C. Hledanou množinou je sjednocení vnitřků kratších oblouků CE a AE kružnice opsané trojúhelníku EAC.

16. Ukažte, že všechny takové přímky procházejí středem X tětivy kolmé na AB skrz B. Vyjde pak Thaletova kružnice nad AX.

17. Začněte od $\triangle BOC$, nakreslete obraz C' bodu C přes OB a ukažte, že A je bod dotyku tečny z C ke kružnici opsané $\triangle BOC'$. Z mocnosti vyjádřete hodnotu poměru $\sqrt{2}$.

18. Ukažte, že D a F jsou připisiště trojúhelníků AEB a ECB.

Literatura a zdroje

Chtěla bych poděkovat *Štěpánovi Šimšovi*, jehož příspěvek jsem téměř beze změn převzala, jenž poděkoval *Pepovi Tkadlecovi*, jehož příspěvek téměř beze změn převzal.

[1] Nathan Altschiller-Court: *An Introduction to the Modern Geometry of the Triangle and the Circle*, Dover Publications, New York, 2007.
[2] V. V. Prasolov: *Zadachi po planimetrii*, MCCME, Moskva, 2006.
[3] *http://www.problems.ru*

Aritmetické vlastnosti polynomů

Daniil Koževnikov

Abstrakt. V této přednášce si představíme trochu netradiční pohled na polynomy. Budeme je zkoumat nikoliv jako funkce, ale jako objekty s operacemi sčítání a násobení. Jedná se o velmi užitečný nástroj nejen ve vysokoškolské algebře, ale i v olympiádní teorii čísel.

Úvod

Nehledě na to, že se budeme zabývat hlavně polynomy s celočíselnými koeficienty, bude se nám občas hodit brát koeficienty z jiné množiny (typicky $\mathbb{Z}_p, \mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$). Obecně ale dávají takové výrazy smysl nad libovolnou strukturou, kde můžeme sčítat a násobit rozumným způsobem. Takové struktury nazýváme *okruhy*[1].

Definice. Je-li R okruh, pak *polynomem nad* R myslíme výraz $a_0+a_1x+\cdots+a_nx^n$ pro $a_i \in R$. Množinu všech polynomů nad R v proměnné x značíme $R[x]$.

Definice. O $\alpha \in R$ řekneme, že je *kořenem* polynomu p, pokud $p(\alpha) = 0$.

Definice. Je-li $p \in R[x]$ polynom $p(x) = a_0 + \cdots + a_nx^n$ a $a_n \neq 0$, pak n nazveme *stupněm* p, což lze psát jako $\deg(p) = n$. Speciálně definujeme $\deg(0) = -\infty$.

Polynomy můžeme sčítat nebo násobit mezi sebou, takže budou rovněž tvořit okruh. Často se také hodí zkoumat dělitelnosti polynomů:

Definice. Pokud $p = qr$ pro $r \in R[x]$, pak říkáme, že q *dělí* p (pro $p, q \in R[x]$), a zapisujeme stejně jako u čísel: $q \mid p$.

Obzvlášť dobře se polynomy chovají nad *tělesy*, tj. okruhy[2], kde můžeme nenulovými prvky i dělit. Takže například $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{Z}_p$ jsou tělesa, zatímco $\mathbb{Z}$ nebo $\mathbb{Z}_n$ pro složená n nikoliv.

Tvrzení. (dělení se zbytkem) *Pro $u, v \in F[x], v \neq 0$ existují polynomy $q, r \in F[x]$ takové, že $u = qv + r$ a $\deg(r) < \deg(v)$.*

Tvrzení. *$\alpha \in F$ je kořenem $p(x) \in F[x]$ právě když $x - \alpha \mid p(x)$.*

[1] Obecný okruh budeme značit R, od anglického *ring*.

[2] Obecné těleso budeme značit F, od anglického *field*.

Důsledek. *Polynom $p \in F[x]$ stupně $n \geq 0$ má nejvýše n kořenů.*

Úloha 1. Rozmyslete si, že předchozí dvě tvrzení platí i pro $\mathbb{Z}[x]$, pokud se v dělení se zbytkem přidá podmínka, že v je monický.

Úloha 2. Najděte polynom $p \notin \mathbb{Z}[x]$ takový, že $p(x) \in \mathbb{Z}$ pro všechna $x \in \mathbb{Z}$.

Úloha 3. (Bézoutova věta) Definujme největšího společného dělitele polynomů nad tělesem stejně jako pro celá čísla. Dokažte, že pro libovolné $p, q \in F[x]$ existují $a, b \in F[x]$ takové, že $\mathrm{NSD}(p(x), q(x)) = a(x)p(x) + b(x)q(x)$.

Úloha 4. Pokud $p \in \mathbb{Z}[x]$ nabývá hodnoty -1 ve třech různých celých číslech, pak p nemá celočíselný kořen.

Dělitelnosti

Nyní se pojďme soustředit na vlastnosti polynomů spojené s celými čísly. Bezesporu nejdůležitější je následující tvrzení:

Tvrzení. *Pokud $a \neq b \in \mathbb{Z}$ a $p \in \mathbb{Z}[x]$, pak platí $a - b \mid p(a) - p(b)$ (dělitelnost je myšlena nad $\mathbb{Z}$).*

Alternativně lze totéž říct i pomocí kongruencí:

Tvrzení. *Polynomy s celočíselnými koeficienty jsou periodické* $\pmod n$ *pro libovolné přirozené n, tj. $p(x + n) \equiv p(x) \pmod n$ pro celá x.*

Pokud se v úloze vyskytují polynomy a dělitelnost, tak se vám nejspíš alespoň jednou bude dané tvrzení hodit.

Celkem dost se toho dá říct i o racionálních kořenech celočíselných polynomů, a to především díky následujícímu tvrzení:

Tvrzení. (Rational Root Theorem) *Pokud* $\mathrm{NSD}(p, q) = 1$ *a $x = \frac{p}{q}$ je kořenem celočíselného polynomu $f(x) = a_n x^n + \cdots + a_0$, pak platí $p \mid a_0$, $q \mid a_n$.*

Důsledek. *Všechny racionální kořeny monického polynomu ze $\mathbb{Z}[x]$ jsou celé.*

Obecně jsou úlohy, které tvrdí něco o souvislostech mezi polynomy a prvočísly, velmi těžké (většina z nich stále zůstává bez odpovědi). Následující tvrzení poskytuje drobný, ale zase velmi užitečný vhled do této problematiky:

Tvrzení. (Schurova věta) *Pokud je množina prvočíselných dělitelů hodnot $p(x)$ konečná (pro $p \in \mathbb{Z}[x], x \in \mathbb{Z}$), pak p je konstantní polynom.*

Úloha 5. Existuje polynom sudého stupně s lichými koeficienty, který má racionální kořen? (MKS 34–6–4)

Úloha 6. Pokud $ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$ a ad je liché, zatímco bc je sudé, tak nemůžou být všechny kořeny tohoto polynomu racionální.

Úloha 7. Pokud $p \in \mathbb{Z}[x], a, b, c \in \mathbb{Z}$, tak $p(a) = b, p(b) = c, p(c) = a$ nastane jedině pokud $a = b = c$.

Úloha 8. Jsou-li $p, q \in \mathbb{Z}[x]$ nesoudělné, monické polynomy, pak posloupnost $a_n = \mathrm{NSD}(p(n), q(n))$ je periodická.

Úloha 9. Mějme $p \in \mathbb{Z}[x]$ se stupněm alespoň dva. Ukažte, že potom existuje dvojice přirozených čísel (m, n) taková, že kongruence $p(x) \equiv m \pmod{n}$ nemá celočíselné řešení.

Ireducibilita[3]

Podobně jako nám rozklad na prvočísla může ledacos prozradit o celých číslech, tak se i u polynomů občas vyplatí zkoumat rozklady na součin. Obdobou prvočísel se pak stávají tzv. ireducibilní polynomy.

Definice. O polynomu $p \in R[x]$ řekneme, že je *ireducibilní nad* $R[x]$, pokud ho nelze napsat jako součin dvou nekonstantních polynomů z $R[x]$.

Pozor: je vždycky nutné uvádět, nad jakým okruhem myslíme ireducibilitu! Například díky základní větě algebry jsou ireducibilní polynomy nad $\mathbb{C}[x]$ právě ty se stupněm nejvýše jedna, zatímco ireducibilní polynomy nad $\mathbb{Z}[x]$ tvoří mnohem komplikovanější strukturu. Následující tvrzení však ukazuje, že ne vždy je rozdíl tak drastický.

Tvrzení. (Gaussova věta) *Polynom $p(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}[x]$ právě tehdy, je-li ireducibilní nad $\mathbb{Q}[x]$.*

Obecně je ireducibilitu nějakého polynomu poměrně obtížné dokázat. Následující tvrzení ale ukazuje, jak lze šikovně použít $\mathbb{Z}_p[x]$.

Tvrzení. (Eisensteinovo kritérium) *Mějme polynom $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ a prvočíslo p, které splňují:*

(1) $p \nmid a_n$,
(2) $p \mid a_i$ *pro* $i = 0, \ldots, n-1$,
(3) $p^2 \nmid a_0$.

Pak je f ireducibilní nad $\mathbb{Z}[x]$.

Úloha 10. Které z následujících polynomů jsou ireducibilní nad $\mathbb{Q}[x]$?

$$x^4 + 2x + 2, \quad x^4 + 18x^2 + 24, \quad x^3 - 9, \quad x^3 + x^2 + x + 1, \quad x^4 + 1, \quad x^4 + 4$$

Úloha 11. Pro různá $a_1, \ldots, a_n \in \mathbb{Z}$ dokažte, že $(x - a_1)(x - a_2) \ldots (x - a_n) - 1$ je ireducibilní nad $\mathbb{Z}[x]$.

Úloha 12. Pro prvočíslo p dokažte, že je $x^{p-1} + x^{p-2} + \cdots + 1$ ireducibilní nad $\mathbb{Q}[x]$.

Úloha 13. Pro $n > 1$ ukažte, že je $x^n + 5x^{n-1} + 3$ ireducibilní nad $\mathbb{Z}[x]$.
(IMO 1993-1)

[3] Česky nerozložitelnost, kdyby se to roztomiloučkým, chlupaťoučkým tuleňům špatně četlo.

Úloha 14. Jsou-li $f, g \in \mathbb{Z}[x]$ dva monické polynomy ireducibilní nad $\mathbb{Z}[x]$, pro které navíc mají čísla $f(n)$ a $g(n)$ shodné množiny prvočíselných dělitelů pro všechna dost velká n, pak nutně platí $f = g$.

Příklady na procvičení

Úloha 15. Ukažte, že pro libovolný monický polynom $p \in \mathbb{Z}[x]$ se stupněm alespoň 2 existuje nekonečná rostoucí posloupnost celých čísel (x_n) taková, že $p(x_n) \mid p(x_{n+1})$.

Úloha 16. Je-li $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + 1 \in \mathbb{Z}[x]$ polynom s nezápornými koeficienty, splňující navíc $a_i = a_{n-i}$ pro všechna i, pak existuje nekonečně mnoho dvojic celých čísel $x < y$ s $x \mid p(y)$ a $y \mid p(x)$. (iKS 2–N5)

Úloha 17. Jsou-li $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ i $\frac{b}{a} + \frac{c}{b} + \frac{a}{c}$ celá pro celá čísla a, b, c, pak $|a| = |b| = |c|$.

Úloha 18. Definujme posloupnost (x_n) jako $x_0 = 0$, $x_{n+1} = p(x_n)$ pro $p \in \mathbb{Z}[x]$. Ukažte, že pokud $x_n = 0$ pro nějaké $n > 0$, pak $x_1 x_2 = 0$. (Putnam 2000)

Úloha 19. Definujme posloupnost (x_n) jako $x_0 = 0$, $x_{n+1} = p(x_n)$ pro $p \in \mathbb{Z}[x]$ takovou, že $p(n) > n$. Pokud pro každé $m \in \mathbb{N}$ obsahuje tato posloupnost nějaký násobek m, pak platí $p(x) = x + 1$. (Írán TST 2004)

Úloha 20. Je-li $p \in \mathbb{Z}[x]$ nekonstantní, pak polynom $p^k(x) - x$ má nejvýše $\deg(p)$ kořenů (p^k značí k-násobné složení). (IMO 2006-5)

Úloha 21. Mějme funkci $f : \mathbb{Z} \to \mathbb{R}$ takovou, že $|f(n)| < p(n)$ pro nějaký polynom p a $k - l \mid f(k) - f(l)$ pro všechna různá celá k, l. Dokažte, že existuje polynom $q \in \mathbb{R}[x]$ takový, že $f(k) = q(k)$ pro všechna $k \in \mathbb{Z}$. (MKS 34–6–8)

Úloha 22. Buď $a, b, c, d, e, f \in \mathbb{N}$ a $S = a+b+c+d+e+f$. Platí-li $S \mid abc+def$ a $S \mid ab+bc+ca-de-ef-fd$, dokažte, že S musí být složené. (IMO SL 2005-N3)

Návody

3. Děl se zbytkem.

4. $p(x) = (x-a)(x-b)(x-c)q(x) - 1$ pro $q \in \mathbb{Z}[x]$.

6. Ukaž sporem pomocí Rational Root Theorem.

7. $a - b \mid p(a) - p(b)$.

8. Z Bézouta $ap + bq = N$ pro nějaké přirozené N; dokaž $a_{n+N} = a_n$.

9. Kdyby tomu tak nebylo, musí $p(x), \ldots, p(x+n-1)$ dávat různé zbytky po dělení n pro libovolné x; zvol $n = p(x+1) - p(x) > 2$.

13. $\mathbb{Z}_3$ a zkus trochu zobecnit Eisensteina (ale opravdu jen trochu, ať nevezmeš všem současným fyzikům práci na sjednocující teorii).

14. Ireducibilita a různost vynucují nesoudělnost, pak Bézout a Schur dokončí oslavu.

16. Funguje-li dvojice (x, y), pak funguje i $(y, \frac{P(x)}{y})$.

17. Vezmi polynom s kořeny $\frac{a}{b}, \frac{b}{c}, \frac{c}{a}$ a na něj aplikuj Rational Root Theorem.

18. $x - y \mid p(x) - p(y)$; vezmi nejmenší x_i.

19. $x - y \mid p(x) - p(y)$.

20. Jsou-li x, y kořeny, pak platí $|x - y| = |p(x) - p(y)|$; nebo použij předchozí úlohu k tomu, aby stačilo vyřešit jen případ $k = 2$.

21. Pomocí toho, že $\mathrm{NSN}(n, n-1, \ldots, n-d) > kn^{d+1}$ pro nějakou konstantu $k > 0$, dokaž, že se hodnoty f shodují s vhodným polynomem.

22. Zkoumej polynom $(x + a)(x + b)(x + c) - (x - d)(x - e)(x - f)$.

Literatura a zdroje

[1] T. Andreescu, G. Dospinescu: *Problems from the Book*, XYZ Press, 2008.
[2] Filip Sládek: *Aritmetické vlastnosti polynómov*, Hostětín, 2013.
[3] *Art of Problem Solving*, *https://artofproblemsolving.com*

Funkcionální rovnice

Daniil Koževnikov

Abstrakt. Na přednášce si představíme základní metody řešení funkcionálních rovnic. Následuje pak řada příkladů různé obtížnosti na procvičení.

Pár slov úvodem

Co jsou to vlastně ty funkcionální rovnice zač? Podrobně si to vysvětlíme na následujícím příkladu:

Úloha. Nalezněte všechny rostoucí funkce $f : \mathbb{R} \to \mathbb{R}$, které pro všechna $x, y \in \mathbb{R}$ splňují

$$f(x + y) = f(x) + f(y).$$

Můžeme si to představovat jako řešení soustavy rovnic s nekonečně mnoha neznámými (které jsou označeny $f(x)$ pro $x \in \mathbb{R}$). Kvůli tomu, že je neznámých tolik, nemají klasické metody na řešení soustav moc velkou šanci fungovat. Například výše uvedená rovnice je „lineární“[1], takže kdyby se jednalo o konečnou soustavu, uměli bychom ji snadno vyřešit. Přítomností nekonečna však můžeme získat mnohem bohatší strukturu, například bez přidané podmínky „f je rostoucí“ by daná rovnice měla spoustu extrémně divných a divokých řešení. Potřebujeme tedy přijít s nějakými novými metodami, které budou fungovat i na nekonečné soustavy. Pojďme si tedy některé z nich předvést a vysvětlit na příkladech!

Substituční metoda

Nejběžnější metodou řešení funkcionálních rovnic je tzv. substituční metoda. Za tímto slušivým názvem se však neskrývá nic jiného než „dosazujeme do rovnice konkrétní věci a doufáme, že z toho něco vypadne“. Pokud totiž rovnice platí pro libovolné hodnoty x, y, tak jistě platí například i pro konkrétní volbu $x = 6$, $y = 2$. V těch nejjednodušších případech můžeme přímo dostat tvar, ve kterém řešení musí být. Občas dostaneme nějaké informace o jejích hodnotách v konkrétních bodech. Nejčastěji však zbude nějaká jiná funkcionální rovnice, která je s trochou štěstí hezčí nebo jednodušší než ta původní.

[1] Ať už to znamená, co to znamená.

V těžších úlohách se však typicky stává, že postupně dokazujeme různé vlastnosti hledané funkce, které jdou dále dobře využít. Následuje výčet užitečných vlastností funkcí, které je třeba mít na paměti:

Definice. O funkci f (do $\mathbb{R}$) řekneme[2], že je:

(1) *sudá* pokud $f(x) = f(-x)$,
(2) *lichá*, pokud $f(x) = -f(-x)$,
(3) *prostá* (nebo že je f *injekce*), pokud $f(x) = f(y)$ vynucuje $x = y$,
(4) *na* (nebo *surjektivní*), pokud pro každé $y \in \mathbb{R}$ existuje x, pro něž $f(x) = y$,
(5) *bijekce*, pokud je *prostá* i *na*,
(6) *rostoucí*, pokud $f(x) < f(y)$ pro $x < y$,
(7) *klesající*, pokud $f(x) > f(y)$ pro $x < y$,
(8) *periodická s periodou p*, pokud je $x+p$ v definičním oboru a $f(x+p) = f(x)$,
(9) *omezená*, pokud existuje M takové, že $|f(x)| \leq M$.

Existuje několik typů dosazení, které se hodí obzvlášť často. Patří mezi ně například:

(1) $x = 0$ a/nebo $y = 0$, případně další konstanty, které situaci zjednoduší,
(2) prohodit x a y,
(3) $x = y$ a $x = -y$: zbaví nás jednoho stupně volnosti, například z toho vyplyne parita hledané funkce,
(4) něco, co vytvoří soustavu rovnic – občas se může stát, že správná dosazení poskytnou například soustavu lineárních rovnic v $f(A(x,y)), f(B(x,y)), f(C(x,y))$ pro nějaké výrazy A, B, C; pak ji (s)prostě vyřešte!
(5) $y = f(x)$ a naopak. Nelze zapomínat, že $f(x)$ je reálné číslo jako každé jiné, takže ho můžeme do rovnice dosadit.
(6) Dosazení, kterým vyrovnáme dva argumenty: například jestliže na jedné straně rovnice máme $f(y \cdot f(x))$ a na druhé $f(x)$, tak se výrazy při volbě $y = \frac{x}{f(x)}$ vykrátí a rovnice značně zjednoduší.
(7) Krok v důkazu sporem: dokazujete-li například prostotu f, často se vyplatí zkoumat, co by se stalo po dosazení $a \neq b$ s $f(a) = f(b)$ za jednu z proměnných.
(8) Vytváření symetrie: například z $f(x + f(y)) = f(x) + y$ plyne po dosazení $x = f(t)$ symetrická rovnice $f(f(t)+f(y)) = f(f(t))+y$, ze které okamžitě plyne $f(f(y)) + t = f(f(t)) + y$.

Úmluva. Dosazení hodnot $x = a, y = b$ do funkcionální rovnice se většinou pro stručnost a přehlednost značí $[a, b]$.

Úmluva. Není-li v úloze upřesněn definiční obor či obor hodnot, míní se jím $\mathbb{R}$.

[2]V těchto definicích chceme, aby vztah platil pro všechna x, resp. y, z definičního oboru f.

Aplikaci těchto metod si ukážeme na následujících příkladech:

Úloha 1. $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x^2) = x + f(y) - \frac{y}{f(y)}$.

Úloha 2. $f(xy + 1) + f(x + y) = (f(x) + 1)(y + 1)$.

Úloha 3. $f(f(x) + f(y)) = f(x) + y$.

Úloha 4. (varovná) $f(x + f(y)) = f(x) + f(y)^2 + 2xf(y)$.

Úloha 5. (též varovná) $f(x^2 + y) + f(f(x) - y) = 2f(f(x)) + 2y^2$.

Úloha 6. $f : \mathbb{R} \setminus \{0, 1\} \to \mathbb{R}$, $f(x) + f(\frac{1}{1-x}) = x$.

Úloha 7. $f : \mathbb{R}^+ \to \mathbb{R}^+$, $(1 + yf(x))(1 - yf(x + y)) = 1$.

Úloha 8. $f(f(x)) = x$, f je rostoucí.

