Branná

Sborník, jaro 2019

Filip Bialas
Filip Čermák
Tonda Češík
Petr Gebauer
„madam Verča“ Hladíková
Honza „Fanda“ Krejčí
Jakub Löwit
Anna Mlezivová
Viki Němeček
Tomáš Novotný
Marian Poljak
Martin Raška
Jáchym Solecký
Michal Töpfer

Autoři: Filip Bialas, Filip Čermák, Tonda Češík, Petr Gebauer, „madam Verča“ Hladíková, Honza „Fanda“ Krejčí, Jakub Löwit, Anna Mlezivová, Viki Němeček, Tomáš Novotný, Marian Poljak, Martin Raška, Jáchym Solecký, Michal Töpfer
Editoři: Viki Němeček a Michal Töpfer
vydání první, náklad 45 výtisků
duben 2019
Díky za pomoc všem, kterým je za co děkovat.

Aritmetické funkce

Filip Bialas

Abstrakt. V této přednášce si zavedeme pojem aritmetických funkcí, které obvykle kódují různé číselně teoretické informace, a ukážeme si několik základních vztahů mezi nimi. Speciálně zavedeme důležitý pojem Dirichletových konvolucí.

Definice. *Aritmetickou funkcí* nazveme libovolnou funkci z přirozených do reálných (nebo i komplexních) čísel.

Zdá se, že pojem aritmetické funkce splývá s pojmem posloupnosti (ke každému přirozenému číslu máme v obou případech přiřazené nějaké libovolné číslo). Aritmetické funkce budeme ale používat v jiném kontextu – klasicky to totiž budou funkce, které vyjadřují nějakou číselně teoretickou vlastnost. Uveďme si nejdříve několik příkladů.

(1) $\varphi(n)$: *Eulerova funkce* udávající počet přirozených čísel nesoudělných s n a menších nebo rovných n.
(2) $\pi(n)$: *Prvočíselná funkce* udávající počet prvočísel menších nebo rovných n.
(3) $\tau(n)$: Počet dělitelů čísla n.
(4) $\sigma(n)$: Součet dělitelů čísla n.

Tvrzení. *Pro všechna $n \in \mathbb{N}$ platí $\sum_{d|n} \varphi(d) = n$.*

Důsledek. *Pro každé prvočíslo p existuje primitivní prvek (přirozené a takové, že mocniny a probíhají všechny nenulové zbytky po dělení p).*

Zaveďme si novou aritmetickou funkci definovanou poněkud zvláštně:

Definice. *Möbiovou funkcí* $\mu(n)$ nazveme aritmetickou funkci, která je pro bezčtvercové n rovna $(-1)^k$, kde k je počet prvočíselných dělitelů čísla n, a 0 jinak.

Tvrzení. *Platí $\sum_{d|n} \mu(d) = 1$ pro $n = 1$ a $\sum_{d|n} \mu(d) = 0$ jinak.*

Tvrzení. *Pro všechna přirozená n platí $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$.*

Důsledek. *Pro všechna přirozená n platí $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$.*

Dirichletovy konvoluce

Definice. *Dirichletovou konvolucí* (též *Dirichletovým součinem*) dvou aritmetic-

kých funkcí f, g máme na mysli aritmetickou funkci h definovanou

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Značíme $h = f \star g$.

Příklad. Pokud I označíme funkci, která je rovna 1 pro $n = 1$ a nula jinak, u konstantní jednotkovou funkci a N identickou funkci, pak platí $N = \varphi \star u$, $I = \mu \star u$, $\varphi = \mu \star N$.

Tvrzení. *Aritmetické funkce, které nejsou v jedničce rovny* 0, *spolu s Dirichletovou konvolucí tvoří komutativní grupu.*

Důsledek. *(Möbius inversion formula) Pokud pro dvě aritmetické funkce f, g a pro všechna přirozená n platí*

$$f(n) = \sum_{d|n} g(d),$$

pak pro všechna přirozená n máme:

$$g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right).$$

Multiplikativní funkce

Definice. O aritmetické funkci f řekneme, že je *multiplikativní*, pokud pro všechna přirozená čísla m, n taková, že $(m, n) = 1$, platí $f(m)f(n) = f(mn)$ a zároveň není identicky nulová. Navíc řekneme, že je *úplně multiplikativní*, pokud dokonce pro všechna přirozená m, n platí $f(m)f(n) = f(mn)$.

Příklad. Aritmetické funkce φ, μ, N, u, I jsou všechny multiplikativní. Z nich pouze N, u, I jsou úplně multiplikativní.

Tvrzení. *Multiplikativní aritmetické funkce tvoří podgrupu grupy všech aritmetických funkcí spolu s Dirichletovým násobením.*

Poznámka. Úplně multiplikativní funkce podgrupu netvoří.

Tvrzení. *Pokud je f úplně multiplikativní, pak $f \star (f\mu) = I$.*

Literatura a zdroje

[1] Tom M. Apostol: *Introduction to Analytic Number Theory*, Springer-Verlag, 1976.

[2] Josef Svoboda, Štěpán Šimsa: *PraSečí seriál Teorie čísel 2014*, *http://mks.mff.cuni.cz/archive/33/uvod3s.pdf*

Kruhová inverze

Filip Bialas

Abstrakt. Kruhová inverze je geometrické zobrazení, které umí měnit kružnice na přímky a naopak. Podíváme se, jaká „magie“ se za tím skrývá, a na příkladech si ukážeme, kdy a jakým způsobem je vhodné inverzi použít.

Úmluva. Rovinu rozšíříme o jediný bod ∞, o kterém tvrdíme, že leží na všech přímkách.

Definice. *Kruhová inverze* je geometrické zobrazení dané kružnicí k se středem O a poloměrem r, které bodu X přiřadí bod X' dle následujících pravidel:

(i) Když je $X = O$, potom $X' = \infty$.

(ii) Když je $X = \infty$, potom $X' = O$.

(iii) Jinak je X' bod polopřímky OX, pro který platí $|OX| \cdot |OX'| = r^2$.

Cvičení. Rozmyslete si následující pozorování o kruhové inverzi:

(i) Body kružnice k jsou samodružné.

(ii) Body, které ležely uvnitř kružnice, se zobrazí ven a naopak.

(iii) Dvakrát provedená kruhová inverze dle stejné kružnice je identita.

Tvrzení. (Konstrukce obrazu) *Je dána kružnice k a bod X vně této kružnice. Tečny ke kružnici k vedené bodem X se jí dotýkají v bodech T, U. Pak obraz X' bodu X v kruhové inverzi podle kružnice k je střed úsečky TU.*

Tvrzení. (Tětivové čtyřúhelníky) *Je dána kružnice k se středem O a body A, B takové, že neleží na jedné přímce s O. Označme A', B' obrazy bodů A, B v inverzi podle k. Pak body A, B, A', B' leží na jedné kružnici.*

Lemma. (Přepočítávací lemma) *Je dána kružnice $k(O, r)$ a body X, Y. Označme X', Y' obrazy bodů X, Y v inverzi podle kružnice k. Pak*

(i) $|\sphericalangle OX'Y'| = |\sphericalangle XYO|$,

(ii) $|X'Y'| = |XY| \cdot \dfrac{r^2}{|OX| \cdot |OY|}$.

Tvrzení. (Stěžejní) *Uvažme kruhovou inverzi určenou kružnicí k se středem O. Pak*

(i) *obrazem přímky procházející bodem O je ona sama,*

(ii) *obrazem přímky* **ne***procházející bodem O je kružnice procházející bodem O,*

(iii) *obrazem kružnice procházející bodem O je přímka* **ne***procházející bodem O,*

(iv) *obrazem kružnice* **ne***procházející bodem O je kružnice* **ne***procházející bodem O.*

Cvičení. Jak vypadají kružnice, které kruhová inverze zobrazí na sebe samotné?

Příklady

Nyní zbývá dodat několik závěrečných rad a následujícím příkladům již nic nestojí v cestě.

(1) V celé řadě úloh nezávisí na poloměru kružnice, dle které se provádí inverze. Důležitý bývá hlavně její střed.

(2) Jako střed bývá zpravidla vhodné volit bod, jímž prochází podezřele velké množství kružnic.

(3) Často se vyplatí hledat inverzi, která převádí nějaký objekt ze zadání na jiný.

Příklad 1. Přímka p protne kružnici k v bodech A a B. Označme S střed jednoho z oblouků AB. Uvažme dvě přímky procházející S, které protnou kružnici k v bodech C a D a přímku p v bodech E a F. Dokažte, že body C, D, E a F leží na kružnici.

Příklad 2. Je dán pravoúhlý trojúhelník ABC s pravým úhlem u vrcholu C. Nechť D a E jsou body na úsečkách AC a BC. Dokažte, že paty kolmic vedené z bodu C na přímky AB, AE, BD a DE leží na jedné kružnici.

Příklad 3. Kružnice vepsaná trojúhelníku ABC se dotýká jeho stran BC, CA a AB po řadě v bodech D, E a F. Nechť X je bod uvnitř trojúhelníka ABC takový, že kružnice vepsaná trojúhelníku ABX se dotýká jeho stran v bodech D, G a H. Dokažte, že body E, F, G, H leží na kružnici. (IMO shortlist 1995)

Příklad 4. Nechť ω je kružnice opsaná trojúhelníku ABC. Uvažme kružnici l, která se dotýká stran AB, AC a navíc kružnice ω v bodě T. Dále mějme kružnici připsanou trojúhelníku ABC proti vrcholu A, která se dotýká strany BC v bodě V. Dokažte, že $|\sphericalangle BAT| = |\sphericalangle CAV|$.

Příklad 5. (Ptolemaiova věta) Pro čtyřúhelník se standardním značením délek stran a úhlopříček dokažte, že

$$ac + bd \geq ef,$$

přičemž rovnost nastává právě tehdy, když je čtyřúhelník tětivový.

Příklad 6. Jsou dány dvě pevné kružnice k a l, které se protínají v bodech A a B. Nechť m a n jsou kružnice, které mají s k vnější dotyk, s l mají vnitřní dotyk,

navíc se samy dotýkají v bodě X. Ukažte, že bod X leží na kružnici nezávislé na volbě m a n. (MKS)

Příklad 7. Nechť Ω je kružnice opsaná trojúhelníku ABC. Uvažme kružnici ω, která se dotýká stran AC, BC a navíc má vnitřní dotyk s Ω v bodě P. Přímka rovnoběžná s AB se dotýká ω uvnitř trojúhelníku ABC v bodě Q. Dokažte, že $|\sphericalangle ACP| = |\sphericalangle QCB|$. (EGMO 2013)

Příklad 8. Nechť k_1, k_2, k_3 a k_4 jsou kružnice takové, že k_1 a k_3 mají vnější dotyk v P a k_2 a k_4 mají rovněž vnější dotyk v P. Označme A, B, C, D druhé průsečíky k_1 s k_2, k_2 s k_3, k_3 s k_4 a k_4 s k_1. Dokažte, že platí

$$\frac{|AB| \cdot |BC|}{|AD| \cdot |CD|} = \frac{|PB|^2}{|PD|^2}.$$

(IMO shortlist 2003)

Příklad 9. Nechť k a l jsou dvě kružnice protínající se v bodech A a B. Tečna ke k vedená bodem A protne l podruhé v bodě C. Tečna k l vedená bodem A protne k podruhé v bodě D. Nechť E je bod na polopřímce AB takový, že $|AE| = 2|AB|$. Dokažte, že body A, C, E a D leží na kružnici.

Příklad 10. Kružnice k_1, k_2 a k_3 mají po dvou vnější dotyk. Kružnice l_1 má vnější dotyk s kružnicemi k_1, k_2 a k_3 v bodech K, L a M. Kružnice l_2 má s kružnicemi k_1, k_2 a k_3 vnitřní dotyk v bodech P, Q a R. Dokažte, že se přímky KP, LQ a MR protínají v jednom bodě.

Příklad 11. Kružnice k_1, k_2 a k_3 mají po dvou vnější dotyk. Navíc se všechny tři dotýkají přímky l. Kružnice k o poloměru jedna má vnější dotyk s k_1, s k_2 i s k_3, ale nemá žádný společný bod s přímkou l. Jaká je vzdálenost středu kružnice k od přímky l?

Literatura a zdroje:

Příspěvek byl neotřele zkopírován od Martina Hory z jarního soustředění 2016, kterému tímto děkuji.

[1] Archiv MKS, *http://mks.mff.cuni.cz/archive*
[2] *http://www.artofproblemsolving.com*
[3] *http://www.imomath.com/*
[4] *http://mathcircle.berkeley.edu/*

Factoring lemma

Filip Čermák

Abstrakt. Factoring lemma je jednoduché, ale zároveň velice užitečné lemma, které nám pomůže vyřešit některé příklady z teorie čísel.

Motivační příklad

Mějme a, b, c, d přirozená čísla taková, že $ab = cd$. Dokažte, že $a + b + c + d$ je složené.

Lemma. *Nechť a, b, c, d jsou přirozená čísla, která splňují $ab = cd$. Potom existují přirozená čísla m, n, p, q taková, že $gcd(n, p) = 1$ a*

$$a = mn, \;\; b = pq, \;\; c = mp, \;\; d = nq.$$

Důkaz. Přepišme podmínku $ab = cd$ jako

$$\frac{a}{c} = \frac{d}{b}.$$

Zlomky $\frac{a}{c}$ a $\frac{d}{b}$ umíme převézt do stejného základního tvaru $\frac{n}{p}$. Přepišme vzniklé rovnice a definujme čísla m a q vztahem

$$\frac{a}{n} = \frac{c}{p} = m, \;\; \frac{d}{n} = \frac{b}{p} = q.$$

Zřejmě m a q jsou přirozená čísla, a tedy m, n, p, q mají požadované vlastnosti. □

Řešení. Náš motivační příklad se tedy bude řešit následovně: Z factoring lemmatu víme, že existují přirozená čísla m, n, p, q taková, že $a = mn$, $b = pq$, $c = mp$ a $d = nq$. Potom

$$a + b + c + d = mn + pq + mp + qn = (m + p)(q + n),$$

což je pro přirozená m, n, p, q složené číslo.

Diofantické rovnice

Úloha. Mějme po dvou nesoudělná přirozená čísla a, b, c splňující $a^2 + b^2 = c^2$. Ukažte, že pokud je navíc a liché, pak umíme nalézt taková přirozená u, v, že $a = u^2 - v^2$ a $b = 2uv$.

Řešení. Přepišme si první rovnici jako

$$b^2 = (c - a)(c + a).$$

Díky našemu lemmatu víme, že existují přirozená čísla m, n, p, q taková, že $b = mn = pq$, $c - a = mp$ a $c + a = nq$. Znovu s využitím lemmatu máme, že existují přirozená čísla x, y, z, w taková, že $m = xy$, $n = zw$, $p = xz$, $q = yw$.

Tedy dostaneme $b = xyzw$ a

$$a = \frac{nq - mp}{2} = \frac{yz}{2}(w^2 - x^2).$$

Jelikož víme, že a je liché a navíc w^2 a x^2 jsou modulo 4 kongruentní s 1 nebo 0, tak dvojka dělí pouze yz. Avšak pokud se podíváme na předešlou rovnici, pak $yz \mid 2a$ a zároveň $yz \mid b = xyzw$.

Z toho tedy už nutně plyne, že $yz = 2$. Tím je důkaz hotov.

Příklad 1. Mejmě po dvou nesoudělná přirozená čísla a, b, c splňující rovnici $a^2 + b^2 = 2c^2$. Dokažte, že pak existují přirozená čísla u a v taková, že

$$\begin{aligned} a &= u^2 - v^2 + 2uv, \\ b &= v^2 - u^2 + 2uv, \\ c &= u^2 + v^2. \end{aligned}$$

Příklad 2. Dokažte, že neexistují tři přirozená čísla x, y, z taková, že

$$2(x^4 - y^4) = z^2.$$

SOS a $\mathbb{Z}[i]$

Příklad 3. Nechť (a, b) a (c, d) jsou dvě různé neuspořádané dvojice přirozených čísel splňující $a^2 + b^2 = c^2 + d^2 = k$. Dokažte, že k je složené.

Lemma 4. *Pokud máme $a, b, c, d \in \mathbb{Z}$. Dokažte, že existují celá čísla m, n, p, q taková, že*

$$2a = mn + pq, \;\; 2b = mp - nq, \;\; 2c = mp + nq, \;\; 2d = mn - pq.$$

Tvrzení 5. *Factoring lemma platí také v Euklidovském okruhu $\mathbb{Z}[i]$, což se nám občas může hodit.*

Lemma 6. *Pokud máme a, b, c, d přirozená čísla splňující $a^2+b^2 = cd$, pak ukažte, že existují taková celá čísla x, y, z, w, t, aby platilo*

$$c = t(x^2 + y^2), \;\; d = t(z^2 + w^2), \;\; a = t(xz + yw), \;\; b = t(xw + yz).$$

Příklad 7. Nechť a, b, c jsou přirozená čísla taková, že $ab = c^2 + 1$. Dokažte, že a i b mohou být zapsána jako součet dvou čtverců.