Cauchyho rovnice a kamarádi

Jedná se nejspíše o nejznámější funkcionální rovnici. Vyplatí se znát ji (i se způsobem řešení). V řešení se totiž objevuje řada užitečných myšlenek: indukce, přechod z $\mathbb{Q}$ do $\mathbb{R}$, ...

Úloha. (Cauchyho rovnice nad $\mathbb{Q}$) $f : \mathbb{Q} \to \mathbb{Q}$, $f(x + y) = f(x) + f(y)$.

Může se zdát, že by nemělo být těžké přejít od řešení nad racionálními čísly k řešení nad reálnými, ale opak je bohužel pravdou. Existuje totiž spousta patologických řešení, jejichž pouhý popis je nad rámec přednášky. Můžeme ale přidat nějaké podmínky, které situaci zachrání:

Úloha. (Cauchyho rovnice nad $\mathbb{R}$) $f(x + y) = f(x) + f(y)$, přičemž známe jednu z následujících vlastností f:

(1) f je monotónní na nějakém intervalu,
(2) f zobrazuje $\mathbb{R}^+$ na $\mathbb{R}^+$,
(3) f je omezená na nějakém intervalu.

Úloha 9. $f(x + y) = f(x)f(y)$, f je rostoucí.

Úloha 10. $f : \mathbb{R}^+ \to \mathbb{R}$, $f(xy) = f(x)f(y)$ a $f(x) > 1$ pro $x > 1$.

Úloha 11. Dokažte, že identita je jediná reálná funkce, zachovávající sčítání i násobení.

Úloha 12. $f(x+y)+f(x)f(y) = f(xy)+f(x)+f(y)$. (Bulharská olympiáda)

Další tipy a triky

Dříve, než se vrhnete na řešení příkladů, tak následuje ještě pár užitečných tipů:

Tipujte řešení
Při hádání můžete postupovat buď intuitivně, nebo do rovnice dosazovat obecné

předpisy (například) pro konstantní, lineární, kvadratickou nebo lineární lomenou funkci. Pokud už nějaká řešení znáte, tento přístup vám může výrazně napomoci: například pokud vyhovuje $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, nemá cenu dokazovat, že f je prostá či monotónní. Někdy nám může řešení poradit dobrou substituci: je-li jediné řešení $f(x) = x + 1$, pak substituce jako $g(x) = f(x) - 1$ či $h(x) = f(x - 1)$ můžou rovnici krásně zpřehlednit.

Dbejte definičního oboru
Pokud řešíte rovnici nad kladnými čísly, nezkoušejte dosazovat nulu (nebo třeba dvojici $(x, -x)$). Naopak definiční obor může někdy něco prozradit o řešení: například je-li to $\mathbb{R} \setminus \{1\}$, pak můžete očekávat jedničku někde ve jmenovateli.

Mějte přehled o tom, co už víte
Při řešení funkcionálek budete typicky dostávat spoustu všemožných vztahů, o kterých si nemůžete být předem jistí, jestli vůbec k něčemu budou. Proto si velmi zjednodušíte život, když budete postupovat co nejsystematičtěji (například zkoušet kombinovat nově získané rovnice s těmi předchozími) a přehledně zapisovat veškerý pokrok, kterého se vám zatím podařilo dosáhnout[3].

Postupujte odzadu
Velmi se hodí včas si uvědomit, že už například jenom stačí dokázat, že f je prostá. Ušetříte si tím spoustu času a pokud se vám náhodou během soutěže nepovede danou vlastnost dokázat, tak můžete rovnici dořešit s tím, že ji budete předpokládat. Pokud se této vlastnosti využívá i ve vzorovém řešení (nebo ji není těžké dokázat), tak i za to dostanete body :).

Dělejte zkoušku ...
... nebo alespoň napište, že jste ji udělali. I soutěžící na IMO kvůli tomu občas zbytečně ztrácí body. Kdybyste si měli z téhle přednášky odnést jednu jedinou věc, tak tohle je ta jediná pravá. Proč je zapotřebí? V průběhu řešení typicky odvozujeme řadu nutných podmínek, které musí funkce f splňovat. Na konci řešení však typicky nevíme nic o tom, jestli jsou tyto podmínky i postačující!

Konečně příklady!

Příklad 13. $f(y - xy) = f(x)y + (x - 1)^2 f(y)$. (CKMO 2017–3)

Příklad 14. $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x)f(y) = f(y)f(xf(y)) + \frac{1}{xy}$. (CKMO 2011–6)

Příklad 15. $f(x^2 + f(x)f(y)) = xf(x + y)$. (MEMO 2017–I1)

Příklad 16. $f : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$, $f(x^2 y f(x)) + f(1) = x^2 f(x) + f(y)$. (MEMO 2015–T2)

Příklad 17. $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x + f(y)) = yf(xy + 1)$. (MEMO 2012–I1)

[3] Ne, že bych to sám dělal. Ale jo, fakt to pomůže.

Příklad 18. $f : \mathbb{R}^+ \to \mathbb{R}^+$, $\frac{f^2(w)+f^2(x)}{f(y^2)+f(z^2)} = \frac{w^2+x^2}{y^2+z^2}$ pro čtveřice čísel splňující $xw = yz$. (IMO 2008–4)

Příklad 19. $f(\lfloor x \rfloor y) = f(x) \lfloor f(y) \rfloor$, kde $\lfloor t \rfloor$ je největší celé číslo, které je větší nebo rovno t. (IMO 2010–1)

Příklad 20. $f : \mathbb{Q}^+ \to \mathbb{Q}^+$, $f(x^2 f(y)^2) = f(x)^2 f(y)$. (IMO SL 2018–A1)

Příklad 21. $(f(x) + f(y))(f(u) + f(v)) = f(xu - yv) + f(xv + yu)$. (IMO 2002–5)

Příklad 22. $f : \mathbb{Q}^+ \to \mathbb{R}$, splňující:

(1) $f(x + y) \geq f(x) + f(y)$,
(2) $f(xy) \geq f(x)f(y)$,
(3) $f(a) = a$ pro nějaké $a > 1$. (IMO 2013–5)

Příklad 23. $f(f(x) + x + y^2) = 2x + f(y)^2$. (iKS 4–A6)

Příklad 24. $f : \mathbb{Q} \to \mathbb{Q}$, $f(x) + f(w) = f(y) + f(z)$ pro aritmetické posloupnosti $x < y < z < w$. (iKS 6–A1, USAJMO 2015–4)

Příklad 25. $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x + f(x)y) = f(x)f(y)$. (Golabova-Schinzelova rovnice)

Návody

13. $[x, 1]$, $[1 - x, y]$ a symetrie.

14. $[1, y]$, $[x, 1]$ a pak zkuste vše vyjádřit s pomocí parametru $c = f(1)$.

15. f má kořen, tak ho dosaďte; pak dokažte prostotu (pro nekonstantní f).

16. Dosazováním jedniček ukažte $|f(1)| = 1$, pak substituujte $g(x) = x^2 f(x)$ a zkoumejte obor hodnot g.

17. Vyrovnejte argumenty a pak pro $y > 1$ zvolte x, aby $y = xy + 1$.

18. $f(x)^2 = f(x^2)$, pak vhodné dosazení dá $f(x) = x$ nebo $f(x) = \frac{1}{x}$ pro každé x; pak třeba zkoušky.

19. Dosaďte nuly a rozeberte pár případů.

20. $f(x^2) = f(x)^2$ a pak dokažte, že $f(x)$ je 2^n-tá mocnina racionálního čísla pro každé $n \in \mathbb{N}$.

21. Různě tam dosazujte nuly, eliminujte konstantní řešení, pak vyjde $f(ab) = f(a)f(b)$, takže stačí monotonie f a lehce obměněný příklad 10.

22. Dokažte, že funkce nabývá jen nezáporných hodnot, z toho odvoďte, že je rostoucí a $f(x) \geq x$.

23. Dokažte $f(0) = 0$, lichost a pak převeďte na Cauchyho rovnici.

24. Přidejte si pátý člen posloupnosti.

25. Vyrovnejte argumenty.

Literatura a zdroje

[1] Vít Musil: *Funkcionální rovnice*, Oldřichov, 2012.

[1] Franta Konopecký: *Funkcionální rovnice*, Rapotín, 2007.

[3] *Art of Problem Solving*, *https://artofproblemsolving.com/*

Úvod do kombinatoriky

Anna Mlezivová

Abstrakt. Příspěvek vysvětluje základní kombinatorické pojmy a obsahuje mnoho lehčích příkladů i s výsledky. Neobsahuje žádnou hlubší teorii.

Kolik různých pořadí může mít závod s pěti účastníky? Kolika způsoby si můžeme ze skříně vybrat oblečení pro dnešní den? Jakou nejdelší abecedu bychom mohli zakódovat v Braillově písmu?

Na tyto a další otázky spolu budeme hledat odpovědi.

Jak různě můžeme vybírat

Jednoho krásného dne se sešlo pět kamarádů - Waldemar, Xaverius, Yvonna, Zdislava a Žibřid.

Potřebujeme-li z nich vybrat jednoho, který musí splnit supertajný úkol, máme zjevně pět možností, koho zvolit. Pokud máme vybrat dva, dělí se nám příklad na různé případy podle toho, jestli nám záleží na jejich pořadí, nebo ne.

V prvním případě dostanou oba vybraní stejný úkol ve stejný čas, nezajímá nás, koho jsme zvolili prvního a koho druhého. Hledáme tedy počet dvojic mezi pěti lidmi, přičemž dvojice Žibřida a Zdislavy je stejná jako dvojice Zdislavy a Žibřida. To zvládneme spočítat třeba výčtem všech možností: k Žibřidovi můžeme přidat postupně Zdislavu, Yvonnu, Xaveria a Waldemara, ke Zdislavě už jen Yvonnu, Xaveria a Waldemara, Yvonna pak s Xaveriem a Waldemarem vytvoří dvě dvojice a Xaverius s Waldemarem nakonec jednu. Dohromady máme $4 + 3 + 2 + 1 = 10$ možných dvojic. Ke stejnému výsledku dojdeme, pokud uvažujeme, že každý má čtyři různé kamarády, s nimiž může utvořit dvojici. To by bylo $5 \cdot 4 = 20$. Jenže, jak již bylo řečeno, je dvojice Žibřida a Zdislavy totožná s dvojicí Zdislavy a Žibřida, a tak jsme tuto (a každou další také) dvojici započítali dvakrát. Vydělením dvěma dostaneme $20/2 = 10$. Můžeme říct, že jsme právě spočítali počet dvoučlenných *kombinací* z pěti prvků.

Pokud začneme jednotlivé kamarády mezi sebou rozlišovat, situace se výrazně změní. Nejprve předpokládejme, že prvnímu vybranému zavážeme oči a druhý ho pak povede po předem vyznačené trase. Kolik máme možností provedení? Pro vybrání prvního pět, pro druhého zbývají jen čtyři, neboť ten vybraný už má zavázané oči a nemůže dělat obojí. Jenže co s těmi čísly teď? Sečíst, vynásobit, umocnit? Pokud

slepý bude Žibřid a povede ho Zdislava, je to úplně jiný příběh, než pokud Zdislavě bude ukazovat cestu Žibřid. Tedy pro každého prvního dobrovolníka existují čtyři druzí dobrovolníci. Máme proto $5 \cdot 4 = 20$ různých dvojic slepec – vodič, což je počet dvoučlenných *variací* z pěti prvků.

Ještě jiný výpočet použijeme, představíme-li si, že vybraný kamarád skupince zatančí čardáš a vrátí se mezi ostatní. Následně vybereme dalšího, který bude chvíli stepovat. Kolika způsoby se tohle mohlo stát? Jako prvního tanečníka můžeme vybrat pět různých lidí. A jako druhého také pět, protože po Žibřidovi můžeme tentokrát vybrat znovu Žibřida. A poučeni z předchozího případu tato čísla vynásobíme, protože pro každého z pěti prvních dobrovolníků existuje pět možných následovníků. Dostaneme $5 \cdot 5 = 25$, neboli počet dvoučlenných *variací s opakováním* z pěti prvků.

Ještě se podíváme na jinou situaci. Naši kamarádi hrají následující hru. Na proužek papíru nakreslí dvě kytičky a následně čtyři svislé čárky (do kytiček se nečárá), podle kterých proužek rozstřihnou. Pak si Xavier vezme první odstřiženou část, Yvonna druhou atd. Zajímá je, kolika způsoby může hra dopadnout, pokud jim jde jen o počet kytiček na jejich papírku. Zamyslíme se nad tím trochu jinak. Podíváme se na původní proužek. Na něm jsou dvě kytičky a čtyři čárky, dohromady šest symbolů. Kolika způsoby můžeme uspořádat šest věcí už umíme spočítat, to je $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2$. Jednotlivé čárky mezi sebou ale nerozlišujeme. Proto výsledek vydělíme počtem všech možných uspořádání čárek, což je $4 \cdot 3 \cdot 2$. Díky dvěma možným uspořádáním kytiček ještě podělíme dvěma. Vyjde nám 15, což je počet dvoučlenných *kombinací s opakováním* z pěti prvků.

Několik matematických pojmů

Ujasníme si názvosloví a pravidlo součtu a součinu mimochodem zmíněné v předchozím odstavci, definujeme si faktoriál a kombinační číslo a zjistíme, k čemu je to dobré.

Tvrzení. (Pravidlo součtu) *Mějme konečné množiny $A_1, A_2, \dots A_n$, které jsou po dvou disjunktní. Potom počet prvků množiny $A_1 \cup A_2 \cup \dots \cup A_n$ je roven součtu počtů prvků množin $A_1, A_2, \dots A_n$.*

Toto pravidlo používáme zcela intuitivně, jak je vidět v následujícím příkladu:

Příklad. Na soustředění jelo jedním vlakem pět účastníků z Prahy, dva z Liberce, čtyři z Karlových Varů a jeden z Plzně. Kolik jich jelo celkem?

Tvrzení. (Pravidlo součinu) *Počet všech uspořádaných n-tic takových, že první složku můžeme vybrat k_1 způsoby, druhou k_2 způsoby, … až n-tou k_n způsoby, je roven $k_1 \cdot k_2 \cdot \dots \cdot k_n$.*

Toto pravidlo jsme už využili při vybírání slepého a vodiče v předchozím textu. Slepého jsme mohli vybrat pěti způsoby, vodiče čtyřmi, dohromady tedy $5 \cdot 4$ způsoby.

Příklad. Kolik je čtyřciferných čísel dělitelných pěti?

Řešení. Na místo tisíců můžeme vybrat devět cifer (nulu ne), na místo stovek deset,

na místo desítek také deset a na místo jednotek jen dvě, nulu nebo pětku. Dohromady máme $9 \cdot 10 \cdot 10 \cdot 2 = 1800$.

Definice. Pojem *k-členná kombinace z n prvků* vyjadřuje počet možností, kterými můžeme vybrat k prvků z n-prvkové množiny, aniž by nám záleželo na pořadí výběru.

Pojem *k-členná variace z n prvků* značí také počet možností, kterými můžeme vybrat k prvků z n-prvkové množiny, ale pokud pořadí výběru zohledníme.

Pojem *permutace na n prvcích* značí počet možných uspořádání n prvků.

Definice. *Faktoriál* n definujeme jako $n! = n \cdot (n-1) \cdot (n-2) \dots 2 \cdot 1$. Speciálně definujeme $0! = 1$.

Tvrzení. *Počet permutací na n prvcích se rovná $n!$.*

Definice. *Kombinační číslo* („en nad ká“) definujeme jako $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Tvrzení. *Počet k-členných kombinací z n prvků vyjadřuje kombinační číslo $\binom{n}{k}$.*

Nejtypičtější příklady

Na konci příspěvku jsou k příkladům uvedeny návody, které mnohdy přímo prozrazují výsledek.

Příklad 1. Kolik existuje sudých čtyřciferných čísel, která nejsou dělitelná pěti? Kolik je pěticiferných čísel, která jsou dělitelná čtyřmi? Kolik je trojciferných čísel, v jejichž desítkovém zápise je každá číslice nejvýš jednou? Kolik je čtyřciferných čísel, v nichž se sudé a liché číslice střídají?

Příklad 2. Kolik úhlopříček má n-úhelník?

Příklad 3. Jakou nejdelší abecedu bychom mohli zakódovat pomocí nejvýše čtyř teček či čárek? A co v Braillově písmu (nejvýše šest vystouplých teček)? (Písmeno může být zakódované i jako nula teček a nula čárek v morseovce a jako žádná vystouplá tečka v Braillu.) A co v semaforu (ukazuje se rukama do osmi různých směrů, přičemž ruce nejsou rozlišitelné a nemohou splývat)?

Příklad 4. K pětadvacátým narozeninám dostala princezna bonboniéru ve tvaru čtverce, kde v každém řádku i sloupci bylo pět bonbonů. Chtěla si jich hned pět sníst, ale tak, aby nevyjedla žádný celý řádek ani sloupec. Kolika způsoby si mohla bonbony vybrat? A co kdyby chtěla z každého řádku i sloupce sníst právě jeden?

Příklad 5. V královské radě tradičně zasedá pět lidí. Do voleb se přihlásilo dvanáct lidí, z toho sedm šlechticů a pět šlechtičen. Protože je království moderní a podporuje rovnost mužů a žen, vyžaduje se, aby v radě byli aspoň dva muži a aspoň dvě ženy. Kolika způsoby může volba dopadnout?

Příklad 6. V jiném královském poradním orgánu zasedá předem neurčený nenulový počet lidí. O tuto funkci mají zájem čtyři muži a tři ženy a tentokrát je jedinou podmínkou pro volbu, aby v radě bylo stejně mužů jako žen. Kolik je možných výsledků?

Příklad 7. Kroketového turnaje se účastní šestnáct lidí. Hrají vždy dvě dvojice proti sobě. Kolika způsoby můžeme všechny hráče rozdělit?

Příklad 8. Elsa každé ráno bezradně kouká do skříně a neví, co si obléct. Vždyť je tak těžké si vybrat! Má patery šaty, troje punčochy, čtyři páry střevíčků, dvě spony do vlasů a dva a půl páru náušnic (jednu ztratila). Z kolika možností každé ráno vybírá, když na sobě podle dvorního protokolu musí mít šaty, punčochy, dva střevíčky, sponu do vlasů a dvě náušnice? V kolika případech na sobě bude mít spárované střevíčky i náušnice? (Střevíčky jsou levé a pravé, kdežto dvě náušnice z páru jsou identické.)

Příklad 9. Dvanáct měsíčků se z nudy stavělo do řady podle stáří, teploty, množství uzrálých jahod a podobných vlastností, až je napadlo: kolika různými způsoby se za sebe můžou postavit? A v kolika z těchto seřazení budou stát vedle sebe měsíce ročního období (tj. mezi měsíci nějakého ročního období nebude stát žádný měsíc jiného ročního období)? A kolika způsoby se můžou seřadit, pokud se červen pohádal s prosincem a odmítají stát vedle sebe?

Další příklady

Příklad 10. Určete počet obarvení šachovnice $1 \times n$ pěti barvami tak, aby žádná dvě sousední políčka neměla stejnou barvu. V kolika vyhovujících případech je šachovnice dvoubarevná nebo má alespoň jedno políčko červené?

Příklad 11. Výrobce hodin se rozzlobil na svůj nudný sortiment a rozhodl se vyrábět nové dokonale kulaté ciferníky, na nichž budou čísla od jedné do dvanácti uspořádána v kruhu libovolně a napsaná tak, aby nebylo poznat, kde je nahoře. Kolikery hodiny bude mít nově v nabídce?

Příklad 12. Milion obyvatel země hlasovalo v zemských volbách o tom, které roční období je nejlepší. Výsledky se udávají ve tvaru uspořádané čtveřice získaných počtů hlasů v pořadí [jaro, léto, podzim, zima]. Kolik možných výsledků volby mají?

Příklad 13. Na dostihových závodech běží pět koní. Pokud jejich čas měříme na celé vteřiny (tedy pokud dva koně doběhnou v jednu vteřinu, doběhli na stejném místě), kolika různých pořadí koní se můžeme dočkat?

Příklad 14. Čísla $1, 2, \ldots, 2017$ dáme do tří barevných kyblíčků: bílého, modrého a červeného. Kolika způsoby můžeme čísla rozházet, pokud žádný z nich není prázdný a dvě po sobě jdoucí čísla nikdy nejsou v témže kyblíčku? (PraSe 30–4–4)

Příklad 15. Kolik vět můžeme vytvořit z šestadvaceti písmen abecedy, pokud každé použijeme právě jednou a za větu považujeme libovolnou posloupnost písmen rozdělenou mezerami (přičemž mezer může být libovolně, ale nikdy ne dvě vedle sebe)?

Příklad 16. Anna dělala zasedací pořádek na svatbu. Pozvala dvacet čtyři hostů, z nichž bylo osmnáct mužů a šest dam. Chtěla vybrat nejlepší posazení hostů tak,

aby u každého kulatého stolu pro čtyři lidi seděla jedna dáma. Z kolika takových vybírala? Když zasedání u stolu jen otočíme, považujeme ho za stejné, podobně nezáleží na tom, u jakého přesně stolu kdo sedí.

V kolika z těchto zasedacích pořádků bude Anna vedle svého ženicha?