Příklad 8. Dokažte, že každé prvočíslo tvaru $4k+1$ může být zapsáno jako součet dvou čtverců.

Teď už jenom počítání ...

Příklad 9. Najděte všechna celočíselná řešení rovnice $x^2 + 3y^2 = z^2$.

Příklad 10. Dokažte, že pokud a, b, c, d jsou přirozená čísla, $N = a^2 + 2b^2 = = c^2 + 2d^2$ a $\{a, b\} \neq \{c, d\}$, pak N je složené.

Příklad 11. Dokažte, že žádné čtyři čtverce nemohou vytvořit nekonstantní aritmetickou posloupnost.

Příklad 12. (IMO Shortlist, 1998) Najděte všechna přirozená čísla n, pro která existuje přirozené m takové, že

$$2^n - 1 \mid m^2 + 9.$$

Příklad 13. Mějme přirozená čísla a, b, c, d a celé číslo x, pro které platí $(a + b - x)(a + b + x) = 2ab$ a $ac = bd$. Dokažte, že $ad + bc$ je složené číslo.

Příklad 14. Najděte všechna celočíselná řešení rovnice $7x^2 + y^2 = z^2$.

Příklad 15. Najděte všechna přirozená čísla a, b, c, pro která platí, že $a^2 + 1$ i $b^2 + 1$ jsou prvočísla a $(a^2 + 1)(b^2 + 1) = c^2 + 1$.

Příklad 16. Najděte všechna prvočísla p, q taková, že

$$p^2 + 1 = q^7 - q.$$

Příklad 17. Mějme lichá přirozená čísla a, b, c, d, kde $a < b < c < d$ a $ad = bc$. Dokažte, že pokud $a + d = 2^k$ a $b + c = 2^m$ pro nějaká přirozená čísla m a k, pak $a = 1$.

Příklad 18. Pro přirozená čísla a, b, c, d, r, s platí $rab = scd$. Dokažte, že $r(a^2 + b^2) + s(c^2 + d^2)$ není prvočíslo.

Literatura a zdroje

[1] Iurie Boreico, Roman Teleuca: *A Factoring Lemma, Mathematical reflections, 2007.*
[2] Art of problem solving: *https://artofproblemsolving.com/community*
[3] Háňa Bendová: *Factoring lemma*, *https://mks.mff.cuni.cz/library/FactoringLemmaHB/FactoringLemmaHB.pdf*

Návody

1. Factoring lemma.

2. Vezměte si nejmenší trojici a zkuste použít factoring lemma na nalezení menší.

4. Předchozí příklad.

6. Rozklad v $\mathbb{Z}[i]$.

7. Lemma 6.

8. Wilsonova věta.

Harmonické čtveřice

Tonda Češík

Abstrakt. Příspěvek seznamuje s konceptem harmonických poměrů v planimetrii. Uvádí tvrzení, díky nimž lze harmonické konfigurace nacházet v geometrických úlohách olympiádního typu a používat je k často rychlému a elegantnímu řešení. Každá kapitolka obsahuje několik úloh k procvičení dané techniky.

Úmluva. Symbolem AB budeme značit tradičně přímku procházející body A, B a někdy navíc i délku *orientované úsečky* s krajními body A a B.

Dvojpoměr a promítání na přímky

Mějme přímku AB a na ní bod X. Polohu bodu X vzhledem k A a B můžeme vyjádřit tzv. *dělicím poměrem*.

Definice. Nechť X je bod na přímce AB různý od bodů A, B. Dělicí poměr bodu X vzhledem k bodům A a B je číslo $(AB, X) = \frac{AX}{BX}$.

Cvičení. Rozmyslete si, že pro dané body A, B je poloha bodu X hodnotou (AB, X) jednoznačně určena. Kdy je $(AB, X) > 0$?

Vzájemnou polohu čtyř bodů na přímce můžeme popsat podobnou veličinou.

Definice. *Dvojpoměr* bodů A, B, C, D (v tomto pořadí) ležících na jedné přímce je číslo

$$(AB, CD) = \frac{(AB, C)}{(AB, D)} = \frac{AC \cdot BD}{AD \cdot BC}.$$

Cvičení. Dokažte, že

$$(AB, CD) = (CD, AB) = (BA, DC) = \frac{1}{(AB, DC)} = \frac{1}{(DC, AB)} = \frac{1}{(BA, CD)}.$$

Poslední cvičení nám říká, že význačné hodnoty dvojpoměru jsou 1 a -1. Z rovnosti $(AB, CD) = 1$ ovšem plyne, že $A = B$ nebo $C = D$, takže nás bude více zajímat hodnota -1.

Definice. Body A, B, C, D ležící na přímce tvoří *harmonickou čtveřici*, pokud $(AB, CD) = -1$.

Cvičení. Rozmyslete si, jak zhruba harmonické čtveřice vypadají. V jakém pořadí mohou na přímce ležet jejich body?

Tvrzení. *Jsou dány přímky p, q a bod X mimo ně. Bodem X procházejí čtyři přímky, které protínají přímku p postupně v bodech A, B, C, D a přímku q postupně v bodech A', B', C', D'. Potom platí $(AB, CD) = (A'B', C'D')$.*

My budeme toto tvrzení používat hlavně pro promítání harmonických čtveřic. Příslušné čtyři přímky tvoří v tom případě *harmonický svazek*.

Jak poznat harmonickou čtveřici?

To nám velmi usnadní následující tvrzení.

Tvrzení. *V následujících běžných konfiguracích se vyskytují harmonické čtveřice:*

(i) *Pokud M je střed AB, pak $(AB, M\infty) = -1$.*
(ii) *Ceviány AD, BE, CF se protínají v P. Označme $D' = EF \cap BC$. Pak $(BC, DD') = -1$.*
(iii) *Na průměru AB kružnice k se středem O je dán bod X. Je-li X' jeho obraz v kruhové inverzi podle k (tj. platí-li $|OX| \cdot |OX'| = |OA|^2 = |OB|^2$), pak $(AB, XX') = -1$.*

Tvrzení. („Dvě ze tří“) *Nechť A, B, C, D leží na přímce a P mimo ni. Pak z libovolných dvou následujících bodů plyne třetí:*

(i) $(AC, BD) = -1$,
(ii) $|\sphericalangle APC| = 90°$,
(iii) $|\sphericalangle BPC| = |\sphericalangle CPD|$, *kde úhly chápeme orientovaně.*

A konečně jsou tady…

Úlohy I

Úloha 1. Mějme trojúhelník ABC, bod I je jeho vepsiště, bod I_a jeho A-připsiště, D je průsečík osy úhlu u A a strany BC. Dokažte, že $(AD, II_a) = -1$.

Úloha 2. Ceviány AD, BE, CF se protínají v P. Označme $Q = BC \cap EF$, $R = AD \cap EF$, $S = CF \cap BR$ a $T = DF \cap BR$. Ukažte, že

$$(QR, EF) = (AP, DR) = (CS, PF) = (BS, RT) = -1.$$

Úloha 3. Body D, E, F jsou zvoleny postupně na stranách BC, CA, AB trojúhelníku ABC tak, že $AD \cap BE \cap CF = K$. Přímka FD protíná přímku BE v bodě X, P je střed úsečky AK a EP protíná přímku AB v bodě Y. Dokažte $XY \parallel AD$.

Úloha 4. Na přímce p jsou dány body B, D, C v tomto pořadí. Dokažte, že všechny body A takové, že AD je osa úhlu BAC, leží na pevné kružnici (tzv. *Apolloniově kružnici*).

Úloha 5. (Blanchet Theorem) Na A-výšce AD trojúhelníka ABC je dán bod P. Označme $X = BP \cap AC$, $Y = CP \cap AB$. Dokažte $|\sphericalangle XDA| = |\sphericalangle YDA|$.

Úloha 6. Je dán trojúhelník ABC, body dotyku kružnice vepsané se stranami BC, CA, AB označme postupně D, E, F. Bod X leží uvnitř trojúhelníku ABC tak, že kružnice vepsaná trojúhelníku XBC se dotýká jeho stran v bodech D, Y a Z. Dokažte, že E, F, Y, Z leží na jedné kružnici. (IMO Shorlist 1995)

Úloha 7. V trojúhelníku ABC označme D patu osy úhlu u A a I_b, I_c vepsiště trojúhelníků ABD, ACD.