Příklad 17. Na velitelském štábu je 6 generálů, 8 plukovníků a 10 majorů. Kolika způsoby se z nich může sestavit osmičlenná prověrková komise? (V armádě je důležitá hodnost, na jméně vůbec nezáleží.) (PraSe 18–5–3)

Příklad 18. Šnek se chce dostat z jednoho rohu krychle do protějšího, avšak plazit se chce pouze po hranách, a to nejvýše po pěti. Kolik takových cest má? Počítáme i ty, během nichž navštíví cíl vícekrát. (PraSe 29–3–4)

Příklad 19. V cukrárně měli n sladkostí, ale každou bohužel jen jednou. Přišli dva mlsouni a nakoupili několik sladkostí, každý aspoň jednu. Kolika způsoby to mohli udělat? (PraSe 25–5–4)

Příklad 20. Do letošní matematické soutěže Náboj se v Praze v kategorii Senioři zaregistrovalo 99 týmů. Organizátoři nyní řeší problém, jak je rozdělit do tří učeben (M1, F1 a F2). Pro jednoduchost předpokládejme, že učebny mají neomezenou kapacitu. Do každé učebny musí být umístěn lichý počet týmů, a navíc nesmí být týmy z tachovského a klatovského gymnázia umístěny současně do učebny F2 (z obou těchto škol je zaregistrovaný právě jeden tým). Kolika způsoby mohou organizátoři rozdělit týmy do místností tak, aby byly všechny uvedené požadavky splněny? (PraSe 32–7–5)

Příklad 21. Slovo DVACETIKORUNY je zajímavé tím, že obsahuje všechny samohlásky v abecedním pořadí. Kolik je všech uspořádání (tj. permutací) písmen takových, že

(1) abecední pořadí samohlásek není dodrženo?
(2) písmena U i V předcházejí C, D, E?
(3) obsahují nejvýše dvě samohlásky bezprostředně za sebou?

(PraSe 18–5–4)

Příklad 22. Mějme čtverečkovaný papír $m \times n$. Kolika způsoby můžeme strany všech čtverečků obarvit pomocí tří barev tak, aby každý čtvereček měl právě dvě strany obarvené jednou barvou a zbývající dvě nějakou jinou jednou barvou? Strany, kterými se sousedící čtverečky dotýkají, považujeme za totožné. (PraSe 33–1–4)

Příklad 23. Kolika způsoby se může posadit deset chlapců a dvanáct děvčat na kolotoč s dvaceti čtyřmi sedadly tak, aby mezi každými dvěma chlapci sedělo aspoň jedno děvče? Posazení, která se liší jen otočením kolotoče, považujeme za totožná. (PraSe 3–6–4)

Návody

1. $9 \cdot 10 \cdot 10 \cdot 4$; $9 \cdot 10 \cdot 10 \cdot 25$; $9 \cdot 9 \cdot 8$; $9 \cdot 5 \cdot 5 \cdot 5$

2. $\frac{n(n-3)}{2}$

3. $2^0 + 2^1 + 2^2 + 2^3 + 2^4$; 2^6; $8 \cdot 7/2$

4. $\binom{25}{5} - 10$; $5!$

5. $\binom{5}{3} \cdot \binom{7}{2} + \binom{5}{2} \cdot \binom{7}{3}$

6. $\binom{4}{1} \cdot \binom{3}{1} + \binom{4}{2} \cdot \binom{3}{2} + \binom{4}{3} \cdot \binom{3}{3}$

7. Do čtveřic: $16!/(4!)^5$, ve čtveřici do dvojic: 3, celkem: $\frac{16! \cdot (3)^4}{(4!)^5}$.

8. $5 \cdot 3 \cdot 4 \cdot 4 \cdot 2 \cdot 8$ (střevíčky jsou levé a pravé, náušnice výčtem možností); $5 \cdot 3 \cdot 4 \cdot 2 \cdot 2$

9. $12!$; $4! \cdot (3!)^4$; $12! - 11! \cdot 2$

10. $5 \cdot 4^{n-1}$; $(5 \cdot 4) + \left(5 \cdot 4^{n-1} - 4 \cdot 3^{n-1}\right) - (2 \cdot 4)$ (dvoubarevné + červené − dvoubarevné červené)

11. $12!/12 = 11!$

12. $\frac{1000003!}{1000000!3!}$.

13. $5! + 4!\binom{5}{2} + 3!\binom{5}{3} + 2!\binom{5}{4} + 1 + 3! \cdot 5 \cdot \frac{\binom{4}{2}}{2} + 2!\binom{5}{2}$;

14. $3 \cdot 2^{2016} - 6$

15. $26! \cdot 2^{25}$ (Mezery se můžou nebo nemusí dát na pětadvacet míst v posloupnosti.)

16. $18!$; $2 \cdot 17!$

17. 42

18. $3 \cdot \frac{5!}{3!} + 6$

19. $3^n - 2 \cdot 2^n + 1$

20. $2 \cdot 3^{97}$

21. $13! - 7!\binom{13}{6}$; $2! \cdot 3! \cdot \binom{13}{5} 8!$; $6! \cdot 7! \cdot 784$

22. $3^{m+n} \cdot 2^{mn}$

23. $\binom{12}{2} \cdot \binom{24}{2} \cdot 9! \cdot 12!$

Literatura a zdroje

Tento příspěvek je z velké části převzatý z přednášky *Báry Kociánové*, které bych tímto chtěla poděkovat.

[1] *PraSečí seriál o kombinatorice*, *http://mks.mff.cuni.cz/archive/27/9.pdf*
[2] Bára Kociánová: *Úvod do kombinatoriky*, Meziměstí, 2017.

Teorie her

Viki Němeček

Abstrakt. V příspěvku se budeme zabývat kombinatorickými hrami s úplnou informací pro dva hráče. Vysvětlíme si základní pojmy, zahrajeme si několik jednodušších her a naučíme se pár klasických triků. Ve druhé části zavedeme SG-funkci a naučíme se sčítat i složitější hry.

Úmluva. Budeme se zabývat pouze hrami, které splňují následující podmínky:

(1) hrají vždy dva hráči proti sobě a pravidelně se střídají v tazích,
(2) pravidla hry určují pro každého hráče v každé pozici možné další tahy,
(3) jsou konečné a skončí vítězstvím jednoho z hráčů,
(4) jsou s úplnou informací (žádné skryté ani simultánní tahy),
(5) jsou bez náhody.

Hra se může ocitnout v konečném počtu různých stavů[1] jednoho z těchto typů:

(1) V – vyhrávající stav = buď existuje takový tah, který změní stav hry na P, nebo se jedná o koncový stav definovaný jako vyhrávající,
(2) P – prohrávající stav = všechny povolené tahy změní stav hry na V.

Počáteční stav je zpravidla jediný, zatímco koncových může být více a o každém by pravidla hry měla vypovídat, zda je V, nebo P.

Poznámka. Hry, které můžou skončit remízou, vůbec neuvažujeme, ale nebyl by problém podobně zavést také neprohrávající a nevyhrávající stavy.

Věta. *Právě jeden z hráčů má vyhrávající strategii.*

Důkaz. Z definice stavů V a P plyne, že pokud se první hráč nachází ve stavu V, tak může zahrát takový tah, že soupeř bude během svého tahu ve stavu P a musí prvního hráče dostat opět do stavu V. Protože je hra konečná, tak tímto opakováním první hráč dosáhne vítězství, a má tedy vyhrávající strategii.

Pokud je ovšem na začátku hra ve stavu P, tak všechny tahy prvního hráče vedou do stavu V a druhý hráč se ocitá v roli prvního v předchozích úvahách, a má tedy vyhrávající strategii.

U každé z následujících her rozhodněte, který z hráčů má vyhrávající strategii.

[1] Stav je jednoznačně popsán pozicí hry a hráčem, který je na tahu.

Příklad 1. (Lámání čokolády) Čokoláda o $m \times n$ čtverečcích se smí lámat rovně po vyznačených čarách. Hráč, který je na tahu, si vybere některý z kousků a jednou ho rozlomí. Hráč, který nemůže nic rozlomit, prohrál.

Časté postupy

U her, v nichž prohraje hráč, který nemůže táhnout, je jedním z častých triků nalezení či vytvoření symetrie. V prvním případě hledáme vyhrávající strategii pro druhého hráče. Pokud se nám podaří nahlédnout, že je hra v nějakém smyslu symetrická a každý tah, který první hráč udělá, může druhý hráč zopakovat podle nalezené symetrie, pak má druhý hráč evidentně vyhrávající strategii.

V druhém, častějším případě sice hra symetrická není, ale dá se na symetrickou převést tahem prvního hráče. Potom je však ve chvíli, kdy se stala hra symetrickou, na tahu druhý hráč, tedy nalezená vyhrávající strategie patří začínajícímu hráči.

Příklad 2. (Lámání čokolády podruhé) Stejná pravidla jako v předchozí hře, ale začíná se s čokoládou $2m \times n$ a nesmí se ulamovat dílky velikosti 1×1.

Příklad 3. (Mince v řadě) V řadě je deset mincí různých hodnot. Hráč, který je na tahu, z jednoho konce řady vezme jednu minci. Vyhrává hráč, který získá největší obnos.

Příklad 4. (Chomp) Čtvercová tabulka čokolády je rozlámaná na kostičky. Kostička v levém horním rohu je otrávená (kdo ji sní, prohraje). Hráč si ve svém tahu vybere kostičku a sní ji, všechny kostičky od ní napravo, všechny kostičky od ní dolů a navíc všechny kostičky, které jsou od ní napravo i dolů. V závislosti na rozměrech určete, kdo zvítězí.

Příklad 5. (Mince na stole) Do kružnice o průměru jeden metr dva hráči střídavě kreslí neprotínající se kruhy o průměru jeden centimetr. Hráč, který první nemá svůj kruh kam nakreslit, prohrál.

Dalším častým trikem je kradení strategií. To lze využít v případě, že se jeden (typicky první) z hráčů může dostat prvním pohybem do nějaké množiny pozic M, a existuje $m \in M$ takové, že se z něj může dále druhý hráč dostat pouze do nějaké (ne nutně vlastní) podmnožiny $M \setminus \{m\}$.

Potom jsou dvě možnosti: buď má hra v pozici m vyhrávající strategii pro hráče, který není na řadě, čímž jsme našli vyhrávající strategii pro začínajícího hráče v původní hře (začne tahem do pozice m a dále hraje podle této strategie). Ve druhém případě existuje strategie pro hráče, který je v pozici m na řadě, a určitě je v ní nějak definovaný první tah. Do stavu, kam vede, se ale evidentně umí dostat začínající hráč v původní hře přímo. Proto má v takové hře vždy vyhrávající strategii první hráč.

Příklad 6. (Čísla v lahvi) V lahvi jsou všechna přirozená čísla od 1 do 16. Hráč, který je na tahu, vyndá z lahve nějaké číslo a všechny jeho dělitele. Prohrává hráč, který nemůže táhnout.

Příklad 7. (Čokoláda počtvrté) Vyřešte znovu úlohu číslo 4 pro obdélníkovou tabulku čokolády.

Příklad 8. (Přičítání dělitele) Začíná se s dvojkou. V jednom kroku hráč přičte k číslu nějakého jeho vlastního dělitele (to je dělitel menší než číslo samotné). Kdo překročí číslo 2011, vítězí. Má začínající hráč vítěznou strategii? A co kdyby ten, kdo překročí 2011, prohrál?

Nim

Nim je kombinatorická hra, na niž je možné spoustu jiných her převést (tuto skutečnost zde nebudeme dokazovat, ale ve skutečnosti lze každá konečná nestranná[2] hra na Nim převést).

Definice. (Nim) V několika hromádkách je určitý počet kamenů. Hráč, který je na tahu, musí odebrat z jedné hromádky alespoň jeden kámen. Vyhrává hráč, který odebere poslední kámen.

Definice. (Nim-součet) *Nim-součtem* čísel x a y je číslo $x \oplus y$, jemuž se běžně říká binární xor. Jedná se o binární sčítání bez přenosu. Např. $21 \oplus 7 = (10101)_2 \oplus (111)_2 = = (10010)_2 = 18$.

Věta. *Ve hře Nim je prohrávající pozice právě ta, v níž se Nim-součet velikostí všech hromádek rovná nule.*

Náznak důkazu. Je potřeba dokázat celkem tři věci. Zaprvé, že v každém koncovém stavu je Nim-součet velikostí všech hromádek roven nule. Zadruhé, že z každého stavu s Nim-součtem rovným nule vedou všechny tahy do stavu s nenulovým Nim-součtem. A konečně za třetí musíme ukázat, že pokud máme nenulový Nim-součet, existuje tah, který ho vynuluje.

První část důkazu je triviální, druhou a třetí si zkuste rozmyslet jako cvičení. Pokud se vám nebude dařit, mezi návody k příkladům najdete radu.

Příklad 9. (Northcottova hra) Pozice ve hře je šachovnice 8×8 s jednou černou a jednou bílou figurkou v každém řádku. Hráč, který je na tahu, táhne figurkou svojí barvy o libovolný počet políček vodorovně směrem k figurce soupeře (nesmí ji přeskočit). Prohrává hráč, který nemůže táhnout.

Příklad 10. (Schody) Na schodišti s 2013 schody je rozmístěno několik mincí (na každém schodě jich může být více, či tam nemusí být žádná). V každém tahu si hráč vybere jeden schod a z něj přesune libovolné množství mincí (nejméně jednu, nejvýše všechny) o schod níže. S mincemi, které se po přesunu z prvního schodu ocitnou na podlaze, už se dál nehraje. Prohrává opět hráč, který nemůže táhnout.

[2]Hra je nestranná, pokud možné tahy z dané pozice jsou pro oba hráče stejné. Tedy například šachy nestranné nejsou, protože jeden hráč může pohybovat jen bílými figurkami, kdežto druhý jen černými.

Sčítání her

Příklad 11. (Šachovnice podruhé) V pravém dolním rohu každé z N šachovnic o rozměrech $a_1 \times b_1, a_2 \times b_2, \ldots, a_N \times b_N$ stojí figurka. Tou se smí v jednom tahu pohnout pouze nahoru, vlevo, nebo šikmo vlevo nahoru, a to buď o jedno, nebo o dvě políčka. Hráč, který je na tahu, si vybere šachovnici a udělá na ní takový tah, aby figurka neopustila šachovnici. Prohrává hráč, který nemůže táhnout.

Definice. (Sprague–Grundyho funkce) *Sprague–Grundyho funkcí* rozumíme funkci g, která každému stavu v přiřadí nejmenší nezáporné celé číslo n takové, že $n \neq g(u)$ pro všechny stavy u, do kterých se dá dostat tahem ze stavu v.

Tvrzení. *Pokud ve hře prohrává hráč, který nemůže táhnout, potom jsou prohrávající právě ty stavy v, pro které $g(v) = 0$.*

Důkaz. Stejně jako v důkazu optimální strategie pro Nim.

Definice. (Sčítání her) *Součtem her* myslíme hru, v níž si hráč může v každém svém tahu vybrat některou z dílčích her a v ní udělat tah. Pro jednoduchost jej budeme definovat pouze pro hry, kde prohrává hráč, který již nemůže táhnout.

Věta. (Sprague, 1936; Grundy, 1939) *Při součtu N her se Sprague–Grundyho funkcemi $g_1, \ldots, g_N$ v počátečních stavech $v_1, \ldots, v_N$ získáme hru s SG funkcí $g(v_1, \ldots, v_N) = g_1(v_1) \oplus g_2(v_2) \oplus \cdots \oplus g_N(v_N)$.*

Příklad 12. (Nim podruhé) Mějme tři hromádky sirek o 9, 10, resp. 14 sirkách. Hráč, který je na tahu, si vybere jednu hromádku a odebere z ní několik sirek. Z první hromádky je možné odebrat 1 až 3 sirky, z druhé 1 až 5 a z té poslední 1 až 7 sirek. Prohrává hráč, který nemůže táhnout.

Příklad 13. (Laskerův Nim) Hra je stejná jako obyčejný Nim, ale navíc lze místo tahu rozdělit hromádku na dvě neprázdné hromádky.

Nějaké další příklady

Příklad 14. (Čtverečky) Na šachovnici $n \times m$, kde n i m jsou alespoň 5, se dva hráči střídají ve vybarvování políček. Jeden vždy vybarví čtverec 2×2, druhý libovolně orientované L-triomino. Žádné políčko nesmí být vybarveno dvakrát a ten, kdo nemůže táhnout, vyhrál. Ukažte, kdo z hráčů má vyhrávající strategii v závislosti na m, n a tom, který z hráčů začíná.

Příklad 15. (Čtvercové piškvorky) Hraje se na čtverečkovaném papíře 10×10. Ve svém tahu nakreslí hráč jeden svůj symbol do nějakého prázdného čtverečku. První hráč se snaží utvořit čtverec 2×2 ze svých symbolů a cílem druhého hráče je mu v tom zabránit.

Příklad 16. (Razítka) Začíná se na šachovnici 8×8. Hráč, který je na tahu, si vybere prázdné políčko a dá na něj razítko. Vybrané políčko musí hranou sousedit s tím předchozím. První hráč může dát razítko, kam chce. Prohrává hráč, který nemůže táhnout.

Příklad 17. (Šachovnice) Na políčku $(x \geq 0, y \geq 0)$ stojí obyčejný šachový kůň. Hráč, který je na tahu, může udělat tah koněm, ale pouze takový, při němž kůň neopustí šachovnici (žádná jeho souřadnice nesmí být záporná) a součet jeho souřadnic klesne. Prohrává hráč, který nemůže táhnout. Jak dopadne hra, v níž bude několik koňů, každý na jiném počátečním políčku, a hráč může táhnout, kolika koni chce, ale vždy alespoň jedním? (MO 60–P–III–2)

Příklad 18. (Kayles) Dva kuželkáři stojí před řadou třinácti kuželek, přičemž druhá kuželka je již shozená. Oba jsou tak šikovní, že svým hodem mohou shodit kteroukoliv kuželku nebo dvojici sousedních kuželek. Vítězem je hráč, který shodí poslední kuželku.

Návody

1. Zkuste si hru párkrát zahrát s malou čokoládou a počítejte, kolik tahů bude celkem hra mít.

4. První hráč vybere kostičku rohem sousedící s otrávenou kostičkou.

5. Je potřeba vyřešit problém, že kruhy, které obsahují střed kružnice, nejde kreslit po dvojicích symetricky podle tohoto středu.

6. Co se stane, když první hráč vytáhne jedničku? A co když ne?

7. Políčko vpravo dole.

8. Vyzkoušejte si prvních pár možných stavů.

Důkaz strategie na Nim. Pro druhou část důkazu si všimneme, že pokud jsme vzali kámen z hromádky, kde bylo n kamenů a po našem tahu jich tam zůstalo m, je Nim-součet nyní právě $m \oplus n$. Pro třetí část si stačí uvědomit, že pokud vezmeme libovolnou hromádku, na níž má počet kamenů jedničku na nejvyšším řádu, kde má jedničku Nim-součet všech hromádek, pak je Nim-součet všech hromádek kromě této menší než velikost této hromádky, takže ji můžeme zmenšit tak, aby se Nim-součet vynuloval.

10. Zkuste si napřed hru vyřešit pro případ, kdy jsou mince pouze na lichých schodech.

17. Nejprve si vyřešte pro jednoho koně. Dejte si pozor na to, že se nejedná o klasický součet her, protože můžeme hrát ve více hrách současně.

Literatura a zdroje

Tato přednáška byla zkopírována ze Zásady, kde jsem ji přednášel také já. Tenkrát byla většina příkladů z tohoto příspěvku převzata od *Filipa Hláska*, který je připravil na soustředění v Hojsově Stráži v roce 2011 a kterému tímto děkuji.

Chinese dumbass notation

Radek Olšák

Abstrakt. Co dělat když dostanete v olympiádě nerovnost a dojde vám zásoba triků? Roznásobit, roznásobit, roznásobit. Většina metod na řešení nerovností dává krátká elegantní řešení. Toto není jedna z nich. Metoda CDN (Chinese dumbass notation) je široce aplikovatelná metoda, která nerovnosti dokazuje bez velkých triků.

Definice. Polynom tří proměnných x, y, z nazveme *homogenní*, pokud pro všechny členy platí, že součet stupňů všech tří proměnných je konstantní v celém polynomu.

Zápis polynomů v CDN

V této přednášce se budeme zabývat zápisem homogenních polynomů ve třech kladných proměnných. Aby byl celý výraz přehlednější, zapíšeme si jejich koeficienty do trojúhelníka. Členy uspořádáme do trojúhelníka o $d+1$ řádcích, kde d je stupeň polynomu. V každém řádku budou všechny členy s pevným stupněm proměnné x a tento stupeň se snižuje odshora dolů. Obdobná vlastnost platí i pro ostatní proměnné – stačí si natočit trojúhelník jiným vrcholem nahoru. Vše objasní následující příklady zápisu polynomů:

$$\begin{pmatrix} [x] \\ [y] \quad [z] \end{pmatrix}, \begin{pmatrix} [x^2] \\ [xy] \quad [xz] \\ [y^2] \quad [yz] \quad [z^2] \end{pmatrix}, \begin{pmatrix} [x^3] \\ [x^2y] \quad [x^2z] \\ [xy^2] \quad [xyz] \quad [xz^2] \\ [y^3] \quad [y^2z] \quad [yz^2] \quad [z^3] \end{pmatrix}, \begin{pmatrix} [x^4] \\ [x^3y] \quad [x^3z] \\ [x^2y^2] \quad [x^2yz] \quad [x^2z^2] \\ [xy^3] \quad [xy^2z] \quad [xyz^2] \quad [xz^3] \\ [y^4] \quad [y^3z] \quad [y^2z^2] \quad [yz^3] \quad [z^4] \end{pmatrix}.$$

Sčítání dvou trojúhelníků, které mají stejnou velikost, funguje po složkách. Tečky značí nuly.

$$\begin{pmatrix} & & \cdot & & \\ & \cdot & & \cdot & \\ \cdot & & -1 & & \cdot \\ 1 & 1 & 1 & 1 \end{pmatrix} + \begin{pmatrix} & & 3 & & \\ & \cdot & & \cdot & \\ 2 & & 2 & & 2 \\ -3 & \cdot & & \cdot & -3 \end{pmatrix} = \begin{pmatrix} & & 3 & & \\ & \cdot & & \cdot & \\ 2 & & 1 & & 2 \\ -2 & 1 & & 1 & -2 \end{pmatrix}.$$

Abychom uměli násobit trojúhelníky mezi sebou, uvědomíme si nejdříve, jak se násobí trojúhelníkem obsahujícím jen jeden nenulový člen. Celý trojúhelník zakořeníme na pozici tohoto členu a pronásobíme jeho velikostí:

$$\begin{pmatrix} \cdot & \\ \cdot & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & & \\ 2 & 3 & \\ 4 & 5 & 6 \end{pmatrix} = 2 \cdot \begin{pmatrix} \cdot & & \\ \cdot & 1 & \\ 2 & 3 & \\ 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} \cdot & & \\ \cdot & 2 & \\ \cdot & 4 & 6 \\ \cdot & 8 & 10 & 12 \end{pmatrix}.$$

Na obecné dva trojúhelníky tedy aplikujeme základní roznásobování:

$$\begin{pmatrix} \cdot & & \\ \cdot & 2 & \\ 3 & \cdot & \cdot \end{pmatrix} \cdot \begin{pmatrix} 1 & \\ 3 & 2 \end{pmatrix} = 2 \begin{pmatrix} \cdot & & & \\ \cdot & 1 & & \\ \cdot & 3 & 2 & \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} + 3 \begin{pmatrix} \cdot & & & \\ \cdot & \cdot & & \\ 1 & \cdot & \cdot & \\ 3 & 2 & \cdot & \cdot \end{pmatrix} = \begin{pmatrix} \cdot & & & \\ \cdot & 2 & & \\ 3 & 6 & 4 & \\ 9 & 6 & \cdot & \cdot \end{pmatrix}.$$

Cvičení. Zapište v trojúhelníkovém tvaru:

- $x^3 + y^3 + z^3$,
- $(x + y + z)^3$,
- $(x + y + z)(x^2 + y^2 + z^2)$,
- $(x + y + z)(xy + yz + zx)$,
- $(x + y)(y + z)(z + x)$,
- $\sum_{cyc}(x + y - z)^2$,
- $\sum_{cyc} x(x + y)(x + z)$,
- $\sum_{cyc}(2x + y + z)^2$,
- $\sum_{cyc}(3x + y)^3$.

Nerovnosti v CDN

Věta. (Vážená AG nerovnost) *Máme několik kladných čísel v trojúhelníku a v místě jejich váženého průměru máme záporně jejich součet (viz příklady). Pak hodnota polynomu, který tento trojúhelník představuje, je nezáporná.*

$$\begin{pmatrix} & 1 & \\ \cdot & -2 & \\ \cdot & \cdot & 1 \end{pmatrix}, \begin{pmatrix} & \cdot & & \\ \cdot & \cdot & & \\ \cdot & \cdot & \cdot & \\ 2 & -3 & \cdot & 1 \end{pmatrix}, \begin{pmatrix} & 1 & & \\ \cdot & \cdot & & \\ \cdot & -3 & \cdot & \\ 1 & \cdot & \cdot & 1 \end{pmatrix}.$$

Věta. (Sudé mocniny) *Další šikovnou, triviálně platnou, nerovností je nerovnost* $(x-y)^{2n}$. *Pro* $n = 1$ *a* $n = 2$ *vypadá následovně:* $(1\ -2\ 1)$, $(1\ -4\ 6\ -4\ 1)$. *První již máme pomocí AG dokázanou, oproti tomu ta druhá pomocí jednoduchého sčítání AG dokázat nelze.*

Věta. (Muirheadova nerovnost) *Máme dva symetrické šestiúhelníky. Jeden tvoří jedničky, druhý mínus jedničky a oba mají stejné těžiště (viz první dva obrazce). Přitom šestiúhelník z mínus jedniček je uvnitř konvexního obalu šestiúhelníka z jedniček. Šestiúhelník může zdegenerovat do trojúhelníka dvojek (třetí ukázka). Pak hodnota polynomu, který tento trojúhelník představuje je nezáporná.*

$$\begin{pmatrix} & & & 1 & & & \\ & & 1 & & 1 & & \\ & -1 & & & & -1 & \\ 1 & & -1 & & -1 & & 1 \\ & -1 & & & & -1 & \\ & & 1 & & 1 & & \end{pmatrix}, \begin{pmatrix} & & & 1 & & & \\ & & 1 & & 1 & & \\ & -1 & & & & -1 & \\ 1 & & -1 & & -1 & & 1 \\ & -1 & & & & -1 & \\ & & 1 & & 1 & & \end{pmatrix}, \begin{pmatrix} & & 2 & & \\ & -1 & & -1 & \\ -1 & & & & -1 \\ & -1 & & -1 & \\ & & 2 & & \end{pmatrix}.$$

Věta. (Schurova nerovnost) *Máme tři stejně velké kosočtverce z jedniček a minus jedniček, které tvoří symetrický útvar jako na obrázku. Kosočtverce se mohou překrývat, v překrytém místě se jejich hodnoty sečtou. Hodnota takto vytvořeného polynomu je nezáporná.*

$$\begin{pmatrix} & & 1 & & \\ & -1 & & -1 & \\ 1 & & & & 1 \\ & -1 & & -1 & \\ & & 1 & & \end{pmatrix}, \begin{pmatrix} & & 1 & & \\ & -1 & & -1 & \\ 1 & & & & 1 \\ & -1 & & -1 & \\ & & 1 & & \end{pmatrix}, \begin{pmatrix} & 1 & & \\ -1 & & -1 & \\ & -1 & & -1 \\ 1 & & -1 & \\ & 1 & & \end{pmatrix}, \begin{pmatrix} & & 1 & & \\ & -1 & & -1 & \\ 1 & & & & 1 \\ & -1 & & -1 & \\ & & 1 & & \end{pmatrix}.$$

Všechny nerovnosti budeme řešit tím způsobem, že se nejdříve zbavíme zlomků vynásobením všech členů jejich společným jmenovatelem. Pracujeme s nerovností, takže je potřeba si hlídat, jestli to, čím násobíme, je kladné nebo záporné. Pokud nerovnost není homogenní, využijeme podmínku a tím ji homogenizujeme. Zapíšeme vše pomocí CDN a roznásobíme. Následně převedeme do tvaru $P \geq 0$ a od tohoto polynomu P odčítáme známé nerovnosti dokud se tím nezbavíme všech záporných členů. Až se nám to povede, je úloha dokázána.

Příklad. (Nesbittova nerovnost) Pro $x, y, z \geq 0$ dokažte:

$$\frac{x}{y+z} + \frac{y}{z+x} + \frac{z}{x+y} \geq \frac{3}{2}.$$

Řešení. Roznásobíme celou nerovnost výrazem $2(y+z)(z+x)(x+y)$, abychom se zbavili zlomků, a dostáváme:

$$2\sum_{cyc} x(x+y)(x+z) \geq 3(x+y)(y+z)(z+x).$$

Zapíšeme v CDN a roznásobíme:

$$2\sum_{cyc}\begin{pmatrix} 1 \\ \cdot\ \ \cdot \end{pmatrix}\begin{pmatrix} 1 \\ 1\ \ \cdot \end{pmatrix}\begin{pmatrix} 1 \\ \cdot\ \ 1 \end{pmatrix} \geq 3\begin{pmatrix} 1 \\ 1\ \ \cdot \end{pmatrix}\begin{pmatrix} \cdot \\ 1\ \ 1 \end{pmatrix}\begin{pmatrix} 1 \\ \cdot\ \ 1 \end{pmatrix},$$

$$\sum_{cyc}\begin{pmatrix} 2 \\ 2\ \ 2 \\ \cdot\ \ 2\ \ \cdot \\ \cdot\ \ \cdot\ \ \cdot\ \ \cdot \end{pmatrix} \geq 3\begin{pmatrix} \cdot \\ 1\ \ 1 \\ 1\ \ 2\ \ 1 \\ \cdot\ \ 1\ \ 1\ \ \cdot \end{pmatrix},$$

$$\begin{pmatrix} 2 \\ 2\ \ 2 \\ 2\ \ 6\ \ 2 \\ 2\ \ 2\ \ 2\ \ 2 \end{pmatrix} \geq \begin{pmatrix} \cdot \\ 3\ \ 3 \\ 3\ \ 6\ \ 3 \\ \cdot\ \ 3\ \ 3\ \ \cdot \end{pmatrix},$$

$$\begin{pmatrix} 2 \\ -1\ \ -1 \\ -1\ \ \ 0\ \ -1 \\ 2\ \ -1\ \ -1\ \ \ 2 \end{pmatrix} \geq 0.$$

Dostali jsme tedy tvar, který potřebujeme. Zbývá najít, jak tuto nerovnost zapsat jako součet známých nerovností. To uděláme postupným odčítáním známých nerovností. Pokud se tímto odčítáním zbavíme všech záporných čísel, tak jsme nerovnost zapsali jako součet platných nerovností, jinými slovy platí. Můžeme rovnou říct, že tato nerovnost je přímo speciálním případem Muirheadovy nerovnosti, ale ukážeme si, jak ji dokázat pomocí AG. Využijeme následující AG k eliminaci jedné mínus jedničky:

$$\begin{pmatrix} \cdot \\ \cdot\ \ \cdot \\ \cdot\ \ \cdot\ \ \cdot \\ \frac{1}{3}\ \ \cdot\ \ -1\ \ \frac{2}{3} \end{pmatrix}.$$

Tento trojúhelník symetricky sečteme. Tím jsme se zbavili všech šesti mínus jedniček, takže jsme zapsali nalezený polynom jako součet nezáporných polynomů, tedy i tento polynom musí být nezáporný. □

Cvičení. Dokažte o následujících polynomech, že jsou nezáporné:

$$\begin{pmatrix} \cdot \\ 4\ \ 4 \\ -1\ \ 2\ -1 \\ -6\ -2\ -2\ -6 \\ -1\ -2\ \ 6\ -2\ -1 \\ 4\ \ 2\ -2\ -2\ \ 2\ \ 4 \\ \cdot\ \ 4\ -1\ -6\ -1\ \ 4\ \ \cdot \end{pmatrix}, \quad \begin{pmatrix} 3 \\ \cdot\ -4 \\ -4\ \ 3\ \ \cdot \\ 3\ \ \cdot\ -4\ \ 3 \end{pmatrix}, \quad \begin{pmatrix} 50 \\ 230\ \ 230 \\ 115\ \ 160\ \ 115 \\ 10\ -336\ -336\ \ 10 \\ 115\ -336\ -714\ -336\ \ 115 \\ 230\ \ 160\ -336\ -336\ \ 160\ \ 230 \\ 50\ \ 230\ \ 115\ \ 10\ \ 115\ \ 230\ \ 50 \end{pmatrix}.$$

Úlohy

Poznámka. Ve všech úlohách předpokládáme $x, y, z \geq 0$.

Dokažte následující nerovnosti.

Úloha 1. $(x+y-z)(y+z-x)(z+x-y) \leq xyz$.

Úloha 2. $(xy+yz+zx)^2 \geq 3xyz(x+y+z)$.

Úloha 3. $\frac{x^3}{yz}+\frac{y^3}{zx}+\frac{z^3}{xy} \geq x+y+z$.

Úloha 4. $(x+y+z)^2+\frac{9xyz}{x+y+z} \geq 4(xy+yz+zx)$.

Úloha 5. $\frac{xy}{x+y}+\frac{yz}{y+z}+\frac{zx}{z+x} \leq \frac{3(xy+yz+zx)}{2(x+y+z)}$.

Úloha 6. $\frac{x^2}{y+z}+\frac{y^2}{z+x}+\frac{z^2}{y+x} \geq \frac{x+y+z}{2}$.

Úloha 7. (Česko-slovensko-polské střetnutí) $\frac{x}{y+2z}+\frac{y}{z+2x}+\frac{z}{x+2y} \geq 1$.

Úloha 8. $8(x^3+y^3+z^3)^2 \geq 9(x^2+yz)(y^2+zx)(z^2+xy)$.

Úloha 9. $\sum_{cyc} \frac{x^2+y^2}{z} \geq 2(x+y+z)$.

Úloha 10. $\sum_{cyc} \frac{x^2-z^2}{y+z} \geq 0$.

Úloha 11. $(x+2y+z)(x+y+z)^2 \geq 4(x+y)(y+z)(z+x)$.

Úloha 12. $xy+\frac{y}{x}+\frac{x}{y} \geq x+y+1$.

Úloha 13. $\frac{yz}{2x+y+z}+\frac{zx}{2y+z+x}+\frac{xy}{2z+x+y} \leq \frac{1}{4}(x+y+z)$.

Úloha 14. Pro $x+y+z=1$: $x^3+y^3+z^3+6xyz \geq \frac{1}{4}$.

Úloha 15. $(x^2y+y^2z+z^2x)(x^2z+z^2y+y^2x) \geq 9x^2y^2z^2$.

Úloha 16. (USAMO 1997) $\sum_{cyc} \frac{1}{x^3+y^3+xyz} \leq \frac{1}{xyz}$.

Úloha 17. (IMO 1984/1) Pro $x+y+z=1$: $0 \leq xy+yz+zx-2xyz \leq \frac{7}{27}$.

Úloha 18. (Iran 1996) $(xy+yz+zx)(\frac{1}{(x+y)^2}+\frac{1}{(y+z)^2}+\frac{1}{(z+x)^2}) \geq \frac{9}{4}$.

Úloha 19. Pro $x+y+z=3$: $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}-1 \geq 2\sqrt{\frac{x^2+y^2+z^2}{3xyz}}$.

Úloha 20. (IMO 2002/2) Pro $xyz=1$: $(x-1+\frac{1}{y})(y-1+\frac{1}{z})(z-1+\frac{1}{x}) \leq 1$.

Úloha 21. (Turnaj měst 1997) Pro $xyz=1$: $\frac{1}{x+y+1}+\frac{1}{y+z+1}+\frac{1}{z+x+1} \leq 1$.

Úloha 22. (IMO 2005) Pro $xyz=1$: $\sum_{cyc} \frac{x^5-x^2}{x^5+y^2+z^2} \geq 0$.

Úloha 23. (IMO 1995) Pro $xyz=1$: $\sum_{cyc} \frac{1}{x^3(y+z)} \geq \frac{3}{2}$.

Úloha 24. Pro $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=x+y+z$: $\sum_{cyc} \frac{1}{(2x+y+z)^2} \leq \frac{3}{16}$.

Úloha 25. Pro $x+y+z=1$: $(\frac{1}{x}+1)(\frac{1}{y}+1)(\frac{1}{z}+1) \geq 64$.

Úloha 26. (Japan TST 2004) Pro $x+y+z=1$: $\frac{1+x}{1-x}+\frac{1+y}{1-y}+\frac{1+z}{1-z} \leq \frac{2x}{y}+\frac{2y}{z}+\frac{2z}{x}$.

Návody

12. Přidejte třetí proměnnou a homogenizujte pomocí $z = 1$.

14. Nahraďte podmínkou jedničku na pravé straně. Roznásobte a nelekněte se, že nesedí součet koeficientů.

19. Nahraďte $1 = \frac{3}{x+y+z}$, umocněte na druhou a bijte.

20. Homogenizujte pomocí $(xyz)^{\frac{1}{3}} = 1$. Pokud se děsíte necelých exponentů, substituujte $x^3 = a$, $y^3 = b$, $z^3 = c$.

21. Homogenizujte pomocí $(xyz)^{\frac{1}{3}} = 1$. Pokud se děsíte necelých exponentů, substituujte $x^3 = a$, $y^3 = b$, $z^3 = c$.

23. Homogenizujte pomocí $(xyz)^{\frac{4}{3}} = 1$. Substituujte třetí mocniny. Kdopak by se 24. stupně bál.

24. Zbavte se zlomků, stupně stran se liší o 2. Využijte podmínku ve tvaru: $xy + yz + zx = x^2yz + xy^2z + xyz^2$.

Literatura a zdroje

[1] Brian Hamrick: *The Art of Dumbassing*, *https://www.tjhsst.edu/~2010bhamrick/files/dumbassing.pdf*

[2] *https://www.quora.com/What-is-Chinese-Dumbass-Notation*

[3] Evan Chen: *Supersums of Square-Weights (SOS) – A Dumbass Perspective*, *http://web.evanchen.cc/handouts/SOS_Dumbass/SOS_Dumbass.pdf*

[4] Matěj Konečný: *Dvě techniky na nerovnosti*, *iksko.org/files/sbornik5.pdf*

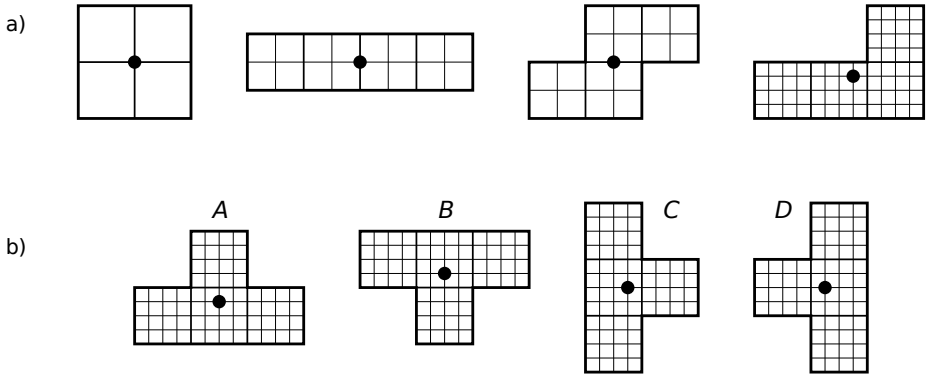
Těžiště v kombinatorice

Radek Olšák

Abstrakt. Příspěvek se zabývá řešením pokrývacích problémů s využitím těžiště a jeho vlastností. Pokud již znáte metodu obarvování, těžiště vám dá alternativní způsob, jak nad takovými problémy uvažovat.

Kombinatorické úlohy, ve kterých máme danými útvary pokrýt určitou plochu, lze elegantně řešit pomocí obarvování. Zde se naučíme tytéž úlohy řešit jinak. Využijeme vlastností těžiště, čímž se řešení úlohy převede na jiný, jednodušší problém. Uvidíme, že zpravidla dojdeme k triviálnímu sporu typu „sudé není liché“ nebo naopak.

Obvykle se plocha pokrývá kostičkami, které se odborně nazývají k-mina nebo polymina (např. trimina, tetramina, pentamina). V následujících úlohách se využívají především tetramina. Těžiště všech existujících tetramin jsou znázorněna na obrázku:



O těžišti

Jedna z hlavních vlastností těžiště, kterou budeme využívat, je

$$m_1\overrightarrow{OX_1} + \cdots + m_n\overrightarrow{OX_n} = \overrightarrow{0},$$

kde O je těžiště bodů $X_1, \ldots, X_n$ s hmotnostmi $m_1, \ldots, m_n$. V našem případě body $X_1, \ldots, X_n$ představují těžiště tetramin, jež mají ale všechny stejnou „hmotnost“, proto platí:

$$\overrightarrow{OX_1} + \cdots + \overrightarrow{OX_n} = \overrightarrow{0}.$$

Jak začít

Než začneme úlohu řešit, rozmyslíme si, kde je těžiště daných kostiček a plochy, kterou pokrýváme. Potom si oba objekty „přeškálujeme“ tak, aby obě těžiště ležela v mřížových bodech (viz obrázek) a dílčí malé kostičky obou objektů měly stejný rozměr. Pak do těžiště pokrývaného útvaru položíme střed souřadného systému. Jednotková vzdálenost bude délka strany malé dílčí kostičky. Potom součet všech x-ových i y-ových souřadnic těžišť k-min musí být roven 0.

Příklady

Příklad 1. Čtvercová podlaha je pokryta dlaždicemi typu 2×2 a 1×4. Jedna dlaždice se ale rozbila. K dispozici máme dlaždici druhého typu. Ukažte, že není možné dlaždice přeskládat tak, aby podlahu pokryly.

Příklad 2. Dokažte, že šachovnici 10×10 nelze pokrýt 25 tetraminy typu T.

Příklad 3. Dokažte, že šachovnici 10×10 nelze pokrýt 25 tetraminy typu I.

Příklad 4. Dokažte, že šachovnici 8×8 nelze pokrýt 15 tetraminy typu T a jedním tetraminem typu O.