(1) Je-li $Q = BC \cap I_bI_c$, dokažte $|\sphericalangle DAQ| = 90°$. (Sharygin 2013)
(2) Označíme-li průsečíky I_bI_c s AB, AC postupně M, N, dokažte, že MC a NB se protnou na AD.

Úloha 8. Je dána kružnice ω se středem O a tětivou AB ($O \notin AB$). Bod C leží na ω tak, že AC půlí úsečku OB. Označme $D = AB \cap OC$ a $F = BC \cap AO$. Dokažte, že $|AF| = |CD|$.

Harmonické čtyřúhelníky

Užitečným nástrojům není zdaleka konec. Co zkusit promítat na kružnice?

Tvrzení. *Je dán bod P ležící na kružnici k a mimo přímku p. Přímky a, b, c, d protnou p v A', B', C', D' a k v A, B, C, D. Pak platí*

$$|(A'B', C'D')| = \frac{|AC| \cdot |BD|}{|AD| \cdot |BC|}.$$ [1]

Definice. Řekneme, že tětivový čtyřúhelník $ABCD$ je *harmonický*, pokud pro délky jeho stran platí $ac = bd$.

Pozorování. *S použitím předchozího tvrzení si snadno rozmyslíme, že čtyřúhelník $ABCD$ vepsaný do kružnice ω je harmonický právě tehdy, když pro libovolný bod $P \in \omega$ tvoří přímky PA, PB, PC, PD harmonický svazek.*[2]

Tvrzení. (O harmonických čtyřúhelnících) *Buď D bod na oblouku BC kružnice k opsané trojúhelníku ABC, který neobsahuje bod A. Pak následující tvrzení jsou ekvivalentní:*

(i) *Čtyřúhelník $ABDC$ je harmonický.*
(ii) *Přímka AD je A-symediána v $\triangle ABC$ (tedy přímka symetrická s A-těžnicí podle osy úhlu u A).*
(iii) *Přímka AD a tečny ke k skrz B a C procházejí jedním bodem.*

Cvičení. Úhlopříčky tětivového čtyřúhelníku $ABCD$ se protínají v P. Dokažte, že pokud je BP symediána v ABC, pak AP je symediána v ABD.

(Rumunsko TST 2006)

[1] Obecnější tvrzení bez absolutních hodnot také platí, ale potřebovali bychom k jeho formulaci komplexní čísla.

[2] Pokud například $P = A$, uvažujeme místo PA tečnu k ω v bodě A.

Pojďme to vyzkoušet!

Úlohy II

Úloha 9. Kružnice vepsaná rovnoramennému trojúhelníku ABC ($|AB| = |AC|$) se dotýká AC v E. Přímka různá od BE vedená bodem B protíná kružnici vepsanou v bodech F, G. Přímky EF, EG protnou BC v K, L. Dokažte $|BK| = |CL|$.
(MEMO 2008)

Úloha 10. V trojúhelníku ABC platí $|AC| = 2|AB|$. Označme P průsečík tečen k jemu opsané kružnici ω vedených body A a C. Dokažte, že průsečík přímky BP a osy strany BC leží na kružnici ω. (ČR TST 2012)

Úloha 11. Paty kolmic z bodu D tětivového čtyřúhelníku $ABCD$ na přímky BC, CA, AB označme postupně P, Q, R. Dokažte, že $|PQ| = |QR|$ právě tehdy, když se osy úhlů $\sphericalangle ABC$ a $\sphericalangle ADC$ protínají na úhlopříčce AC. (IMO 2003)

Úloha 12. V tětivovém pětiúhelníku $ABCDE$ platí $AC \parallel DE$ a střed M tětivy BD splňuje $|\sphericalangle AMB| = |\sphericalangle BMC|$. Dokažte, že BE půlí tětivu AC.

Návody

1. Využijte tvrzení „dvě ze tří“.

2. Vždy najděte správný bod, z nějž promítat.

3. Najděte harmonický svazek vycházející z Y.

4. Dokreslete čtvrtého do party k B, D, C a využijte tvrzení „dvě ze tří“.

5. Zkombinujte konfiguraci „Ceva–Mene“ a tvrzení „dvě ze tří“.

6. Čtvrtý do party k B, D, C a mocnost.

7. (1) Kde je čtvrtý do party k I_bI_c a $X = AD \cap I_bI_c$? (2) Pokud mají dvě harmonické čtveřice společný bod, pak spojnice zbylých tří odpovídajících si dvojic procházejí jedním bodem.

8. Dokažte sporem(!), že $OB \parallel FD$.

9. Označte zbylé body dotyku, najděte harmonický čtyřúhelník a promítněte ho.

10. Dokažte, že BX, kde X je průnik osy BC a ω, je symediána v ABC.

11. Dokažte, že oba výroky jsou ekvivalentní s tím, že $ABCD$ je harmonický.

12. Začněte tím, že AC je symediána v ABD.

Literatura a zdroje

Tento příspěvek je zkrácenou verzí příspěvku *Davida Hrušky*, kterému tímto děkuji.

[1] David Hruška: *Harmonické čtveřice*, Sborník MKS, Zásada 2014
[2] Pepa Tkadlec: *Dvoupoměr a poláry*, Sborník *i*KS, 2013

Základní grafové algoritmy

Petr Gebauer

Abstrakt. Na přednášce se seznámíme s několika algoritmy, které nám pomáhají udělat si lepší představu o struktuře grafu, např. nám jej rozdělí na části s nějakou vlastností, určí vzdálenosti v něm nebo nám zvolí nejmenší část, která nějakým způsobem drží graf pohromadě.

Prosvištíme si slovíčka:

Ne/orientovaný graf, podgraf, sled, tah, cesta, délka cesty, ne/orientovaný cyklus, silná souvislost, slabá souvislost, vzdálenost, strom; asymptotická časová a asymptotická paměťová složitost.

Definice. *Topologické uspořádání* orientovaného grafu $G = (V, E)$ je prosté zobrazeni $t : V \to \{1, 2, \ldots, |V|\}$ takové, že pro každou hranu $(u, v) \in E$ je $t(u) < t(v)$. Neformálně se na něj můžeme dívat jako na pořadí jeho vrcholů.

Definice. Orientovaný graf $G = (V, E)$ je *slabě souvislý*, pokud je souvislý neorientovaný graf $G' = (V, E')$, kde $\{u, v\} \in E' \Leftrightarrow (u, v) \in E \vee (v, u) \in E$. Dále řekneme, že G je *silně souvislý* pokud pro každé dva různé vrcholy u, v existuje v G orientovaná cesta z u do v a orientovaná cesta z v do u.

Definice. *Komponenta* (silné nebo slabé souvislosti v případě orientovaného grafu) grafu $G = (V, E)$ je takový podgraf $K = (V', E')$, který je souvislý, ale pro každý vrchol $v \in V$ je každý podgraf obsahující všechny vrcholy množiny $V' \cup \{v\}$ nutně nesouvislý.

Úmluva. Všechny grafy, které budeme uvažovat, jsou konečné.

Dekompozice a cykly

Cvičení. Rozmyslete si, že orientovaný graf má topologické uspořádání právě tehdy, když neobsahuje (orientovaný) cyklus.

Algoritmus. (DFS – prohledávání do hloubky aka Depth-first search):
Vstup: Graf $G = (V, E)$ a počáteční vrchol $v_0 \in V$.

(1) Pro všechny vrcholy v:
(2) stav(v) $\leftarrow$ nenalezený,
(3) in(v), out(v) $\leftarrow$ nedefinováno,
(4) $T \leftarrow 0$.
(5) Zavoláme DFS-Návštěva(v_0).

Procedura **DFS-Návštěva**(v):

(1) stav(v) $\leftarrow$ otevřený,
(2) $T \leftarrow T + 1$, in(v) $\leftarrow T$.
(3) Pro všechny následníky w vrcholu v:
(4) Je-li stav(w) = nenalezený, zavoláme DFS-Návštěva(w).
(5) Stav(v) $\leftarrow$ uzavřený,
(6) T $\leftarrow T + 1$, out(v) $\leftarrow T$.

Algoritmus. (DFSr – opakovaná (repeat) verze DFS):
Vstup: Graf $G = (V, E)$.

(1) $v_0 \leftarrow$ libovolný vrchol G,
(2) DFS(v_0),
(3) Pro každý vrchol $v \in V$:
(4) Je-li stav(v) = nenalezený, zavoláme DFS-Návštěva(v).

Poznámka. DFS běží v čase $\Theta(n + m)$.

Definice. Klasifikujme si hrany podle stavu koncových vrcholů v okamžiku, kdy DFS hranou poprvé prochází.

Hranu (u, v) nazveme:

- *stromovou*, pokud byl v nenalezený - pak $\text{in}(u) < \text{in}(v)$, $\text{out}(u) > \text{out}(v)$,
- *zpětnou*, pokud byl v otevřený, pak $\text{in}(u) > \text{in}(v)$, $\text{out}(u) < \text{out}(v)$,
- *dopřednou*, pokud byl v uzavřený a $\text{in}(v) > \text{in}(u)$, pak $\text{out}(u) > \text{out}(v)$,
- *příčnou*, pokud byl v uzavřený a $\text{in}(v) < \text{in}(u)$, pak $\text{out}(u) > \text{out}(v)$.

Tvrzení. *Mějme acyklický orientovaný graf G (DAG – directed acyclic graph). Spusťme DFSr na G. Pak seřazení vrcholů sestupně podle out(v) je topologické uspořádání G.*

Cvičení. Mějme orientovaný graf G. Označme G' graf, jehož vrcholy jsou komponenty silné souvislosti G a z vrcholu u do vrcholu v grafu G' vede hrana právě tehdy, když existuje v G hrana vedoucí z komponenty u do komponenty v. Rozmyslete si, že G' je acyklický.

Definice. Komponentu nazveme *zdrojovou*, pokud **do** ní nevede žádná hrana, a *stokovou*, pokud nevede žádná hrana **z** ní.

Tvrzení. *Nechť C_1, C_2 jsou komponenty grafu G takové, že z C_1 do C_2 vede hrana. Pak při spuštění (opakovaného) DFS na grafu G platí $max_{v\in C_1} out(v) > max_{v\in C_2} out(v)$.*

Důkaz rozborem podle pořadí procházení C_1, C_2.

Cvičení. (lehké) Mějme graf G. Nechť G^T značí graf, který vznikne z G otočením směru všech hran. Rozmyslete si, ze G^T má stejné komponenty jako G.

Speciálně tedy vrchol s největším out(v) leží ve zdrojové komponentě.

Algoritmus. (KompSilnéSouvislosti)
Vstup: Orientovaný graf G.

(1) Sestrojíme graf G^T s obrácenými hranami.
(2) Z ← prázdný zásobník.
(3) Pro všechny vrcholy v nastavíme komp(v) ← nedefinováno.
(4) Spouštíme DFS v G^T opakovaně dokud neprozkoumáme všechny vrcholy. Kdykoliv přitom opouštíme vrchol, vložíme ho do Z. Vrcholy v zásobníku jsou tedy setřízené podle out(v).
(5) Postupně odebíráme vrcholy ze zásobníku Z a pro každý vrchol v:
(6) Pokud komp(v) = nedefinováno:
(7) Spustíme DFS(v) v G, přičemž vstupujeme pouze do vrcholů s nedefinovanou hodnotou komp$(\dots)$ a tuto hodnotu přepisujeme na v.

Výstup: Pro každý vrchol v vrátíme identifikátor komponenty komp(v).
Uvedený algoritmus najde komponenty silné souvislosti v čase $\Theta(n+m)$.

Krátce o nejkratších cestách

Cvičení. Najděte (neohodnocený) graf a dva jeho vrcholy u a v tak, že při nějakém pořadí procházení hran v něm DFS najde cestu z u do v, která nebude nejkratší.

Algoritmus. (BFS – prohledávání do šířky aka Breadth-first search):
Vstup: Graf $G = (V, E)$ a počáteční vrchol $v_0 \in V$.

(1) Pro všechny vrcholy v:
(2) stav(v) ← nenalezený,
(3) $D(v) = \emptyset$, $P(v) \leftarrow \emptyset$.
(4) Stav(v_0) ← otevřený,
(5) $D(v_0) \leftarrow 0$.
(6) Založíme frontu Q a vložíme do ní vrchol v_0 .
(7) Dokud je fronta Q neprázdná:

(8) Odebereme první vrchol z Q a označíme ho v.
(9) Pro všechny následníky w vrcholu v:
(10) Je-li stav(w) = nenalezený:
(11) stav$(w) \leftarrow$ otevřený,
(12) $D(w) \leftarrow D(v) + 1$, $P(w) \leftarrow v$.
(13) Přidáme w do Q.
(14) Stav$(v) \leftarrow$ uzavřený.

Cvičení. Rozmyslete si, že BFS běží v čase $\Theta(m + n)$.

Definice. *Ohodnocením hran* v grafu $G = (V, E)$ nazýváme zobrazení $d : E \to \mathbb{R}$. *Délkou cesty* p obsahující právě hrany $e_1, \ldots, e_k$ vzhledem k ohodnocení d je $d(e_1) + \cdots + d(e_k)$. Vzdálenost z vrcholu u do vrcholu v v ohodnocení d je délka nejkratší cesty z u do v vzhledem k ohodnocení d.

Cvičení. (pro pokročilé) Mějme graf G, ve kterém jsou hrany ohodnocené k různými nezápornými čísly (k je poměrně malé). Najděte algoritmus, který pro dva různé vrcholy u, v z G najde nejkratší cestu z u do v v čase $O(k \cdot (n + m))$. Jak to udělat v čase $O(\log(k) \cdot (n + m))$?

Pár příkladů

Cvičení. Upravte DFS tak, aby pro zadaný graf G a jeho hranu e zjistilo, zda se e nachází v nějakém cyklu G.

Cvičení. Mějme orientovaný graf a některé vrcholy v něm označené. Najděte algoritmus běžící v čase $O(n + m)$, který zjistí, zda některý z označených vrcholů je v orientovaném cyklu. Proč nefunguje přímočaré použití DFS?

Cvičení. Rozmyslete si, které grafy mají jednoznačné topologické uspořádání.

Cvičení. Orientovaný graf nazveme *polosouvislým*, pokud pro každé dva různé vrcholy u, v v něm existuje orientovaná cesta z u do v nebo z v do u. Navrhněte algoritmus, který umí zjistit, zda je zadaný graf polosouvislý. Proč nepožaduji rozklad na komponenty polosouvislosti?

Minimální kostry

Definice. *Kostra* (neorientovaného) grafu je jeho podgraf, který je strom a obsahuje všechny vrcholy. Minimální kostra vzhledem k ohodnocení hran je taková kostra, kde součet ohodnocení všech jejích hran je ze všech koster nejmenší.

Definice. Mějme graf $G = (V, E)$. Množinu $R \subseteq E$ nazveme *řezem*, pokud graf $(V, E \setminus R)$ není souvislý. Pokud existuje množina $M \subseteq V$ taková, že každá $e \in R$ má jeden konec v M a druhý v $V \setminus M$, nazýváme R *elementárním*.

Budeme uvažovat pouze grafy, ve kterých žádné dvě hrany nemají stejné ohodnocení.

Lemma. (řezové) *Nechť G je souvislý graf s unikátně ohodnocenými hranami a R jeho elementární řez. Pak každá minimální kostra obsahuje nejlehčí hranu R (tj. hranu R s nejmenším ohodnocením).*

Algoritmus. (Jarníkův)
Vstup: Souvislý graf s váhovou funkcí w.

(1) Pro všechny vrcholy v:
(2) stav$(v) \leftarrow$ mimo,
(3) $h(v) \leftarrow +\infty$,
(4) $p(v) \leftarrow$ nedefinováno,
(5) $v_0 \leftarrow$ libovolný vrchol grafu,
(6) $T \leftarrow$ strom obsahující vrchol v_0 a žádné hrany,
(7) stav$(v_0) \leftarrow$ soused,
(8) h$(v_0) \leftarrow 0$.
(9) Dokud existují nějaké sousední vrcholy:
(10) Označme u sousední vrchol s nejmenším $h(u)$.
(11) Stav$(u) \leftarrow$ uvnitř,
(12) přidáme do T hranu $\{u, p(u)\}$, pokud je $p(u)$ definováno.
(13) Pro všechny hrany uv:
(14) Je-li stav$(v) \in$ {soused, mimo} a $h(v) > w(uv)$:
(15) stav$(v) \leftarrow$ soused,
(16) $h(v) \leftarrow w(uv)$,
(17) $p(v) \leftarrow u$.

Výstup: Minimální kostra T.
Jarníkův algoritmus s haldou běží v čase $\Theta(m \cdot \log(n))$.

Cvičení. Rozmyslete si, že minimální kostra grafu s unikátně ohodnocenými hranami je jednoznačně určená.