Příklad 5. Máme šachovnici $n \times n$ bez rohových polí. Pro jaká n lze šachovnici pokrýt tetraminy typu L?

Příklad 6. (Prasolov) Středově souměrný útvar je složený z n tetramin L a k tetramin I. Dokažte, že n je sudé.

Příklad 7. Čtverec 7×7 je pokryt šestnácti dílky 3×1 a jedním 1×1. Kde všude může být dílek 1×1?

Příklad 8. (Dobosevych) Máme šachovnici $n \times n$ pokrytou tetraminy typu T. Nechť a, b, c, d jsou počty tetramin všech čtyř možných orientací (dle obr. b) označených A, B, C, D. Dokažte, že $4 \mid (a + b - c - d)$.

Příklad 9. Lze nějakou středově souměrnou plochu pokrýt tetraminy typu L a triminy typu „roh“? Polymina je zakázáno otáčet či převracet.

Literatura a zdroje

Chtěl bych poděkovat *Monče Pospíšilové*, jejíž příspěvek jsem takřka beze změny převzal.

[1] Harun Šiljak: *Centroids and Tiling Problems*, Mathematical reflections 5, 2009.

[2] Arthur Engel: *Problem-Solving Strategies*, Springer, UK, 1998.

Lineární algebra

Terka Poláková

Abstrakt. Příspěvek si klade za cíl seznámit čtenáře se základními definicemi a pojmy týkajících se matic.

Příspěvek se sice věnuje maticím, ale předtím než si matice zadefinujeme, podívejme se na příklad toho, k čemu se matice můžou hodit. S jejich pomocí můžeme třeba reprezentovat soustavu lineárních rovnic.

Příklad. Soustavu lineárních rovnic

$$\begin{aligned} x + 2y + 3z &= 4, \\ 2x + y &= -1, \\ -x + 2z &= 0, \end{aligned}$$

lze reprezentovat maticí

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 2 & 1 & 0 & -1 \\ -1 & 0 & 2 & 0 \end{array}\right).$$

Definice. Reálnou (resp. komplexní) *maticí A typu $m \times n$* rozumíme tabulku o m řádcích a n sloupcích, jejíž políčka obsahují reálná (resp. komplexní) čísla. Těmto políčkům říkáme prvky matice A a prvek v i-tém řádku a j-tém sloupci značíme a_{ij}.

Matici je možné vynásobit libovolným číslem t, výsledkem bude matice, jejíž prvky budou rovny původním prvkům vynásobeným o dané číslo t.

Definice. *Nulovou maticí* typu $m \times n$ rozumíme matici, která má všechny prvky rovné 0. Značíme ji $0_{m\times n}$.

Definice. *Jednotkovou maticí* typu $m \times m$ rozumíme čtvercovou matici, která má na diagonále 1 a mimo diagonálu 0 (diagonálou myslíme hlavní diagonálu z levého horního rohu). Značíme ji I_m.

Definice. (Sčítání matic) Mějme matice A a B typu $m \times n$. Pak jejich *součtem* je matice C typu $m \times n$, pro kterou platí $c_{ij} = a_{ij} + b_{ij}$.

Definice. *Vektory* budeme nazývat matice typu $1 \times n$, resp. $n \times 1$.

Definice. Mějme vektory $v_1, v_2, \ldots, v_n$. Pak řekneme, že vektor u je *lineární kombinací* těchto vektorů s koeficienty $a_1, a_2, \ldots, a_n$, když $u = \sum_{i=1}^{n} a_i v_i$ pro nějaká reálná čísla a_i.

Definice. (Násobení matic po prvcích) Mějme matici A typu $m \times n$ a matici B typu $n \times p$. Pak *součinem* matic $A \cdot B$ rozumíme matici C typu $m \times p$, kde $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.

Pro násobení matic se používají ještě následující dva způsoby:

(1) (Násobení matic sloupcovým pohledem) Je-li $A = (a_{ij})$ matice typu $m \times n$ a $B = (b_{jk})$ matice typu $n \times p$, pak pro každé $j = 1, 2, \ldots, n$ platí, že j-tý sloupec v součinu AB je lineární kombinací sloupců matice A s koeficienty j-tého sloupce matice B.

(2) (Násobení matic řádkovým pohledem) Je-li $A = (a_{ij})$ matice typu $m \times n$ a $B = (b_{jk})$ matice typu $n \times p$, pak pro každé $i = 1, 2, \ldots, m$ se i-tý řádek v součinu AB rovná lineární kombinaci řádků matice B s koeficienty v i-tém řádku matice A.

Cvičení. Následující příklady na násobení matic spočítejte s použitím všech tří způsobů. Rozmyslete si, kterým způsobem se Vám násobí nejlépe.

$$\begin{pmatrix} 5 & 4 & 3 \\ 2 & 7 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 8 \\ 14 \end{pmatrix}, \begin{pmatrix} 4 & 2 & 3 \\ 1 & 3 & 2 \\ 5 & 8 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 15 & 9 \\ 5 & 10 & 2 \\ 4 & 3 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 8 \\ 1 \end{pmatrix},$$

$$\begin{pmatrix} 12 \\ 8 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 2 & 3 \\ 1 & 3 & 2 \\ 5 & 8 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 15 & 9 \\ 5 & 10 & 2 \\ 4 & 3 & 5 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 8 \\ 1 \end{pmatrix}$$

Liší se výsledek třetího a čtvrtého příkladu, a pokud ano, jak? Je násobení matic komutativní (násobení dvou matic je komutativní, pokud platí $A \cdot B = B \cdot A$)?

Tvrzení. (Asociativita a komutativita sčítání matic) *Máme-li matice A, B a C typu $m \times n$. Potom platí*

(1) $A + B = B + A$,
(2) $(A + B) + C = A + (B + C)$.

Cvičení. Jsou dány následující matice A, B a C

$$A = \begin{pmatrix} 12 & 45 & 3 \\ 31 & 23 & 7 \\ 52 & 64 & 4 \end{pmatrix}, B = \begin{pmatrix} 115 & 153 & 9 \\ 54 & 104 & 72 \\ 435 & 345 & 35 \end{pmatrix}, C = I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Spočtěte $A + B$, $B - A$, $A - C$, $(A - C) + B$.

Tvrzení. (Asociativita násobení matic) *Máme-li matice A typu $m \times n$, B typu $n \times p$ a C typu $p \times q$, potom platí*

(1) $(A \cdot B) \cdot C = A \cdot (B \cdot C)$.

Cvičení. Co musí splňovat matice A a B, aby byly definovány oba součiny $A \cdot B$ i $B \cdot A$? Najděte několik různých dvojic matic A a B, aby navíc platila rovnost $A \cdot B = B \cdot A$.

Soustavy lineárních rovnic

Nyní se vrátíme k motivačnímu příkladu ze začátku

$$\begin{aligned} x + 2y + 3z &= 4, \\ 2x + y &= -1, \\ -x + 2z &= 0. \end{aligned}$$

Levou stranu můžeme reprezentovat maticí A, pravou stranu vektorem b. Dohromady takto celou soustavu reprezentujeme rozšířenou maticí soustavy $(A|b)$[1]:

$$(A|b) = \left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 2 & 1 & 0 & -1 \\ -1 & 0 & 2 & 0 \end{array}\right).$$

Vyřešit soustavu lineárních rovnic je potom ekvivalentní s nalezením všech vektorů x, které splňují rovnici $A \cdot x = b$. Vektor x je v tomto případě

$$x = \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Shrnuto v maticovém zápisu má naše soustava lineárních rovnic tvar

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 0 \\ -1 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 4 \\ -1 \\ 0 \end{pmatrix}.$$

Cvičení. Najděte všechny vektory x splňující rovnici

$$\begin{pmatrix} 1 & 2 & 2 \\ 2 & 0 & 1 \\ 1 & 1 & 2 \end{pmatrix} \cdot x = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

Definice. *Elementární řádkové úpravy* rozšířené matice soustavy jsou

(1) prohození dvou řádků matice,
(2) vynásobení jednoho z řádků matice nenulovým číslem,
(3) přičtení libovolného násobku jednoho řádku k jinému řádku.

[1]Touto maticí rozumíme matici A, kterou vpravo rozšíříme sloupcem tvořeným vektorem b. Neboli splácneme dohromady matici A s vektorem b.

Poznámka. Obdobné úpravy fungují i pro samotnou soustavu rovnic a pro nás je důležité, že nemění množinu řešení soustavy.

Cvičení. Zamyslete se, jestli lze z elementárních řádkových úprav složit algoritmus, který soustavu vyřeší. Pokud ano, jak bude algoritmus vypadat?

Definice. *Elementární matice* je matice, která vznikne z jednotkové matice jednou elementární řádkovou úpravou.

Cvičení. Zkuste najít elementární matice E_1, E_2, E_3 typu 3×3 takové, že pokud jimi vynásobíme matici A zleva, tak docílíme:

(1) prohození prvního a druhého řádku,
(2) vynásobení druhého řádku číslem 5,
(3) přičtení trojnásobku druhého řádku k třetímu řádku,

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 0 \\ -1 & 0 & 2 \end{pmatrix},$$

$$E_1 \cdot A = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 3 \\ -1 & 0 & 2 \end{pmatrix}, E_2 \cdot A = \begin{pmatrix} 1 & 2 & 3 \\ 10 & 5 & 0 \\ -1 & 0 & 2 \end{pmatrix}, E_3 \cdot A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 0 \\ 5 & 3 & 2 \end{pmatrix}.$$

Definice. *Lineární zobrazení* je takové zobrazení $f : \mathbb{R}^m \to \mathbb{R}^n$, pro které platí $f(u+v) = f(u)+f(v)$ a $f(tu) = tf(u)$ pro reálné číslo t a vektory u a v. Ke každému lineárnímu zobrazení $f : \mathbb{R}^m \to \mathbb{R}^n$ existuje jednoznačně určená matice A typu $n \times m$ taková, že pro všechny $v \in \mathbb{R}^m$ platí $f(v) = Av$.

Cvičení. Nalezněte matice typu 2×2 těchto lineárních zobrazení: identické zobrazení, osová souměrnost, středová souměrnost, stejnolehlost. Na co se při nich zobrazí čtverec s vrcholy $(0,0), (0,1), (1,1), (1,0)$?

Cvičení. Nalezněte geometrický význam lineárního zobrazení určeného maticí

$$\begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}.$$

Inverzní matice

Definice. Je-li A matice typu $m \times n$, X matice typu $n \times m$, pak X nazýváme *inverzní maticí zprava* k matici A, pokud platí $A \cdot X = I_m$, matice A se v tom případě nazývá *invertovatelná zprava*.

Definice. Je-li A matice typu $m \times n$, X matice typu $n \times m$, pak X nazýváme *inverzní maticí zleva* k matici A, pokud platí $X \cdot A = I_n$, matice A se v tom případě nazývá *invertovatelná zleva*.

Definice. Jsou-li A a X čtvercové matice typu $n \times n$, pak X nazýváme *inverzní maticí* k matici A, pokud platí $X \cdot A = A \cdot X = I_n$, matice A se v tom případě

nazývá *invertovatelná matice*. Je-li A invertovatelná matice, pak matici inverzní k A značíme A^{-1}.

Cvičení. Musí inverzní matice existovat ke každé matici A? Je A^{-1} (pokud existuje) určena jednoznačně?

Cvičení. Najděte matici inverzní zprava k matici

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 9 & 8 \end{pmatrix}.$$

.

Cvičení. Najděte matici inverzní zleva k matici

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}.$$

Cvičení. Najděte inverzní matici k matici

$$\begin{pmatrix} 1 & 3 \\ 2 & 9 \end{pmatrix}.$$

.

Literatura a zdroje

[1] Libor Barto, Jiří Tůma: *Lineární algebra*
[2] Martin „E.T.“ Sýkora: *Matice ze všech stran*, Zásada, 2017.

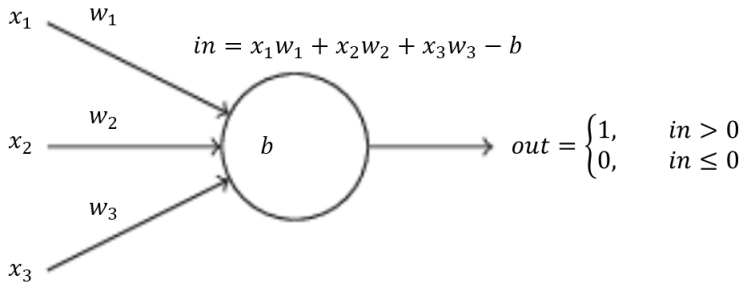
Neuronové sítě

Marian Poljak

Abstrakt. Dnešní svět se stále více točí kolem *machine learningu*. Neuronové sítě jsou aktuálně nástrojem, který dosahuje *state-of-the-art* výsledků v mnoha oborech. V této přednášce si ukážeme základy – jak neuronové sítě fungují a pomocí jakých metod dovedou vstřebávat a zobecňovat obrovské množství informací.

Neuron

Co je to vlastně neuronová síť? Neuronové sítě jsou inspirovány lidským mozkem, ve kterém máme spoustu neuronů – tyto neurony se mohou *aktivovat*, dostanou-li správný impulz od nějaké množiny s nimi propojených neuronů. Je-li neuron aktivován, naopak jiné množině neuronů impulz odešle. Právě tímto procesem vznikají nesmírně komplexní procesy např. v lidském těle. Tak proč to nezkusit v počítačích?



Na obrázku vidíme jeden neuron se třemi *vstupy* a jedním *výstupem*. Jak by mohl přenos informací fungovat? Dejme tomu, že každý vstup je buď aktivovaný, nebo ne, čemuž přiřadíme binární hodnotu jedničky a nuly (formálně $x_1, x_2, x_3 \in \{0, 1\}$). Ještě přiřadíme každému propojení *váhu*, čímž se snažíme vyjádřit, jak moc je toto propojení „silné“ – důležité pro neuron ($w_1, w_2, w_3 \in \mathbb{R}$). Neuron nyní dostane od vstupů vážený průměr in, který závisí na vstupech a na síle (váze) konexí.

Nyní bychom chtěli rozhodnout, zda-li je tento „impulz“ dostatečný pro aktivaci našeho neuronu. Přidáme neuronu ještě další vlastnost $b \in \mathbb{R}$, zvanou *bias*, která vyjadřuje, jak „těžké“ je neuron aktivovat. Neuron nyní vyšle signál $out \in \{0, 1\}$

podle toho, jestli se impulzu *in* povedlo bias překonat – pokud ano, neuron vyšle jedničku a je *aktivovaný*.[1]

Tomuto modelu neuronu se říká *perceptron*.

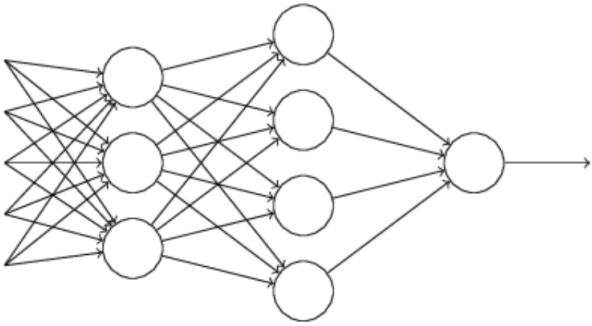
Příklad. Zkusme si z tohoto snadného modelu udělat rozhodovací proces:

$$\begin{aligned} x_1 &= \text{„Hedvika by se mnou šla na zmrzku.“} \\ x_2 &= \text{„Venku zrovna prší.“} \\ x_3 &= \text{„Zmrzka mi chutná.“} \\ out &= \text{„Půjdu na zmrzku!“} \end{aligned}$$

Každé z těchto tvrzení může být buď nepravda (0) nebo pravda (1). Určete váhy w_1, w_2, w_3 a bias b tak, aby se rozhodlo, že s Hedvikou se rozhodneme jít na zmrzku vždycky a bez ní jen tehdy, pokud zmrzka nám chutná a neprší.

Struktura neuronové sítě

Vidíme, že už jeden neuron je schopný dělat zajímavá rozhodnutí. Co takhle postavit celou strukturu neuronů? Například na následujícím obrázku je vstupní vrstva, která nastavuje neurony v první vrstvě. Výstup neuronů první vrstvy je vstupem druhé vrstvy neuronů, která zase svými aktivacemi určí aktivaci posledního výstupního neuronu.



Motivací pro tuto vrstevnatou strukturu (*neuronovou síť*) je, že neurony ve vyšších vrstvách by mohly provádět abstraktnější a komplexnější rozhodnutí, jelikož se zakládají na snazších/elementárnějších rozhodnutích v předchozí vrstvě.[2]

[1] Můžeme si to také představit tak, že tento neuron „váží“ důkazy, které mu vstupy poskytnou, a podle toho se rozhodne aktivovat či ne.

[2] Pár upřesnění: Vstupní vrstvu nepovažujeme za neurony, výstupní vrstvu ano. Ostatním vrstvám říkáme *skryté* vrstvy (anglicky *hidden layers*). Sítím s více než jednou skrytou vrstvou se říká *hluboké* neuronové sítě.

Příklad. Ukažte, že s pomocí vhodné struktury perceptronů lze vyjádřit libovolnou logickou funkci $f : \{0,1\}^n \to \{0,1\}$.[3]

Vidíme, že neuronové sítě umí modelovat víceméně jakékoliv výpočetní rozhodnutí. Jak ale najít správné váhy a biasy pro velkou neuronovou síť? Ručně asi těžko.

Dosud jsme se zabývali perceptrony – jiným typem neuronu je tzv. *sigmoid*. Tento neuron nerozhoduje binárně, ale prožene svůj vážený vstup funkcí $\sigma(x) = \frac{1}{1+e^{-x}}$ a tuto hodnotu pošle na výstup.[4] První znatelnou výhodou sigmoidu je, že jeho výstup spojitě pokrývá interval $(0,1)$, díky čemuž se výstupy těchto neuronů dají interpretovat jako pravděpodobnosti jevů. Hlavní výhoda je ale právě v jeho spojitosti, díky čemuž se neuronové sítě složené ze sigmoidů dají trénovat, což jde s perceptrony kvůli jejich binárnímu chování ztuha. Nadále proto považujme neurony za sigmoidy.

Derivace a gradienty

Představíme si způsob, jak neuronovou síť trénovat, tedy jak nastavit váhy a biasy neuronové sítě automaticky pomocí trénovacích dat. Idea je následující – ukážeme počítači vstupy a očekávané výstupy, např. spoustu obrázků koček a spoustu obrázků bez koček. Pomocí těchto dat vhodný algoritmus nastaví váhy a biasy. Poté bude neuronová síť umět u nových obrázků určovat, jestli na nich je či není kočka.

Budeme muset zabrousit do matematické analýzy – jakmile z ní ale vybrousíme, budeme vyzbrojeni dosud možná nejdůležitějším algoritmem tohoto století.

Úmluva. V počítačích umíme čísla vyjadřovat jen do určité přesnosti a derivace počítáme numerickými metodami. Proto bude následující text zpravidla taky korektní jen do určité přesnosti – teoreticky patologické případy v počítači nejsou problém, protože nenastanou. Předpokládejme tedy, že funkce, se kterými pracujeme, jsou dostatečně *hezké* :).

Představme si funkci $f(x)$, u které chceme najít minimum. Jak na to?

Definice. *Směrnicí* přímky myslíme tangens úhlu, který svírá s kladným směrem osy x. Jestliže má graf funkce f v bodě x tečnu, pak směrnici této tečny nazýváme *derivací* f v bodě x a značíme $f'(x)$. Exaktněji, $f'(x) = \lim_{h\to 0} \frac{f(x+h)-f(x)}{h}$ (pokud je funkce definovaná na okolí x a daná limita existuje).

Tvrzení. *Pokud je f diferencovatelná („derivovatelná“) v x, pak $f'(x)$ je reálné číslo takové, že pro $h \in \mathbb{R}$ platí $f(x+h) = f(x) + hf'(x) + h\alpha(h)$ pro funkci α, která splňuje $\lim_{h\to 0} \alpha(h) = 0$.*

Tím pádem derivace funkce úzce souvisí s její nejlepší *lokální* aproximací přímkou, protože na pravé straně rovnosti máme právě rovnici přímky plus zbytek, který je v blízkém okolí x zanedbatelný.

[3] To znamená, že perceptron je tzv. *výpočetně univerzální* součástka.

[4] Těmto funkcím se obecně říká *aktivační funkce* a je jich spousta. Například perceptron má vlastně také svou aktivační funkci s binárním výstupem.

Derivace má spoustu zajímavých vlastností a existuje pár jednoduchých pravidel, pomocí kterých můžeme zderivovat prakticky cokoliv.

Tvrzení. *Pokud jsou f a g diferencovatelné ve správných bodech, tak platí:*

$$\begin{aligned}(f(x)+g(x))' &= f'(x)+g'(x) \quad (\textit{linearita derivace})\\ (f(x)g(x))' &= f'(x)g(x)+f(x)g'(x) \quad (\textit{derivace součinu})\\ (f(g(x)))' &= g'(x)f'(g(x)) \quad (\text{„řetízkové pravidlo“, } \tfrac{df}{dx}=\tfrac{dg}{dx}\tfrac{df}{dg})\end{aligned}$$

Pro představu si ukážeme, co derivace vyjadřuje. Spolu s předchozím tvrzením nám bude stačit linearita derivace a základní pravidlo $(x^n)' = nx^{n-1}$ pro přirozené n.