Literatura a zdroje

[1] Martin Mareš, Tomáš Valla: *Průvodce labyrintem algoritmů*, CZ.NIC, 2017 (v době přednášky dostupné z https://knihy.nic.cz/files/edice/pruvodce_labyrintem_algoritmu.pdf)

[2] Cvičení Vikiho Němečka z ADS a cvičení Martina Mareše z programování na Matfyzu.

Švrčkův bod

„madam Verča“ Hladíková

Abstrakt. Příspěvek shrnuje základní vlastnosti středu oblouku kružnice, tzv. Švrčkova bodu. Tento bod figuruje v mnoha geometrických úlohách a jeho dobrá znalost je tedy pro úspěch při řešení velmi užitečná. To vše v příspěvku ilustruje řada příkladů.

Ještě než stočíme pozornost ke Švrčkovu bodu, připomeneme si několik základních vlastností os úhlu, středu kružnice vepsané a středů kružnic připsaných. Poté zformulujeme a dokážeme pár užitečných tvrzení o Švrčkově bodu a využijeme je při řešení úloh.

Definice a značení

Definice. Nechť je trojúhelník ABC vepsaný do kružnice ω. Střed oblouku BC, který neobsahuje A, označme $\check{S}_a$ a říkejme mu *Švrčkův bod* trojúhelníka ABC vzhledem k A. Body $\check{S}_b$, $\check{S}_c$ definujme analogicky.

V trojúhelníku ABC označme ω kružnici opsanou, I střed kružnice vepsané, $\check{S}_a$, $\check{S}_b$, $\check{S}_c$ odpovídající Švrčkovy body, E_a, E_b, E_c odpovídající středy kružnic připsaných s poloměry r_a, r_b, r_c a konečně AD, BE, CF osy úhlů v $\triangle ABC$, kde $D \in BC$, $E \in AC$, $F \in AB$.

Osy úhlu, středy kružnice vepsané a kružnic připsaných

Tvrzení 1. *Kolem středů kružnice vepsané a kružnic připsaných jsou úhly*

(i) $|\sphericalangle BIC| = 90^\circ + \frac{\alpha}{2}$ a $|\sphericalangle BIF| = 90^\circ - \frac{\alpha}{2}$,

(ii) $|\sphericalangle AE_aB| = \frac{\gamma}{2}$ a $|\sphericalangle BE_aC| = 90^\circ - \frac{\alpha}{2}$.

Tvrzení 2. (O ose vnitřního úhlu)

$$\frac{|BD|}{|DC|} = \frac{|AB|}{|AC|}.$$

Základní vlastnosti Švrčkova bodu

Tvrzení 3. *V trojúhelníku ABC se osa úhlu BAC a osa strany BC protínají na kružnici ω. Jejich průsečíkem je $\check{S}_a$.*

Tvrzení 4. *Body B, C, I, E_a leží na jedné kružnici se středem $\check{S}_a$. Platí tedy $|\check{S}_aI| = |\check{S}_aB| = |\check{S}_aC| = |\check{S}_aE_a|$.*

Tvrzení 5. *Bodem $\check{S}_a$ veďme polopřímky p a q, které protnou stranu BC postupně v bodech X a Y a kružnici ω protnou podruhé postupně v Z a W. Pak body X, Y, Z, W leží na jedné kružnici.*

Tvrzení 6. *V trojúhelníku ABC platí $|\check{S}_aD| \cdot |\check{S}_aA| = |\check{S}_aI|^2 = |\check{S}_aC|^2 = |\check{S}_aB|^2$.*

Tvrzení 7. *Je dán trojúhelník ABC a kružnice ω_1, která má vnitřní dotyk s kružnicí ω v bodě A a se stranou BC v bodě D'. Pak $D = D'$.*

Příklady

Příklad 8. Je dán trojúhelník ABC. Označme O střed kružnice opsané trojúhelníku BCI. Dokažte, že $|\sphericalangle OKB| = |\sphericalangle OLC|$, kde K, L jsou body dotyku kružnice vepsané ABC po řadě se stranami AB, AC. (China girls 2012/5)

Příklad 9. Čtyřúhelník $ABCD$ je vepsán do kružnice ω. Středy sousedních oblouků AB, BC, CD, DA označme postupně $\check{S}_a$, $\check{S}_b$, $\check{S}_c$, $\check{S}_d$. Dokažte, že přímky $\check{S}_a\check{S}_c$ a $\check{S}_b\check{S}_d$ jsou na sebe kolmé.

Příklad 10. V trojúhelníku ABC s běžným značením ukažte, že I je ortocentrem trojúhelníka $\check{S}_a\check{S}_b\check{S}_c$.

Příklad 11. Označme $\check{S}'_a$ průsečík osy vnějšího úhlu u vrcholu A a osy protější strany. Ukažte, že tento „Antišvrk“

(i) leží na kružnici opsané trojúhelníku ABC,

(ii) leží ve středu E_bE_c,

(iii) jeho vzdálenost od přímky BC je $\frac{r_b+r_c}{2}$.

Příklad 12. Je dán trojúhelník ABC se středem kružnice vepsané I a vnitřním bodem P. Platí

$$|\sphericalangle PBA| + |\sphericalangle PCA| = |\sphericalangle PBC| + |\sphericalangle PCB|.$$

Ukažte, že $|AP| \geq |AI|$, přičemž rovnost nastává, právě když $P = I$. (IMO 2006)

Příklad 13. Nechť jsou AL a BK osy úhlů nerovnoramenného trojúhelníka ABC (L leží na straně BC, K leží na straně AC). Osa úsečky BK protne přímku AL v bodě M. Bod N leží na přímce BK a platí, že LN je rovnoběžná s MK. Dokažte, že $|LN| = |NA|$. (Junior Balkan 2010)

Příklad 14. Kružnice ω_1 a ω_2 mají vnější dotyk v bodě T a obě se vnitřně dotýkají kružnice ω postupně v bodech R a S. Buď Q druhý průsečík RT a ω. Ukažte, že $|\sphericalangle QST| = 90°$. (KMS)

Příklad 15. Nechť BC je průměr kružnice k se středem O. Dále buď A bod na k takový, že $|\sphericalangle AOB| < 120°$, a D buď střed toho oblouku AB, který neobsahuje C. Rovnoběžka s DA vedená bodem O protne AC v bodě I. Osa úsečky OA protne k v bodech E a F. Ukažte, že I je středem kružnice vepsané trojúhelníku CEF. (IMO 2002)

Příklad 16. V trojúhelníku ABC dokažte při zavedeném značení následující metrické vztahy:

(i) $|A\check{S}_a| \cdot |AD| = |AI| \cdot |AE_a| = |AB| \cdot |AC|$,

(ii) $|IA| \cdot |E_aD| = |E_aA| \cdot |ID|$.

Příklad 17. Nechť ABC je ostroúhlý trojúhelník ($|AB| \neq |AC|$). Kružnice nad průměrem BC protne strany AB a AC postupně v bodech M a N. Označme O střed strany BC a R průsečík os úhlů BAC a MON. Dokažte, že kružnice opsané trojúhelníkům BMR a CNR se protínají na straně BC. (IMO 2004)

Příklad 18. Trojúhelník ABC splňuje vztah $|AC|+|BC| = 3|AB|$. Kružnice jemu vepsaná se středem I se dotýká stran BC a CA postupně v bodech D a E. Nechť K, L jsou obrazy bodů D, E ve středové souměrnosti podle I. Ukažte, že body A, B, K a L leží na jedné kružnici. (IMO shortlist 2005)

Příklad 19. Je dán trojúhelník ABC se středem I kružnice vepsané a kružnicí opsanou Γ. Přímka AI protne kružnici Γ podruhé v bodě D. Buď E bod na oblouku BDC a F bod na úsečce BC takový, že $|\sphericalangle BAF| = |\sphericalangle CAE| < \frac{1}{2}|\sphericalangle BAC|$. Dále buď G střed úsečky IF. Dokažte, že přímky EI a DG se protínají na kružnici Γ. (IMO 2010)

Příklad 20. Přímka ℓ protíná kružnici Γ v bodech A, B. Kružnice Γ_1 a Γ_2 jsou vepsané do stejné úseče určené přímkou ℓ a mají vnější dotyk. Dokažte, že jejich vnitřní společná tečna prochází pevným bodem, pohybují-li se Γ_1, Γ_2 ve vymezené úseči. (Prasolov)

Příklad 21. Je dán trojúhelník ABC, jeho kružnice opsaná ω a bod D na straně BC. Buď ω_1 kružnice dotýkající se úsečky AD v bodě F, strany BC bodě E a kružnice ω v bodě K. Dokažte, že střed I kružnice vepsané $\triangle ABC$ leží na přímce EF. (Sawayama-Thebault theorem, PraSe 29/myšmaš)

Návody

8. Všimněte si, že na poloze bodů B, C příliš nezáleží, úloha je symetrická podle osy úhlu.

9. Úhel mezi $\check{S}_a\check{S}_c$ a $\check{S}_b\check{S}_d$ je součet velikostí oblouků nad $\check{S}_a\check{S}_b$ a nad $\check{S}_c\check{S}_d$. Jakou část kružnice tyto oblouky dohromady zabírají?