Příklad. Mějme polynom $p(x) = (x-3)(x+1)(x+2)$. Jaká je jeho derivace a co z ní můžeme o polynomu zjistit?

Tvrzení. *Jestliže má funkce f na nějakém okolí bodu x kladnou derivaci, pak je na nějakém jeho okolí ostře rostoucí. Pokud má naopak derivaci zápornou, je naopak na nějakém okolí ostře klesající.*

Tvrzení. *Jestliže má funkce f v bodě x lokální minimum nebo maximum, pak derivace v tomto bodě buď neexistuje, nebo je nulová.*

Nyní budeme potřebovat zobecnit na funkce více proměnných. Tučnými písmenky značme tzv. *vektory* více proměnných, např. $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. Pro multidimenzionální funkce platí analogie výše uvedených poznatků.

Definice. Mějme funkci $f(\mathbf{x})$, kde $\mathbf{x} \in \mathbb{R}^n$ je vektor více proměnných. *Parciální derivaci* funkce f podle její i-té složky značíme $\frac{\partial f}{\partial x_i}$. V podstatě funkci zderivujeme podle jediné vstupní proměnné, přičemž ostatní považujeme za konstanty.

Parciální derivace udává rychlost růstu/klesání funkce vůči jedné složce vstupu. Pokud všechny parciální derivace složíme do jednoho vektoru, dostaneme souhrnnou informaci o tom, jak se funkce chová ve všech směrech.

Definice. *Gradientem* funkce f v bodě $\mathbf{x}$ nazveme vektor parciálních derivací $\nabla f = (\frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n})$.

Opět si gradient ukážeme na snadném příkladu.

Příklad. Mějme polynom $p(x, y) = \frac{3}{2}x^2 + \frac{1}{2}y^2$. Určete jeho gradient a zamyslete se nad ním.

Tvrzení. *Stejně jako u derivací funkcí jedné proměnné, gradient v bodě $\mathbf{a}$ je nejlepší aproximací funkce f na lokálním okolí bodu $\mathbf{a}$.*

Gradientový sestup

Pointa metody gradientového sestupu je, že se vždy podle gradientu „posuneme“ směrem, kterým hodnotu funkce nejvíce snížíme.

Příklad. Známe hodnotu funkce f v bodě $\mathbf{a} \in \mathbb{R}^n$. V tomto bodě známe i (nenulový) gradient $\nabla f(\mathbf{a}) \in \mathbb{R}^n$. Dokažte, že směr nejrychlejšího snížení funkce f je $-\nabla f(\mathbf{a})$.

Loss function

Pojďme si neuronovou síť lépe formalizovat. Označme $a_j^{(l)}$ aktivaci j-tého neuronu v l-té vrstvě, $b_j^{(l)}$ jeho bias (dohodněme se, že bias budeme vždy přičítat). Považujme $\mathbf{a}^{(0)}$ za vstup a $\mathbf{a}^{(L)}$ za výstup poslední vrstvy neuronů, tedy výstup (predikci) celé sítě. Označme n_l počet neuronů v l-té vrstvě. Nechť je $w_{jk}^{(l)}$ váha spojení neuronů s aktivacemi $a_k^{(l-1)}$ a $a_j^{(l)}$.

Jako *vážený vstup* neuronu s konečnou aktivací $a_j^{(l)}$ označme hodnotu

$$z_j^{(l)} = \sum_k w_{jk}^{(l)} a_k^{(l-1)} + b_j^{(l)}$$

Platí tedy $a_j^{(l)} = \sigma\left(z_j^{(l)}\right)$.

Celý přechod od aktivací jedné vrstvy k aktivacím druhé vypadá v maticovém zápise následovně: $\mathbf{a^{(l)}} = \sigma\left(\mathbf{w}^{(l)}\mathbf{a}^{(l-1)} + \mathbf{b}^{(l)}\right)$.[5]

Neuronová síť je vlastně jedna velká funkce $f(\mathbf{x}) : \mathbb{R}^{n_0} \to \mathbb{R}^{n_L}$ kde $\mathbf{x}$ je vstup. To, co na síti chceme optimalizovat, jsou její parametry, tedy váhy w a biasy b. Chtěli bychom nějakým způsobem měřit, jak je síť „dobrá“ vzhledem k trénovacím datům $(\mathbf{x}_0, \mathbf{y}_0), \ldots, (\mathbf{x}_{n-1}, \mathbf{y}_{n-1})$, kde x jsou vstupy a y správné výstupy.[6]

Pořídíme si proto tzv. *ztrátovou funkci*: $C(\mathbf{w}, \mathbf{b}) = \frac{1}{n}\sum_{j=0}^{n-1} \|\mathbf{y}_j - f(\mathbf{x}_j)\|^2$.[7]

Tato ztrátová funkce porovnává správný výstup s tím, co spočítala síť. Čím méně se predikce shodují, tím větší hodnotu funkce má. Ztrátová funkce tedy doslova měří, jak moc jsou predikce neuronové sítě na našich datech (s jejími současnými parametry) špatné, a to se hodí. Přesně ztrátovou funkci totiž chceme optimalizovat. Stačí spočítat záporný gradient této funkce vzhledem k parametrům sítě a posunout se v jeho směru – tohle opakujeme, dokud nedosáhneme lokálního minima.

Zpětná propagace

Zbývá poslední – jak vlastně spočítat gradient této (většinou velmi složité) funkce $C(\mathbf{w}, \mathbf{b})$? Jelikož gradient vůči všem trénovacím datům získáme snadno zprůměrováním gradientů pro jednotlivá trénovací data, ukážeme si, jak spočítat gradient

[5] Pokud se v argumentu funkce objeví vektor, aplikujeme funkci po složkách. $\mathbf{w}^{(l)}$ je dokonce matice (vektor vektorů) sdružující všechny váhy z $(l-1)$-ní do l-té vrstvy.

[6] Tato anotovaná data mohou vypadat např. takto: [(Hedvika chce do kina & prší & mám rád zmrzku, 1), (Hedvika nechce do kina & neprší & nemám rád zmrzku, 0), ...]

[7] Stejně jako u aktivačních funkcí je dobré zmínit, že mimo tuto kvadratickou ztrátovou funkci existuje i spousta dalších v praxi užitečných ztrátových funkcí.

pro jediný ukázkový vstup a výstup. Algoritmu na jeho spočítání se říká *zpětná propagace*.

Pro rekapitulaci – gradient funkce $C(\mathbf{w}, \mathbf{b})$ se skládá ze všech možných parciálních derivací $\frac{\partial C}{\partial w_{jk}^{(l)}}$ a $\frac{\partial C}{\partial b_j^{(l)}}$. Abychom tyto hodnoty spočítali, dává smysl postupovat v neuronové síti „odzadu“. Nejdříve zjistíme, jak ovlivňuje ztrátovou funkci výstup poslední vrstvy neuronů a jak bychom tedy měli poslední vrstvu změnit. Pak rekurzivně pokračujeme – jak změnit předposlední vrstvu neuronů, abychom změnili aktivace poslední vrstvy správným směrem? A jak změnit předpředposlední vrstvu, abychom změnili aktivace předposlední vrstvy správným směrem? A tak dál.

Definice. Definujme *chybu* j-tého neuronu v l-té vrstvě jako

$$\delta_j^{(l)} = \frac{\partial C}{\partial z_j^{(l)}}$$

Idea zpětné propagace se poté dá shrnout následovně.

Věta. (4 rovnice zpětné propagace v maticovém zápisu)

$$\boldsymbol{\delta}^{(L)} = \nabla_{\mathbf{a}^{(L)}} C \odot \sigma'(\mathbf{z}^{(L)}) \tag{BP1}$$

$$\boldsymbol{\delta}^{(l)} = ((\mathbf{w}^{(l+1)})^T \boldsymbol{\delta}^{(l+1)}) \odot \sigma'(\mathbf{z}^{(l)}) \tag{BP2}$$

$$\frac{\partial C}{\partial b_j^{(l)}} = \delta_j^{(l)} \tag{BP3}$$

$$\frac{\partial C}{\partial w_{jk}^{(l)}} = a_k^{(l-1)} \delta_j^{(l)} \tag{BP4}$$

Easy, ne?

První dvě rovnice vysvětlují, jak spočítat chybu neuronu pro všechny neurony. Druhé dvě vysvětlují, jak to využít k výpočtu gradientu.

(BP1) vyjadřuje chybu poslední vrstvy na základě vlivu aktivací v poslední vrstvě na ztrátovou funkci – vektor těchto parciálních derivací vůči výstupům poslední vrstvy (gradient) značíme $\nabla_{\mathbf{a}^{(L)}} C$. Také je zapotřebí vzít v potaz vliv aktivační funkce, kterou hodnota $z^{(L)}$ prochází.[8]

(BP2) vyjadřuje chybu l-té vrstvy sítě na základě chyby $(l+1)$-ní vrstvy – zde provádíme maticové násobení vahami mezi těmito dvěma vrstvami, přičemž opět musíme vzít na vědomí i vliv aktivační funkce.[9]

Pomocí (BP1) a (BP2) tedy dovedeme „odzadu“ spočítat chybu všech neuronů sítě.

(BP3) je dobrá zpráva – derivace ztrátové funkce vůči biasu neuronu je přímo chyba tohoto neuronu.

[8]Tomu divnému kolečku se říká *Hadamardův součin*, znamená to násobení po složkách.

[9]To divné T-čko je tzv. *transpozice* matice.

(BP4) je zajímavá – derivace ztrátové funkce vůči váze propojující tento neuron s nějakým předchozím neuronem je úměrná aktivaci toho předchozího neuronu. Jinak řečeno, z aktivního neuronu dostaneme silné impulzy na změnu z něj vycházejících vah. Naopak, je-li neuron málo aktivní (tj. jeho aktivace je blízká nule), je z pohledu ztrátové funkce příslušná konexe málo důležitá, proto vznikne jen malý impulz pro změnu její váhy.

Příklad. Dokaž rovnice zpětné propagace pomocí výše uvedeného tzv. *řetízkového* pravidla.

Věta. (Univerzalita neuronových sítí) *Už pomocí neuronové sítě s jedinou schovanou vrstvou neuronů lze libovolně dobře aproximovat libovolně složitou spojitou funkci.*

Závěrem

Proniknout do matiky, na které jsou postavené neuronové sítě, nejde naráz. V tomto příspěvku jsou uvedené ty nejzákladnější věci, ale je toho mnohem víc – plejáda různých aktivačních a ztrátových funkcí nebo jiné architektury. Například konvoluční sítě, které jsou používány pro rozpoznávání obrázků, nebo rekurentní neuronové sítě (LSTM) používané pro zpracovávání lidské řeči a překlad. Doporučuji zkusit si nějakou neuronovou síť nakódit, viz zdroje :)

Literatura a zdroje

[1] Michael Nielsen: *Neural Networks and Deep Learning*, *http://neuralnetworksanddeeplearning.com*
[2] 3Blue1Brown: *But what is a neural network?*, *https://www.youtube.com/watch?v=aircAruvnKk*
[3] Jakub Krásenský: *Derivace (s trochou mýdla)*, Zásada, 2017 podzim.
[4] Danil Koževnikov: *Analýza v MO*, iKS, 2019.

Mocnost bodu ke kružnici

Hedvika Ranošová

Abstrakt. Příspěvek seznamuje se základními vlastnostmi mocnosti bodu ke kružnici a ilustruje její použití v geometrických úlohách.

Trocha teorie na úvod

Definice. Je dán bod M a kružnice k se středem O a poloměrem r. *Mocností* bodu M ke kružnici k rozumíme číslo $p(M,k) = |MO|^2 - r^2$.

Poznámka. Pokud bod M leží vně, resp. uvnitř kružnice k, je číslo $p(M,k)$ kladné, resp. záporné. Leží-li bod M na kružnici k, je $p(M,k) = 0$.

Poznámka. Nechť M a N jsou dva různé body. Pak $p(M,k) = p(N,k)$, právě když $|MO| = |NO|$.

Tvrzení. *Nechť přímka p vedená bodem M protne kružnici k v bodech A, B. Pak platí*

$$p(M,k) = \begin{cases} |MA| \cdot |MB|, & \text{leží-li } M \text{ vně } k, \\ -|MA| \cdot |MB|, & \text{leží-li } M \text{ uvnitř } k. \end{cases}$$

Jestliže speciálně M leží vně k a označíme T bod dotyku tečny ke kružnici k vedené bodem M, pak $p(M,k) = |MT|^2$.

Tvrzení. *Nechť $ABCD$ je čtyřúhelník a $M = AD \cap BC$. Pak $ABCD$ je tětivový, právě když $|MA| \cdot |MD| = |MB| \cdot |MC|$.*

Definice. Nechť k, l jsou kružnice. Množinu bodů X splňujících $p(X,k) = p(X,l)$ nazýváme *chordálou* kružnic k, l.

Tvrzení. *Chordála dvou nesoustředných kružnic je přímka kolmá na spojnici jejich středů.*

Tvrzení. *Uvažme tři kružnice k_1, k_2, k_3. Pak jejich vzájemné chordály procházejí jedním bodem (nebo jsou všechny rovnoběžné). Tomuto bodu se říká potenční střed kružnic k_1, k_2, k_3.*

Příklady

Příklad 1. Kružnice k, l se středy K, L se protínají v bodech A, B. Přímka AB protne společnou tečnu kružnic k, l, která se jich dotýká v bodech T, U, v bodě P. Pak $|PT| = |PU|$.

Příklad 2. Na prodloužení tětivy KL kružnice k se středem O leží bod A. Tečny z bodu A ke kružnici k se jí dotýkají v bodech T, U. Označme M střed úsečky TU. Ukažte, že čtyřúhelník $KLMO$ je tětivový.

Příklad 3. Kružnice vepsaná trojúhelníku ABC se dotýká jeho stran AB, BC, CA v bodech F, D, E. Označme písmeny Y_1, Y_2, Z_1, Z_2, M středy úseček FB, BD, DC, CE, BC. Konečně buď $X = Y_1Y_2 \cap Z_1Z_2$. Dokažte, že $XM \perp BC$.

Příklad 4. Mějme pravoúhlý trojúhelník ABC s přeponou AB. Na jeho odvěsně AC zvolme bod D. Nyní sestrojme kružnici k_1, která se dotýká AB v bodě A a prochází bodem D. Dále též kružnici k_2, která se dotýká AB v bodě B a též prochází bodem D. Označme E druhý průsečík kružnic k_1 a k_2. Dokažte, že úhly BAC a DEC jsou shodné. (Hradiště 2007)

Příklad 5. Tečny skrz A ke kružnici k se jí dotýkají v bodech T a U. Buď M střed AT. Úsečka MU protne k podruhé v bodě X. Dokažte, že $XA = 2 \cdot MX$.

Příklad 6. Na přímce p leží body A, B, C, D v tomto pořadí. Kružnice nad průměry AC, BD se protnou v X, Y. Na přímce XY zvolíme bod P ($P \notin BC$). Přímka CP protne kružnici nad AC podruhé v bodě M, přímka BP kružnici nad BD v bodě N. Ukažte, že přímky AM, DN, XY procházejí jedním bodem. (IMO 1995)

Příklad 7. V trojúhelníku ABC označme B_0, C_0 paty příslušných výšek. Zvolme bod P tak, aby přímka PB byla tečnou ke kružnici opsané $\triangle PAC_0$ a přímka PC tečnou ke kružnici opsané $\triangle PAB_0$. Dokažte, že AP je kolmá na BC. (MEMO 2011, MR&JT)

Příklad 8. Body P a Q leží na stranách CA a AB trojúhelníka ABC. Označme K, L a M postupně středy úseček BP, CQ a PQ. Dále předpokládejme, že přímka PQ je tečnou ke kružnici opsané trojúhelníku KLM. Ukažte, že body P a Q jsou stejně vzdálené od středu kružnice opsané $\triangle ABC$. (IMO 2009)

Příklad 9. Je dán ostroúhlý trojúhelník ABC s ortocentrem H. Kružnice se středem ve středu strany BC procházející bodem H protne BC v A_1, A_2. Body B_1, B_2, C_1, C_2 definujeme podobně. Dokaztem že těchto šest bodů leží na kružnici. (IMO 2008)

Příklad 10. Je dána kružnice k a přímka p. Bod P se nachází na p. Tečny z P ke k se jí dotýkají v T a U. Uvažme kružnici se středem P procházející body T, U. Dokažte, že všechny takové kružnice procházejí dvěma společnými body.

Příklad 11. Na straně BC trojúhelníka ABC s výškami BM, CN a kolmištěm H je dán bod W. Body X, Y jsou zvoleny tak, aby WX, WY byly průměry kružnic BWN, respektive CWM. Dokažte, že body X, Y, H leží na přímce. (IMO 2013)

Příklad 12. Nechť $ABCD$ je čtyřúhelník vepsaný do kružnice k takový, že přímky AD a BC se protínají v bodě Q. Označme M průsečík přímky BD a rovnoběžky s přímkou AC vedené bodem Q. Zvolme $T \in k$ tak, aby MT byla tečnou kružnice k. Dokažte, že $|MT| = |MQ|$. (MKS 2005)

Příklad 13. Je dán trojúhelník ABC s vepsištěm I a opsištěm O. Kolmice na AI skrz I protne BC v A'. Podobně definujme B' a C'. Dokažte, že body A', B', C' leží na přímce kolmé na OI.

Příklad 14. Úhlopříčky nerovnoramenného lichoběžníku $ABCD$ se protínají v bodě P. Nechť A_1 je druhý průsečík kružnice opsané $\triangle BCD$ s přímkou AP, body B_1, C_1, D_1 definujeme obdobně. Dokažte, že $A_1B_1C_1D_1$ je také lichoběžník.
(Turnaj měst 2008)

Příklad 15. Osy úhlů u vrcholů A, B protnou protější strany trojúhelníka ABC v bodech D, E a samy sebe v I. Přímka DE protne kružnici opsanou v M a N. Dokažte, že připisště I_A a I_B leží na kružnici MIN. (ARO 2006)

Příklad 16. V pravoúhlém trojúhelníku ABC s přeponou AB označme G těžiště. Bod P na polopřímce AG splňuje $\sphericalangle CPA = \sphericalangle CAB$, bod Q na polopřímce BG splňuje $\sphericalangle CQB = \sphericalangle ABC$. Dokažte, že se kružnice AQG a BPG protínají na AB.
(Kanada 2013)

Návody

1. Uvažujte mocnost z bodu P.

2. Použijte pravoúhlé trojúhelníky.

3. Uvažujte B, C jako nulové kružnice.

4. Přímka DE prochází středem úsečky AB, použijte úsekové úhly.

5. Dokreslete kružnici opsanou AXU.

6. Hledaný průsečík bude potenčním středem.

7. Bod P je průsečík výšky z vrcholu A a Thaletovy kružnice nad BC.

8. Ukažte, že trojúhelníky MKL a AQP jsou si podobné.

9. Dokažte, že na kružnici leží vždy dvě dvojice bodů. Mohlo by se jednat o různé kružnice?

10. Přímka p je chordála k a nějakého bodu.

11. Protněte kružnice podruhé.

12. Dokažte, že MQ je tečnou ke kružnici opsané BDQ.

13. Uvažujte I jako kružnici s nulovým poloměrem.

14. Kombinujte čtyři rovnosti získané z mocností.

15. Dokažte, že DE je chordála dvou kružnic.

16. Úhlové podmínky převeďte na tečnosti a tipněte správný bod na AB.

Literatura a zdroje

Čerpala jsem z příspěvků Tondy Le a Verči Hladíkové, kterým tímto velice děkuji.

[1] Anh Dung „Tonda“ Le : *Mocnost bodu ke kružnici*, Hojsova Stráž, 2016.
[2] Verča Hladíková: *Mocnost bodu ke kružnici*, *i*KS Strmilov, 2018.

Ramseyovky

Martin Raška

Abstrakt. Pravidelné struktury se v matematice skrývají všude. I když si vezmeme náhodně vytvořené objekty, tak často stačí, aby byly dost velké, a máme zajištěnou určitou pravidelnost. V teorii grafů se tímto zabývá převážně Ramseyova teorie, jejíž nejdůležitější věty a příklady na ně si v této přednášce předvedeme.

Věta. (Dirichletův princip) *Pro přirozená n, k mějme $nk+1$ míčků obarvených k barvami. Pak musí existovat $n+1$ míčků stejné barvy.*

Úloha. (Motivace) Mějme skupinu 6 lidí, kde se každí dva lidé navzájem buď znají, nebo neznají. Ukažte, že existuje trojice, ve které se každí dva znají, nebo každí dva neznají.

Věta. (Ramseyova věta – dvojbarevná) *Pro každá přirozená n, m existuje N takové, že když obarvíme hrany úplného grafu na N vrcholech červenou a modrou, tak vždy nalezneme červený úplný podgraf velikosti n nebo modrý úplný podgraf velikosti m.*

Definice. Nejmenší takovéto číslo N z předcházející věty se značí $R(m,n)$.

Tvrzení. *Platí nerovnost $R(m,n) \leq R(m-1,n) + R(m,n-1)$.*

Poznámka. Podle motivační úlohy je $R(3,3) \leq 6$. Ukažte, že skutečně $R(3,3) = 6$.

Věta. (Ramseyova věta – vícebarevná) *Pro každá přirozená $n_1, \ldots, n_k$ existuje N takové, že když obarvíme hrany úplného graf na N vrcholech k barvami, tak pro nějaké $1 \leq i \leq k$ nalezneme úplný podgraf na n_i vrcholech, jehož hrany mají všechny i-tou barvu.*

Definice. Nejmenší takovéto číslo N z předcházející věty se značí $R(n_1, \ldots, n_k)$.

Tvrzení. *Platí nerovnost $R(n_1, \ldots, n_k) \leq R(n_1, \ldots, n_{k-2}, R(n_{k-1}, n_k))$.*

Podobná tvrzení se dají zformulovat i pro nekonečné grafy. My se podíváme pouze na nekonečno „stejně velké“ jako množina přirozených čísel. Výsledky jde zobecňovat i dále, ale na to už jsou potřeba netriviální znalosti z teorie množin.

Věta. (Ramseyova věta – nekonečná) *Mějme nekonečný graf, kde vrcholy tvoří množina přirozených čísel a hrany všechny dvojice přirozených čísel. Když hrany*

tohoto grafu libovolně obarvíme konečným počtem barev, tak vždy bude existovat nekonečný jednobarevný úplný podgraf.

Poznámka. Platnost nekonečné verze Ramseyovy věty implikuje platnost konečné verze.

Klasická definice grafu nám pomáhá ukazovat vztahy mezi dvojicemi objektů. Co kdybychom se ale rozhodli zkoumat vlastnosti trojic, čtveřic, atd.? K tomu bychom museli klasickou definici grafu rozšířit na strukturu, které se říká hypergraf. Jednoduše řečeno za hrany lze považovat nějakou p-tici vrcholů a ne jenom dvojice. Formální definici si uvádět nebudeme, ale význam by měl být jasný z následující věty.

Věta. (Ramseyova věta – pro p-tice) *Pro každá přirozená n, p, k existuje přirozené N takové, aby platilo následující. V úplném grafu na N vrcholech přiřadíme každé p-tici vrcholů jednu z k barev, potom vždy existuje úplný podgraf o n vrcholech, kde každá p-tice z daných n vrcholů má stejnou barvu.*

Poznámka. Stejná věta platí i pro nekonečné grafy, ostatně z ní se často konečná věta i vyvozuje.

Perličky na přirozených číslech

Věta. (Van der Waerdenova) *Pro libovolná přirozená čísla d, k existuje přirozené N takové, že když jakkoli obarvíme čísla $1, \dots, N$ k barvami, tak vždy najdeme jednobarevnou aritmetickou posloupnost délky d.*

Definice. Nejmenší takovéto číslo N z předcházející věty se značí $W(d, k)$.

Tvrzení. $W(3, 2) \leq 5 \cdot (2 \cdot 2^5 + 1)$.

Tvrzení. $W(3, 3) \leq 7 \cdot (2 \cdot 3^7 + 1) \cdot (2 \cdot 3^{7 \cdot (2 \cdot 3^7 + 1)} + 1)$.

Důkaz výše uvedených tvrzení využívá toho, že najdeme dostatek jednobarevných (ale navzájem různě barevných) aritmetických posloupností délky 2 mířících do stejného místa. Tím zajistíme, že číslo na tomto místě už musí doplňovat jednu z těchto posloupností na jednobarevnou posloupnost délky 3. Stejnou myšlenkou ve spojení s dvojnásobnou indukcí podle délky posloupnosti a počtu barev lze dokázat Van der Waerdenovu větu i v obecném případě. Pro formální důkaz se hodí uvažovat jedno zanoření indukce navíc. Konkrétně pokud bychom chtěli dokázat konečnost $W(d, k)$, tak dokazovat, že pro všechna přirozená $i \leq k$ existuje N takové, že libovolné obarvení množiny $\{1, \dots, N\}$ obsahuje jednobarevnou aritmetickou posloupnost délky d nebo i různě barevných jednobarevných aritmetických posloupností délky $d - 1$ mířících do stejného místa.

Věta. (Schurova věta) *Pro každé obarvení přirozených čísel dvěma (resp. konečně mnoha) barvami existují $x, y, z \in \mathbb{N}$ mající stejnou barvu a splňující $x + y = z$.*

A jsou tu i nějaké příklady!

Úloha 1. (Erdős-Szekeres) V posloupnosti $(n-1)(m-1)+1$ různých přirozených čísel vždy existuje klesající podposloupnost délky n nebo rostoucí délky m.

Úloha 2. Každý bod v rovině je obarven buď modře, nebo červeně. Ukaž, že existuje obdélník s vrcholy stejné barvy.

Příklad 3. Dokaž, že dokonce $W(3,2) = 9$.

Příklad 4. Dokaž, že $R(k,l) < R(k-1,l) + R(k,l-1)$, pokud jsou obě čísla $R(k-1,l)$ a $R(k,l-1)$ sudá.

Příklad 5. Dokaž, že existuje nekonečná množina přirozených čísel H taková, že pro každá dvě různá čísla $x, y \in H$ má číslo $x+y$ sudý počet různých provočíselných dělitelů. (Staré PraSe – myšmaš)

Příklad 6. Dokaž, že existuje množina H z předchozího příkladu, která obsahuje dokonce po dvou nesoudělná čísla.

Příklad 7. (Happy ending problem) Dokaž, že pro každé $n \in \mathbb{N}$ existuje $N \in \mathbb{N}$ takové, že každá množina N bodů v obecné poloze v rovině obsahuje n bodů v konvexní poloze (tj. vrcholy konvexního n-úhelníka).

Příklad 8. V úplném grafu o 17 vrcholech je každá hrana obarvena modře, červeně, nebo zeleně. Dokaž, že v grafu existuje jednobarevný trojúhelník. (IMO 1964)

Příklad 9. (Modulární Velká Fermatova věta) Ukaž, že pro každé přirozené n existuje p_0 takové, že pro všechna prvočísla $p > p_0$ má kongruence

$$x^n + y^n \equiv z^n \pmod{p}$$

řešení pro nějaká x, y, $z \in \mathbb{N}$, kde $xyz \not\equiv 0 \pmod{p}$.

Příklad 10. Existuje funkce $f : \mathbb{N}^2 \to \mathbb{N}$ taková, že pro libovolnou nekonečnou podmnožinu M přirozených čísel platí $\{f(a,b); a, b \in M\} = \mathbb{N}$?

Příklad 11. (těžší) Obarvěme čísla $\{1, \ldots, 1978\}$ libovolně šesti barvami. Dokaž, že existují tři stejnobarevná čísla x, y, z splňující $x + y = z$. (IMO 1978)

Návody

1. Uvažujte dvojice čísel říkající, jaké nejdelší klesající a rostoucí podposloupnosti na konkrétních číslech v posloupnosti končí.

2. Vezměte si mřížku bodů s celočíselnými souřadnicemi a podívejte se na svislé trojice bodů.

5. Aplikuj Ramseyovky třeba na množinu čísel dávající po dělení 3 zbytek 1.

7. Nejdřív vyšetři případ pro $n = 4$.

8. Ke spočetní $R(3,3,3)$ použij fakt, že $R(3,3)=6$.

9. Pomocí primitivního prvku pro p si všechna čísla v $\mathbb{Z}_p^*$ napiš jako mocninu tohoto prvku a následně je obarvi podle velikosti exponentu modulo n.

10. Neexistuje. Dokonce neexistuje, i kdybychom dvojice přirozených čísel „barvili“ pouze 4 barvami místo všech přirozených čísel.

Literatura a zdroje

[1] B. M. Landman, A. Robertson: *Ramsey theory on the Integers*, SML, 2014.
[2] Ben Green, *Ramsey Theory and the IMO*, *https://www.jstor.org/stable/3621841*
[3] Jongmin Baek: *Introduction to Infinite Ramsey Theory*, 2017.
[4] Vašek Rozhoň: *Úvod do Ramseyovy teorie*, Lipová-lázně, 2016.

Simsonova přímka

Martin Raška

Abstrakt. Příspěvek obsahuje některé vlastnosti Simsonovy přímky a řadu úloh, k jejichž řešení lze Simsonovu přímku využít.

Věta. (Simsonova přímka) *Označme K, L, M paty kolmic vedených z bodu P na strany trojúhelníka BC, CA, AB trojúhelníka ABC. Pak body K, L, M leží v přímce právě tehdy, když bod P leží na kružnici opsané trojúhelníku ABC. Této přímce se říká Simsonova přímka bodu P vzhledem k trojúhelníku ABC.*

Zajímavost. (Šikmá Simsonova přímka) *Body leží na přímce i pokud v předchozím tvrzení nahradíme kolmice přímkami, které svírají s příslušnými stranami stejný úhel (orientovaný).*

Cvičení. Simsonovou přímkou vrcholu trojúhelníka je výška na protější stranu.

Cvičení. Simsonovou přímkou obrazu vrcholu podle středu kružnice opsané je protější strana.

Tvrzení 1. *Je-li H ortocentrum, pak Simsonova přímka bodu P půlí úsečku PH.*

Tvrzení 2. *Je-li S střed kružnice opsané, pak Simsonovy přímky bodů P a Q svírají úhel $\frac{1}{2}|\sphericalangle PSQ|$.*

Důsledek. *Simsonovy přímky protějších bodů jsou na sebe kolmé a protínají se na Feuerbachově kružnici.*

Důsledek. *Mají-li dva trojúhelníky společnou kružnici opsanou, pak úhel Simsonových přímek bodu P vzhledem k těmto trojúhelníkům nezávisí na volbě bodu P.*

Příklady

Příklad 1. (Kamarád bodu na kružnici) Pro bod P na kružnici opsané trojúhelníku ABC platí, že obrazy přímek PA, PB, PC v osových souměrnostech postupně podle os úhlů BAC, CBA, ACB jsou rovnoběžné a navíc svírají se Simsonovou přímkou pravý úhel.

Příklad 2. Na kratším z oblouků CD kružnice opsané pravoúhelníku $ABCD$ zvolme bod P. Paty kolmic z bodu P na přímky AB, AC a BD označme postupně

K, L, M. Ukažte, že úhel $\sphericalangle LKM$ má velikost 45°, právě když $ABCD$ je čtverec. (MO 58-III-2)

Příklad 3. (Miquelův bod) Mějme čtyři přímky v obecné poloze (žádné dvě nejsou rovnoběžné a žádné tři se neprotínají v jednom bodě). Každá trojice z nich definuje trojúhelník a uvážíme-li kružnice opsané těmto čtyřem trojúhelníkům, protínají se v jednom bodě.

Zajímavost. (Cliffordův řetízek) *Pět Miquelových bodů definovaných čtveřicemi z pěti přímek v obecné poloze leží na kružnici, šest těchto kružnic daných všemi pěticemi přímek ze šesti přímek v obecné poloze se protínají v jednom bodě atd.*

Příklad 4. Na přímce jsou dány body A, B, C a mimo ni bod P. Dokažte, že bod P leží na kružnici opsané trojúhelníku tvořenému středy kružnic opsaných trojúhelníkům ABP, BCP, ACP.

Příklad 5. V trojúhelníku ABC protíná osa úhlu BAC protější stranu v bodě D. Označme P, Q paty kolmic vedených bodem D na strany AB, AC. Kolmice na BC z bodu D protne PQ v bodě X. Ukažte, že X leží na těžnici z bodu A.

Příklad 6. Konvexní pětiúhelník $AXYZB$ je vepsán do půlkružnice se středem O a průměrem AB. Označme P, Q, R, S postupně paty kolmic z bodu Y na přímky AX, BX, AZ, BZ. Dokažte, že velikost ostrého úhlu, který svírají přímky PQ a RS, je rovna $\frac{1}{2}|\sphericalangle XOZ|$. (USAMO 2010)

Příklad 7. Nechť kružnice vepsaná trojúhelníku ABC má střed I a dotýká se stran BC, CA, AB postupně v bodech D, E, F. Nechť dále M je střed strany BC. Pak se přímky EF, DI a AM protínají v jednom bodě.

Příklad 8. Na kružnici opsané trojúhelníku ABC leží body P, Q tak, aby $PQ \parallel BC$. Paty kolmic z bodů P a Q na AB, respektive AC označme postupně X_1, Y_1, respektive X_2, Y_2. Dokažte, že přímky X_1X_2 a Y_1Y_2 se protínají na výšce na stranu BC.

Příklad 9. Uvažujme pět bodů A, B, C, D, E takových, že $ABCD$ je rovnoběžník a $BCED$ je tětivový čtyřúhelník. Přímka l prochází bodem A, protíná úsečku DC v jejím vnitřním bodě F a přímku BC v bodě G. Platí-li $|EF| = |EG| = |EC|$, ukažte, že l je osou úhlu DAB. (IMO 2007)

Příklad 10. Nechť $ABCD$ je tečnový čtyřúhelník a g je přímka procházející bodem A, která protíná stranu BC v bodě M a přímku CD v bodě N. Označme I_1, I_2, I_3 středy kružnic vepsaných trojúhelníkům ABM, MNC a NDA. Ukažte, že ortocentrum trojúhelníka $I_1I_2I_3$ leží na přímce g. (IMO Shortlist 2009, G8)

Příklad 11. Označme H ortocentrum ostroúhlého trojúhelníka ABC a k jeho kružnici opsanou. Přímka procházející bodem H protne kratší oblouky AC, BC kružnice k postupně v bodech M, P. Rovnoběžka se Simsonovou přímkou bodu P vzhledem k trojúhelníku ABC vedená bodem M protne k v bodě K, rovnoběžka

s BC vedená bodem P protne k podruhé v bodě Q. Označme J průsečík BC a KQ. Dokažte, že trojúhelník KJM je rovnoramenný. (China TST 2011)

Příklad 12. Nechť ABC je ostroúhlý trojúhelník a ω kružnice jemu opsaná. Dále nechť t je tečna kružnice ω a t_a, t_b, t_c jsou po řadě obrazy přímky t v osové symetrii podle přímek BC, CA, AB. Ukažte, že kružnice opsaná trojúhelníku určenému přímkami t_a, t_b, t_c se dotýká kružnice ω. (IMO 2011, 6)

Návody

1. Pro kolmost obrazu přímky PC uvažte tětivový čtyřúhelník $PCKL$.

2. Dokreslete paty kolmic z P na AD a BC. Nalezněte Simsonovy přímky a uvědomte si, že $|\sphericalangle LKM| = |\sphericalangle APB|$.

3. Protněte dvě z kružnic v bodě P a uvědomte si, že paty kolmic v jednotlivých trojúhelnících definují stejné přímky.

4. Interpretujte středy úseček AP, BP, CP jako paty kolmic.

5. Spusťte kolmici ze středu kratšího oblouku BC a použijte stejnolehlost.

6. Všimněte si, že PQ a RS se protínají na AB.

7. Použij Simsonovu přímku ze Švrčkova bodu.

8. Dokreslete kolmice z P, Q na BC a najděte rovnoběžníky.

9. Uvažte Simsonovu přímku bodu E vzhledem k trojúhelníku BCD a vyúhlete.

10. Využijte Tvrzení 1 pro Simsonovu přímku bodu C vzhledem k trojúhelníku $I_1I_2I_3$.

11. Označte $S = MP \cap BC$ a uvědomte si, že stačí, aby $KSJM$ byl tětivový.

12. Označme T dotyk t s ω, A' průsečík t_b s t_c a analogicky B' a C'.

(i) Body X, Y, Z definujeme jako obrazy T podle BC, CA, AB. Dokažte, že leží v přímce.
(ii) Dokažte $\sphericalangle(XC, XC') = \sphericalangle(YC, YC')$.
(iii) Označte K Miquelův bod pro přímky $A'B'$, $B'C'$, $C'A'$, XY.
(iv) Doúhlete, že K je hledaný bod dotyku.

Literatura a zdroje

Celý příspěvek je bezostyšně zkopírován od *Štěpána Šimsy*, kterému tímto děkuji.

[1] Štěpán Šimsa: *Simsonova Přímka*, Meziměstí, 2017.
[2] Pepa Tkadlec: *Simsonova Přímka*, Hojsova Stráž, 2011.
[3] Martina Vaváčková: *Simsonova Přímka*, Zásada, 2014.
[4] *www.artofproblemsolving.com*

Kvantové počítače

Rado van Švarc

Abstrakt. Cílem přednášky bude stručný úvod do toho, jak skutečně fungují kvantové počítače a co dělají.

Varování: V tomto příspěvku se bude nacházet jen velmi zředěná verze přednášky. Pokud chcete kvantové počítače pochopit a nechcete/nemůžete přijít na přednášku, projděte si zdroje uvedené v sekci Literatura a zdroje (doporučuji v pořadí, v jakém jsou seřazeny).

Též počítejte s tím, že dost věcí bude řečeno vcelku neformálně. Jestli to chcete formálněji, přečtěte si zdroje.

Seznámení s qubitem

Tvrzení. (Churchova-Turingova teze) *Pokud nějaký algoritmus skládající se z manipulace symbolů umí provést člověk, počítač to zvládne taky.*

Definice. *Qubit* (čteme „kjůbit“) je označení pro neurčený jednotkový vektor v $\mathbb{R}^n$. *Stav* qubitu je konkrétní vektor.

Značení. Vektor v takzvaném *ket* zápisu značíme $|\varphi\rangle$. Konkrétně ve dvojrozměrném prostoru používáme $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ a $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Příklad. Každý vektor se dá zapsat jako lineární kombinace $|0\rangle$ a $|1\rangle$. Například vektor $\begin{pmatrix} 0{,}6i \\ -0{,}8 \end{pmatrix}$ můžeme zapsat jako $0{,}6i|0\rangle - 0{,}8|1\rangle$. Takové lineární kombinaci říkáme *superpozice*.

Definice. *Amplituda* qubitu na nějaké pozici je příslušný koeficient v lineární kombinaci.

Poznámka. To, že je qubit vektor jednotkové velikosti, znamená, že součet druhých mocnin absolutních hodnot amplitud je roven jedné.

Příklad. Vektor $0{,}6i|0\rangle - 0{,}8|1\rangle$ má na pozicích $|0\rangle$ a $|1\rangle$ amplitudy $0{,}6i$ a $-0{,}8$. Toto je skutečně stav qubitu, protože $|0{,}6i|^2 + |-0{,}8|^2 = 0{,}6^2 + 0{,}8^2 = 0{,}36 + 0{,}64 = 1$.

Základní kvantové brány a obvody

Definice. *Kvantový drát* nic nedělá, jenom přesouvá qubit (kreslíme, jako by byl v prostoru, ale často je přenos spíš v čase). Dá se vyjádřit maticí

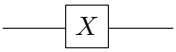
$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Graficky se značí následovně:

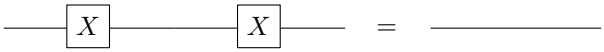
Definice. *Kvantová* NOT *brána* (značíme jí obvykle písmenem X) prohazuje stavy $|0\rangle$ a $|1\rangle$ a na zbytek se lineárně rozšíří. Tedy $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$ a obecně $X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$. Dá se vyjádřit maticí

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Graficky se značí následovně:



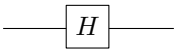
Poznámka. Kvantová NOT brána je sama k sobě inverzní.



Definice. *Hadamardova brána* (značíme ji obvykle písmenem H) je dána jako brána, pro kterou platí $H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ a na ostatní se rozšíří lineárně. Dá se vyjádřit maticí

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Graficky se značí následovně:



Poznámka. Hadamardova brána je sama k sobě inverzní.

Odbočka k lingebře

Definice. Pokud A je $m \times n$ komplexní matice, která má v i-tém řádku a j-tém sloupci číslo $a_{i,j}$, pak A^* je $n \times m$ komplexní matice, která má v i-tém řádku a j-tém sloupci číslo $\overline{a_{j,i}}$.

Definice. Komplexní matici U nazveme *unitární*, pokud platí $UU^* = I = U^*U$.

Cvičení. Rozmyslete si, že I, X, H a matice $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ a $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ jsou všechny unitární.

Definice. Pokud máme vektor $|\varphi\rangle$ v ket zápisu, pak $\langle\varphi| := |\varphi\rangle^*$ je takzvaný *bra* zápis.

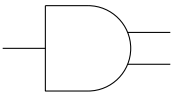
Poznámka. Velikost vektoru $|\varphi\rangle$ se rovná $\sqrt{\langle\varphi||\varphi\rangle}$.

Věta. *Čtvercová matice M je unitární právě tehdy, když pro každý vektor $|\varphi\rangle$ má $|\varphi\rangle$ a $M|\varphi\rangle$ stejnou velikost.*

Poznámka. Všechny brány, kterými qubit prochází, musí být unitární.

Měření qubitu

Definice. *Měřící brána* je taková brána, která když do ní přijde qubit $\alpha|0\rangle + \beta|1\rangle$ změří 0 s pravděpodobností $|\alpha|^2$ a 1 s pravděpodobností $|\beta|^2$. Značí se:

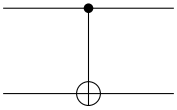


Cvičení. Na vstupu dostanete buď qubit $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, nebo $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Jak zjistíte, který z nich to je?