10. Úhel mezi $\check{S}_b\check{S}_c$ a $A\check{S}_a$ je součet velikostí oblouků nad $A\check{S}_c$ a nad $\check{S}_a\check{S}_b$. Jakou část kružnice tyto oblouky dohromady zabírají?

11. (ii) Použijte střední příčky v trojúhelníku $E_aE_bE_c$ (případně kružnici devíti bodů).

12. Dokažte, že P leží na kružnici opsané trojúhelníku BIC, a využijte trojúhelníkovou nerovnost.

13. Ukažte, že M je Švrčkův bod nějakého trojúhelníku, a pak to ukažte i pro N.

14. Protněte společnou tečnu ω_1, ω_2 s kružnicí ω a dokažte, že Q je Švrčkův bod nějakého trojúhelníku.

15. Bod A je Švrčkův bod v trojúhelníku CEF, takže stačí dokázat, že I leží na kružnici se středem v A procházející body E, F. Dokažte, že $|AF|$ i $|AI|$ je poloměr kružnice k.

16. Hledejte podobnosti trojúhelníků.

17. Ukažte, že R je Švrčkův bod trojúhelníku AMN.

18. Tipněte si, kde leží střed kružnice, a převeďte úlohu na počítání vzdáleností.

19. Dokreslete E_a, abyste se zbavili bodu G.

20. Použijte tvrzení 7, tvrzení 5 a mocnost bodu ke kružnici.

21. Protněte osu úhlu u vrcholu A s EF (dokreslete i Švrčkův bod) a využijte tvrzení 6. Po využití mocnosti bodu ke kružnici a tvrzení 7 už stačí jen úhlit.

Literatura a zdroje

Tento příspěvek je z větší části převzatý z příspěvku *Švrčkův bod* od Štěpána Šimsy, jemuž tímto děkuji.

[1] Štěpán Šimsa, *Švrčkův bod*, 2015 Staré město,

[2] Martina Vaváčková, *Švrčkův bod*, *http://mks.mff.cuni.cz/library/*,

[3] Michal Rolínek, Josef Tkadlec: *The Š point*, *www.onlinemathcircle.com*.

P+R

Honza „Fanda“ Krejčí

Abstrakt. Cílem této přednášky je ukázat, k čemu jsou dobré řady především při aproximaci funkcí. Přednáška je především zamýšlená jako motivační, tedy některé věci nebudou dokázány.

Jak už bylo zmíněno v abstraktu, konečným cílem bude aproximace funkcí na okolí bodu. Začneme tím, že si řekneme něco o posloupnostech čísel a pak začneme aproximovat. Ukážeme si Taylorův polynom a co vlastně taková věc umí. Zadaří-li se, tak dokonce něco sami zaproximujeme.

Řady čísel

Příklad. Jak sčítat mocniny?

(1) Jaký je součet $1 + 2 + \cdots + n$?

(2) A co $1^2 + 2^2 + \cdots + n^2$?

(3) Nakonec, v závislosti na prvních $k - 1$ součtech, jaký je součet

$$1^k + 2^k + \cdots + n^k?$$

Definice. (Posloupnost) Formálně řečeno, *posloupnost* je zobrazení, které každému přirozenému číslu přiřadí nějaké reálné číslo: $n \mapsto a_n$. Posloupnost také značíme $\{a_n\}_{n=1}^{\infty}$. Řekneme, že posloupnost *konverguje* k číslu A, pokud

$$\forall \varepsilon > 0 \exists n_0, \text{ tak, že } \forall n \geq n_0, |A - a_n| < \varepsilon.$$

Neformálně si lze posloupnost představovat jako uspořádanou množinu prvků. Posloupnost pak konverguje k A, pokud pro libovolně široký interval $(A - \varepsilon, A + \varepsilon)$ najdeme index tak, že žádný prvek z posloupnosti, který má index vyšší než n_0, z tohoto pásu nevypadne.

Cvičení. Co pro posloupnost celých čísel znamená, že konverguje?

Příklad. (součet aritmetické a geometrické posloupnosti) Dokažte pro $a, c \in \mathbb{R}$, $q \neq 1$:

(1) $a + (a + c) + (a + 2c) + \cdots + (a + (n - 1)\, c) = \frac{n}{2}\,(2a + (n - 1)\, c)$,

(2) $a + aq + aq^2 + \cdots + aq^{n-1} = a\frac{q^n-1}{q-1}$.

Poznámka. Posloupnosti, kterou sčítáme jako první v příkladu výše, se říká *aritmetická posloupnost* a té druhé *geometrická posloupnost*. Číslům c a q se postupně říká *diference* a *kvocient*.

Příklad. Jak jsou na tom s konvergencí posloupnosti:

(1) $\{n\}_{n=1}^{\infty}$,
(2) $\{\frac{1}{n}\}_{n=1}^{\infty}$.
(3) geometrická posloupnost (v závislosti na kvocientu),
(4) $\sqrt{n+1} - \sqrt{n}$?

To je hezké, ale jsou na to i příklady v olympiádě?

Příklad. Víme, že celá čísla a a b splňují, že pro každé n je $2^n a + b$ čtverec nějakého celého čísla. Ukažte, že pak $a = 0$. (Polské výběrko)

Příklad. Mějme reálné polynomy f a g stejného stupně. Pro každé reálné x platí: pokud $f(x)$ je celé číslo, pak je i $g(x)$. Dokažte, že existují celá m, n, pro která $g(x) = mf(x) + n$ pro všechna reálná x. (Bulharská olympiáda)

Definice. (řada) Mějme posloupnost $\{a_n\}$. Symbolem $\sum_{i=1}^{\infty} a_i$ označujeme *nekonečnou řadu*. Dále, vztahem $S_n = \sum_{i=1}^{n} x_i$ definujeme *n-tý částečný součet* této řady. Řekneme, že řada S je *konvergentní* a má součet M, pokud $\lim_{n\to\infty} S_n = M$. Řekneme, že řada je *absolutně konvergentní*, pokud je konvergentní řada $\sum_{i=1}^{\infty} |a_i|$.

Věta. (vztah konvergence a absolutní konvergence) *Je-li řada absolutně konvergentní, pak je také konvergentní.*

Příklad. (nutná podmínka konvergence řady) Pokud je součet řady konečný, pak $\lim_{n\to\infty} a_n = 0$.

Příklad. Jaký součet má řada $\sum_{k=0}^{\infty}(-1)^k = 1 - 1 + 1 - 1 + \ldots$?

Věta. (rozdíl mezi absolutní a neabsolutní konvergencí) *Mějme řadu $\sum_{i=1}^{\infty} a_i$. Konverguje-li řada absolutně, pak i její libovolné přerovnání konverguje absolutně a má stejný součet. Pokud řada konverguje, ale nekonverguje absolutně, pak pro každé číslo $s \in \mathbb{R} \cup \{\pm\infty\}$ existuje takové přeuspořádání řady, že její součet je roven s.*

Řady funkcí

Tak jako jsme zavedli ne/konečné řady čísel, umíme stejně zavést řady funkcí. Řada je pak také funkcí, jejíž funkční hodnota v bodě je dána součtem hodnot funkcí řady v daném bodě. Je důležitou otázkou, zda je tato hodnota vůbec definována (viz $\sum_{k=0}^{\infty}(-1)^k$).

Jednoduchým případem (konečné) řady jsou polynomy. Vzhledem k tomu, že polynom je součet konečně mnoha čísel, tak jemu odpovídající řada je definována

na celé reálné přímce. U řad, kde nemáme pouze konečně mnoho nenulových členů, je otázka toho, kdy je součet řady definován, těžší.

Aproximace pomocí polynomů

Motivace. Jednou z důležitých otázek části matematiky je, jak aproximovat složitý objekt jednodušším. V případě reálných funkcí je to např. aproximace funkce pomocí polynomů.

Příklad. Mějme danou (dostatečně hladkou) funkci f definovanou na intervalu $[-1,1]$. My o ní však víme jenom to, jak se chová v bodě 0. Cílem je najít polynom stupně nejvýše n, který co nejlépe aproximuje funkci na okolí bodu 0.