Další kvantové brány

Poznámka. V systému můžeme mít víc než jeden qubit. Potom na něj pohlížíme jako jednu velkou superpozici. Například pro dva qubity, jeden $\alpha|0\rangle + \beta|1\rangle$ a druhý $\gamma|0\rangle+\delta|1\rangle$, s nimi pracujeme jako s jedním qubitem $\alpha\gamma|00\rangle+\alpha\delta|01\rangle+\beta\gamma|10\rangle+\beta\delta|11\rangle$.

Definice. *Kontrolovaná* NOT *brána*, zkráceně CNOT brána, je brána daná tak, že $\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ přiřazuje $\alpha|00\rangle + \beta|01\rangle + \delta|10\rangle + \gamma|11\rangle$. Obrázek vypadá následovně:



Horní qubit se nazývá *kontrolní* a spodní *cílový*. CNOT brána pak vlastně znamená, že pokud je horní qubit $|1\rangle$, pak funguje jako NOT brána na cílový qubit. Jinými slovy tak platí $|x, y\rangle \mapsto |x, x \oplus y\rangle$.

Cvičení. Pro bázové stavy CNOT nemění kontrolní qubit. Najděte stav, kdy CNOT brána změní kontrolní qubit a nezmění cílový.

Poznámka. CNOT brána je unitární zobrazení a je sama svým vlastním inverzem.

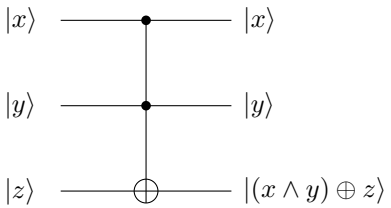
Definice. *Globální fázová brána* je brána, které pro nějaké reálné α všechny amplitudy vynásobí číslem $e^{i\alpha}$.

Poznámka. Globální fázové brány nic neovlivňují a mohou být ignorovány. Speciálně můžeme všechno vynásobit -1 a vše bude fungovat úplně stejně.

Tvrzení. *Kvantový počítač umí spočítat všechno, co umí spočítat normální počítač, a to v (asymptoticky) stejném nebo lepším čase.*

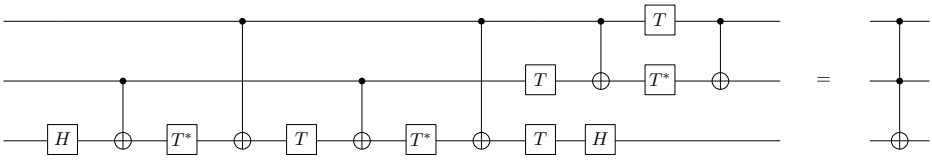
Cvičení. Brána, která působí jako AND brána, nejde postavit jen za pomoci (unitárních) jednoqubitových bran a CNOT bran, které jeden ze zkoumaných qubitů berou jako kontrolní a druhý jako cílový.

Definice. *Toffoliova brána* je brána se dvěma kontrolními qubity a jedním cílovým qubitem daná na bázových qubitech tak, že působí na cílový qubit jako NOT brána a kontrolní qubity nemění, pokud jsou oba kontrolní qubity $|1\rangle$, jinak nemění žádný z qubitů. Jinými slovy $|x, y, z\rangle \mapsto |x, y, z \oplus (x \wedge y)\rangle$. Značíme:



Tvrzení. *Toffoliova brána lze sestrojit jen z (unitárních) jednoqubitových bran a CNOT bran.*

Důkaz. Vezmeme $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ a rozmyslíme si, že funguje toto:



Poznámka. Inverz Toffoliovy brány je Toffoliova brána.

Využívání superpozice

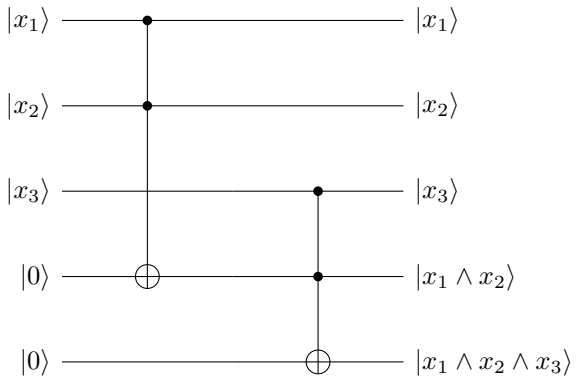
Definice. Jako *vyhledávací problém* myslíme úlohu, při které máme nějakou množinu N potenciálních řešení, z nichž přesně jedno je skutečné řešení, a program (budeme mu říkat *černá krabička*), který umí o daném potenciálním řešení posoudit, je-li skutečným řešením.

Při použití normálního počítače bychom na najití skutečného řešení potřebovali řádově N použití černé krabičky. S kvantovým počítačem nám většinou stačí $\frac{\pi\sqrt{N}}{4}$ použití.

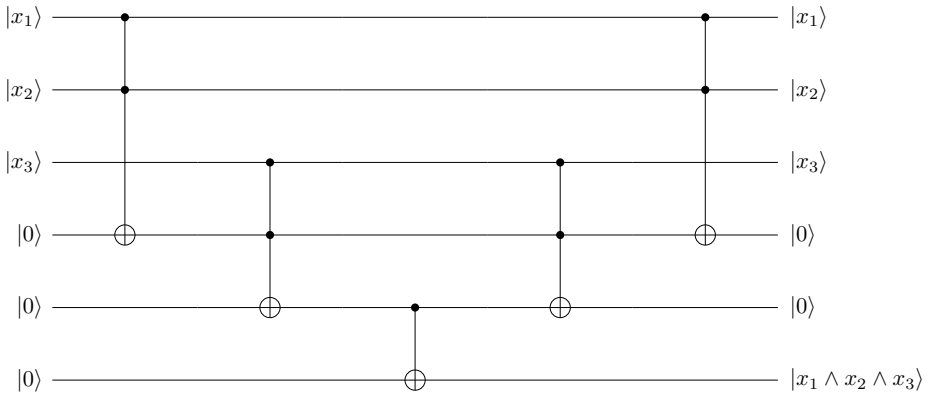
Značení. Řešení uvažovaného vyhledávacího problému budeme značit $|S\rangle$. Jako C_S budeme značit verzi černé krabičky, která funguje jako brána takovým způsobem, že vícerozměrnému qubitu $|x\rangle|0\rangle$ přiřadí $|x\rangle|s(x)\rangle$, kde $s(x) = 1$, pokud $x = S$, a $s(x) = 0$ jinak.

Definice. Mějme kvantovou bránu, která $|x\rangle|0\rangle|0\rangle$ (potenciálně i s více nulami na konci) přiřazuje $|x\rangle|f(x)\rangle|g(x)\rangle$, kde $f(x)$ je hodnota, která nás zajímá a $g(x)$ je, pro naše účely, přebytečná informace. Potom použijeme takzvaný *znepočet*, který se podívá na každou bránu ve výpočtu, pomocí CNOT brány s nulovým cílovým qubitem zkopíruje $f(x)$ a pak pomocí inverzů všech bran z výpočtu převede $|x\rangle|f(x)\rangle|g(x)\rangle$ na $|x\rangle|0\rangle|0\rangle$.

Příklad. Máme-li $|x_1\rangle$, $|x_2\rangle$, $|x_3\rangle$ a chceme spočítat $|x_1 \wedge x_2 \wedge x_3\rangle$, můžeme to provést následovně:



To nám dá zbytečný qubit $|x_1 \wedge x_2\rangle$, kterého se však znepočtem můžeme zbavit:



Značení. $|E\rangle$ vznikne z $|0\rangle|0\rangle\ldots|0\rangle$ aplikací Hadamardovy brány na každý qubit, čili jde o

$$\sum_{x_1,x_2,\ldots,x_n=0,1} \frac{|x_1x_2\cdot x_n\rangle}{2^{\frac{n}{2}}}.$$

Tvrzení. *Brány na obrázcích představují překlopení přes $|S\rangle$ a $|E\rangle$.*

Využívání neurčitosti

Problém. Přirozené číslo N je součinem dvou prvočísel. Jak je rychle najít?

Definice. Nechť q a n jsou nesoudělná čísla. Pak *řád* q vůči n (značíme $\mathrm{ord}_n q$) je nejmenší číslo p takové, že $q^p \equiv 1 \pmod{n}$.

Fakt. Nechť n je pevné a q je náhodné číslo s ním nesoudělné. Pak s pravděpodobností alespoň $\frac{3}{8}$ je $p := \mathrm{ord}_n q$ sudé a n nedělí ani jedno z čísel $q^{\frac{p}{2}}+1$, $q^{\frac{p}{2}}-1$.

Úmluva. Vícerozměrný qubit budeme značit číslem příslušejícím jeho binárnímu zápisu, tj. třeba $|100101\rangle$ budeme zjednodušeně značit $|37\rangle$.

Fakt. Pokud změříme některý qubit, pak všechny ostatní jsou v nejnáhodnější pozici, ve které mohou být, aby změřený mohl vyjít podle pozorování.

Definice. Za Fourierovu transformaci rozměru Q budeme považovat transformaci, která $|k\rangle$ přiřadí $\frac{1}{\sqrt{Q}}(\sum_{i=0}^{Q}\omega^{ik}|i\rangle)$, kde ω je komplexní Q-tá odmocnina z jedničky.

Literatura a zdroje

[1] Andy Matuschak, Michael Nielsen: *Quantum computing for the very curious*, *https://quantum.country/qcvc*

[2] Andy Matuschak, Michael Nielsen: *How the quantum search algorithm works*, *https://quantum.country/search*

[3] Minutephysics: *How Quantum Computers Break Encryption*, *https://youtu.be/lvTqbM5Dq4Q*

[4] Scott Aaronson: *Shor, I'll do it*, *https://www.scottaaronson.com/blog/?p=208n*

[5] Scott Aaronson: *Introduction to Quantum Information Science – Lecture Notes*, *https://www.scottaaronson.com/qclec/combined.pdf*

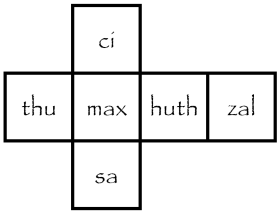
Lingvistika

Michal Töpfer

Abstrakt. Co budete dělat, když se ztratíte v Jerevanském metru a nebudete rozumět nápisům v arménštině? No přeci zapojíte svoje lingvistické schopnosti a budete hledat podobnosti a souvislosti. Cílem tohoto příspěvku je představit lingvistiku jako vědní obor úzce související s matematikou a schopností řešit problémy. Obsahuje několik lingvistických úloh převzatých především z České lingvistické olympiády.

Etruská kostka

V této úloze vidíte tzv. Toskánskou kostku – archeologickou památku popsanou následujícími etruskými slovy: *ci*, *huth*, *max*, *sa*, *thu*, *zal*. Každé z těchto slov odpovídá jednomu z čísel mezi 1 a 6. Rozložení těchto slov na síti kostky vidíte níže:



Při překladu vycházeli lingvisté z následujících informací, které poslouží i vám:

(1) součet protilehlých stran dává dohromady vždy 7,
(2) *thu*, *ci* a *zal* označují (nikoli nutně v tomto pořadí) čísla 1, 2 a 3,
(3) *ci*, ale nikoli *thu* a *zal*, se velmi často objevují na tzv. Lněné knize, která byla objevena na obinadle mumie a která obsahuje rituální texty,
(4) následující dvojice slov se vyskytují v epitafech (náhrobních nápisech):

thu clan; thu at; thu mezu; thu vinac; thu thuscu; ci clenar; zal clenar; ci atr; zal atr; ci mesur; zal mesur; ci vinacr; zal vinacr; ci thuscur; zal thuscur,

(5) v řadě starověkých středomořských kultur mělo číslo 3 zvláštní magický význam.

Úloha. Vepište na správná místa v síti čísla odpovídající jednotlivým slovům.

ČLO-16/17-I-3

Arabština

Přiřaď k českým větám (1-7) jejich arabské ekvivalenty (a-g).

1. Jak se máš?	(a) اسكن أمام المنطقة الجديدة.
2. Jím chléb se sýrem.	(b) اين جبن؟
3. Kde je sýr?	(c) كيف حالك؟
4. Seděli jsme pod oknem jednoho domu.	(d) هذا بيت قديم.
5. Žena sedí na židli.	(e) آكل خبز و جبن.
6. Toto je starý dům.	(f) تجلس مرأة في الكرسية.
7. Žiji před novou čtvrtí.	(g) جلسنا تحت شباك بيت.

ČLO-12/13-I-2

Ztraceni v Jerevanu

Skupinka amerických turistů se vydala na výlet do Jerevanu. Záhy se jim ale podařilo navzájem se ztratit v metru. Posílali si tedy smsky ve snaze zjistit, kde se mají znovu setkat. Jedna skupinka vystoupila na stanici, jejíž jméno si zapsali jako „Shengavit“, druhá skupinka posílala zprávu z „Barekamoutyun“, kde vystoupili oni. Ani jedna ze skupinek však nedokázala najít svou stanici na plánku metra, protože neznali arménské písmo. Dokážete jim pomoci? Práci by vám mohla usnadnit jména několika dalších stanic, která měli turisté zapsaná ve svém průvodci: „Gortsaranain“, „Zoravar Andranik“, „Charbakh“ a „Garegin Njdehi Hraparak“.



Úloha 1. Pokud se první skupinka z Shengavit vydá správným směrem vstříc zbytku výpravy, jak se bude jmenovat první stanice, kterou projedou?

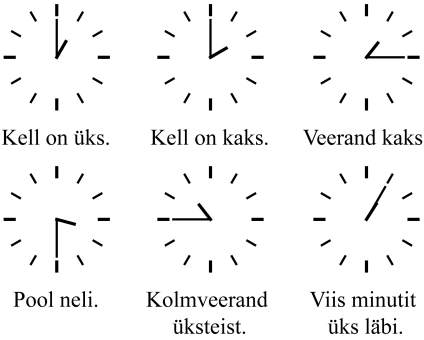
Úloha 2. Kolik stanic musí první skupinka ujet z Shengavit, aby se dostala na Barekamoutyun? (Přičemž následující stanice je jedna, další dvě atd., Barekamoutyun se také počítá.)

Úloha 3. Přepište jméno stanice na konci připojující se pětizastávkové linky. (Písmeno, které vypadá jako S, je ve skutečnosti T!)

ČLO-11/12-I-2

Kolik hodin je v Tallinu

Tallin je hlavní město Estonska, kde přibližně 1 milion lidí mluví estonštinou, neindoevropským jazykem příbuzným finštině.



Některá čísla v estonštině:

6 – kuus, 7 – seitse, 8 – kaheksa, 10 – kümme.

Úloha 1. Přeložte následující časy do estonštiny:

a) 8:45,
b) 4:15,
c) 11:30,
d) 7:05,
e) 12:30.

Úloha 2. Zapište, jaký čas označují následují estonské fráze:

a) Kakskümmend viis minutit üheksa läbi.
b) Veerand neli.
c) Pool kolm.
d) Kolmveerand kaksteist.
e) Kolmkümmend viis minutit kuus läbi.

ČLO-14/15-I-2

O opicích a dětech

Jazyk apinayé patří do brazilské jazykové rodiny Ge. V současnosti jím mluví méně než 800 lidí, a je tedy vážně ohrožený.

Níže vidíte ukázku šesti vět ze zmíněného jazyka spolu s jejich českými překlady. V jejich zápisu jsme použili i některé znaky, které nepatří ani do české, ani portugalské abecedy; abyste však úlohu vyřešili, nepotřebujete vědět, jak se tyto znaky vyslovují.

Kukrɛ̃ kokoi.	Opice jí.
Ape kra.	Dítě pracuje.
Ape kokoi ratš.	Velká opice pracuje.
Ape mï mɛtš.	Dobrý muž pracuje.
Ape mɛtš kra.	Dítě pracuje dobře.
Ape punui mï piŋetš.	Starý muž pracuje špatně.

Úloha 1. Přeložte do češtiny:

Ape ratš mï mɛtš.
Kukrɛ̃ ratš kokoi punui.
Ape piŋetš mï.

Úloha 2. Přeložte do apinayé:

Velké dítě pracuje dlouho.
Stará opice jí hodně.

Úloha 3. Vysvětlete význam těchto slov:

ratš:
mɛtš:
piŋetš:

ČLO-13/14-I-2

Počítání v gáwríjštině

Gáwríjština je jedním z asi 30 jazyků severopákistánských horských vesnic. Tento jazyk se řadí do indoárijské větve indoevropské jazykové rodiny, což znamená, že je velmi vzdáleně příbuzný češtině.

Prohlédněte si následující gáwríjské číslovky:

5 – paandž, 44 – čorteedubiš, 14 – čun, 63 – tlaateetläbiš, 24 – čorteebiš,
72 – bääteetläbiš, 33 – tlooteebiš, 81 – ääkteečorbiš, 34 – čunteebiš.

Úloha 1. Napište gávríjsky: 13, 52, 61, 94.

Zde je několik dalších gávríjských číslovek:

55 – paandžkämtläbiš, 76 – čorkämčorbiš, 97 – tlaakämpandžbiš.

Úloha 2. Napište gávríjsky: 36, 57, 79, 103.

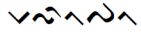
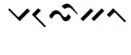
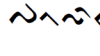
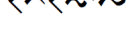
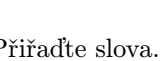
ČLO-17/18-I-2

Lontara

Bugijština je jazyk z austronéské rodiny, kterým mluví přibližně 5 milionů lidí v oblasti ostrova Sulawesi.

Ve dvou sloupcích máte zadána slova v bugijštině v náhodném pořadí. V levém řádku v písmu lontara, ve druhém v přepisu do latinky s českým překladem.

Pozn.: Apostrof (’) i „h“ označují výslovnostní variantu předcházející samohlásky.

A.		1.	batuwa (náctiletý)
B.		2.	polisih (policie)
C.		3.	marenu (šťastný)
D.		4.	polotoh (tužka)
E.		5.	bata (pochybnost)
F.		6.	badi’ (tradiční meč)
G.		7.	toli (vždy)
H.		8.	maleko (ohyb)
I.		9.	telepisi (televize)
J.		10.	juku’ (ryba)
K.		11.	goluh (míček)
L.		12.	malopo (velký)

Úloha 1. Přiřaďte slova.

Úloha 2. Zapište písmem lontara:

lagoh (švagr), kabusuh (křeslo), mateh (umřít),
pasarah (trh), purinah (strýc), sikola (bronzový).

ČLO-14/15-I-1

Čínské znaky

V následující tabulce je uvedeno několik čínských znaků, jejich fonetický přepis a překlad do češtiny.

汀	tīng	pobřeží	浯	wú	řeka Wu
咏	yǒng	zpívat	咀	jǔ	žvýkat
燂	tán	kouř	烘	hōng	grilovat
沮	jǔ	uplakaný	吵	chāo	mluvit hlasitě
叮	dīng	kousnout	炷	zhù	knot
洪	hōng	potopa	浅	qiǎn	mělký
炒	chǎo	smažit	炊	chūi	vařit
唔	wú	číst nahlas	哄	hōng	smát se
注	zhù	nalít	吹	chūi	foukat

Úloha 1. Na základě informací z tabulky přiřaďte k těmto znakům český překlad:

1. 泳 2. 焐 3. 叫

a) křičet b) plavat c) zahřát

Úloha 2. Přiřaďte ke znakům jejich fonetický přepis:

1. 玎 2. 烘 3. 吵 4. 怛 5. 吾

a) dīng b) jù c) chào d) wú e) hōng

ČLO-12/13-I-5

Irština

V tabulce níže vidíte seznam irských slov, jejich fonetický přepis a překlad do češtiny:

čeština	irský zápis	irská výslovnost
dítě	páiste	paːštə
pes	gadhair	gajər
lodě	báid	baːd
láska	searc	šark
krev	fuil	ful
med	meala	malə
bude	bíodh	biːɣ
kniha	leabhar	laur
byl	bhi	vi
televize	teilifisean	tiləfəšən
místnost	seomra	šomrə

Úloha. Přepište výslovnost těchto irských slov:

a) teo,
b) bhíomar,
c) Sáile,
d) anseo.

ČLO-13/14-I-3

Literatura a zdroje

[1] *Česká lingvistická olympiáda*, *http://ufal.mff.cuni.cz/clo*

Obsah

Algebraické triky neboli... fígle (Filip Čermák) 3
Zbytky a mocnění (Filip Čermák) 11
Pellova rovnice a kvadratické okruhy (Matěj Doležálek) 15
Koulítko a rovinítko (Verča Hladíková) 22
Geometrické množiny bodů (Lenka Kopfová) 24
Aritmetické vlastnosti polynomů (Danil Koževnikov) 28
Funkcionální rovnice (Danil Koževnikov) 33
Úvod do kombinatoriky (Anna Mlezivová) 39
Teorie her (Viki Němeček) 45
Chinese dumbass notation (Radek Olšák) 51
Těžiště v kombinatorice (Radek Olšák) 57
Lineární algebra (Terka Poláková) 59
Neuronové sítě (Marian Poljak) 64
Mocnost bodu ke kružnici (Hedvika Ranošová) 71
Ramseyovky (Martin Raška) 75
Simsonova přímka (Martin Raška) 79
Kvantové počítače (Rado van Švarc) 82
Lingvistika (Michal Töpfer) 88