Idea je vcelku jednoduchá. Abychom dosáhli co nejlepší aproximace, chceme, aby se funkční hodnota polynomu v nule shodovala s funkční hodnotou f. Pak budeme chtít, aby se funkční hodnoty polynomu na okolí daného bodu měnily stejně rychle jako daná funkce (aby nám z něj neutíkala moc rychle nebo pomalu). Budeme-li mít dále volnost, budeme chtít, aby rychlost změny polynomu byla stejná jako u samotné funkce, atd. No a nakonec uvidíme, co nám z toho vypadne.

(1) pro $n = 0$ je situace jednoduchá, lepší tip než $P(x) = f(0)$ nemáme.

(2) pro $n = 1$ je situace horší, nicméně dobrou aproximaci nám dává polynom $P(x) = f'(0) \cdot x + f(0)$, kde $f'(0)$ je derivace funkce v bodě 0. Všimněme si, že platí $\lim_{x\to 0} \frac{|f(x)-P(x)|}{x} = 0$.

(3) pro $n > 1$, lze ukázat, že polynom s vlastností $\lim_{x\to \frac{1}{2}} \frac{|f(x)-P(x)|}{(x-\frac{1}{2})^n} = 0$ je

$$P_n = f(0) + \frac{f'(0)}{1}x + \frac{f''(0)}{2!}x^2 + \cdots + \frac{f^{(i)}(0)}{i!}x^i + \ldots \frac{f^{(n)}(0)}{n!}x^n.$$

K příkladu výše se hodí několik poznámek. Zaprvé, dostatečně hladká v tomto kontextu znamená, že derivace všech potřebných řádů existují a jsou konečné. Je dobré si uvědomit, že při derivování polynomu přirozeně dochází k tomu, že vyšší mocniny mají větší vliv na hodnotu než nižší, protože při jejich derivaci před ně vypadne vyšší koeficient. Přesně proto jsou u těchto derivací koeficienty $\frac{1}{n!}$, aby tento efekt potlačily.

Dále se naskýtá otázka, zda s rostoucím n je aproximace skutečně lepší. Vzhledem k tomu, že $\lim_{x\to a} \frac{(x-a)^{n+k}}{(x-a)^n} = 0$, je odpověď kladná. Zajímavou otázkou rovněž je, zda lze najít jiný polynom Q stupně nejvýše n, který nemá tvar výše, ale platí pro něj $\lim_{x\to a} \frac{f(x)-Q(x)}{(x-a)^n} = 0$. Ukazuje se, že ne. Platí-li pro polynom $\lim_{x\to a} \frac{f(x)-Q(x)}{(x-a)^n} = 0$, pak už $Q = P_n$. To znamená, že uvažujeme-li o „nejlepších“ aproximacích ve smyslu $\lim_{x\to a} \frac{f(x)-P(x)}{(x-a)^n} = 0$, tak ty jsou určené jednoznačně.

Na závěr bychom také rádi věděli, jak dobrou aproximaci jsme našli. Dá se ukázat, že pokud f má v každém bodě $[a,x]$ konečnou $(n+1)$-ní derivaci, pak $f(x) - P_n(x) = \frac{1}{(n+1)!} f^{(n+1)}(\xi)(x-a)^{n+1}$, kde $\xi \in (a,x)$.

Vzhledem k tomu, že víme, že přesnost aproximace roste se stupněm polynomu, pak dává smysl (pro dostatečně hladké funkce) místo polynomu definovat Taylorovu řadu $\sum_{i=0}^{\infty} \frac{f^{(i)}(b)}{n!}(x-b)^i$. Má to jen dva drobné nedostatky – zaprvé ne všechny funkce mají derivace všech řádů a za druhé existují funkce, které mají derivace všech řádů, ale nejsou rovny své Taylorově řadě. Například funkce f, která je 0 pro $x \leq 0$ a $f(x) = e^{\frac{-1}{x}}$ pro $x > 0$.

Exponenciála, logaritmus a výlet do historie

První z elementárních funkcí je exponenciální funkce. Motivace pro její použití byl rozvoj obchodu a financí. Předpokládejme, že někomu půjčíme 1 korunu s úrokem 100% na 1 rok. Budeme-li chtít, aby se částka zúročila jednou, pak jistě na konci roku dostaneme dvojnásobek původní částky. Nicméně, můžeme taky chtít částku úročit 2x pokaždé s polovičním úrokem, tj. chceme $(1+\frac{1}{2})^2 = \frac{9}{4} > 2$, 3x s třetinovým úrokem, tj. $(1+\frac{1}{3})^3 = \frac{64}{27} > \frac{9}{4}$. Nastává otázka, jak se úročení chová, pokud bychom chtěli úročit „spojitě“, tj. uvažovat $\lim_{n\to\infty}(1+\frac{1}{n})^n$. Ukazuje se, že tento výraz má limitu, kterou z nedostatku lepších nápadů, označujeme e a je to Eulerova konstanta ($\approx 2,72$). V principu se jedná o funkci jejíž růst je roven její hodnotě, což můžeme s pomocí derivace rovněž zapsat jako $x'(t) = x(t)$, $t \in \mathbb{R}$, $x(0) = 1$.

Můžeme si zkusit rozmyslet, že mocninná řada $\sum_{k=1}^{\infty} \frac{x^k}{k!}$ splňuje tuto diferenciální rovnici. Dá se ukázat, že řada je definovaná na celé reálné přímce a řešení předchozí diferenciální rovnice je jednoznačné, tedy tato řada je jejím jediným řešením. Nakonec ještě poznamenejme, že existuje ještě třetí možnost, jak exponenciálu jednoznačně definovat a to pomocí požadavku $e^{x+y} = e^x \cdot e^y$ a $e(0) = 1$.

Další důležitou funkcí je přirozený logaritmus. K jeho definici došlo v souvislosti s kvadraturou hyperboly. Předmětem studia bylo určit obsah útvaru, který je vytnutý hyperbolou $xy = 1$ a polopřímkami procházejícími počátkem a protínajícími hyperbolu v bodech $(a, \frac{1}{a})$, $(b, \frac{1}{b})$. Ukazuje se, že pokud $A(t)$ označíme obsah mezi body $a = 1$ a $b = t$, pak platí $A(tu) = A(t) + A(u)$. Jinak řečeno, funkce převádí násobení na sčítání. Pro naše potřeby je ovšem lepší definovat logaritmus jako inverzní funkci k exponenciále. Tedy je to funkce definovaná na kladných reálných číslech splňující $\log(e^x) = x$.

Příklad. Spočti Taylorovu řadu pro $\log(1+x)$.

Příklad. Aproximuj $\log 2$.

Literatura a zdroje

[1] S. Hencl, L. Pick, J. Spurný a M. Zelený: *Matematická analýza 1*,

[2] History of logarithms, *https://en.wikipedia.org/wiki/History_of_logarithms*,

[3] The force, *universe*,

[4] Pavel Turek: *Konvergentní posloupnosti v* $\mathbb{N}$, soustředění iKSka, Kunžak

Generující funkce

Jakub Löwit

Abstrakt. V přednášce se naučíme pracovat s takzvanými generující funkcemi, které tvoří pevný most mezi kombinatorikou a analýzou. Jejich znalost nám dá poměrně koncepční vhled do některých kombinatorických úloh. Získaná intuice se může hodit nečekaně často.

Motivační okénko

Základní myšlenku generujících funkcí můžeme dobře ilustrovat na následujících cvičeních.

Cvičení 1. Jaký koeficient má polynom $(1 + x^5 + x^7)^{20}$ u členu x^{17}?

Cvičení 2. Máme tři košíky s vejci. V prvním jsou dvě žlutá, v druhém dvě modrá a ve třetím tři červená vejce. Kolika způsoby lze vybrat 4 vejce?

V prvním příkladě si místo „roznásobení“ závorek zjevně situaci chceme pouze kombinatoricky představit, zatímco druhý příklad lze přímočaře převést na násobení trojice polynomů a eliminovat tím možnost chyby. V tuto chvíli by samozřejmě kdokoli mohl říct, že jen slovíčkaříme a počítáme triviality. Korespondenci mezi kombinatorickými a analytickými úlohami lze ale dotáhnout mnohem dál, a v tu chvíli začne být překvapivě užitečná. Tak vzhůru na to!

Hodí se vědět

Shrneme pár spíše jednoduchých věcí, které se bude hodit mít na paměti.

Tvrzení. *Pro libovolné* $x \in \mathbb{R}$, $n \in \mathbb{N}_0$ *platí* $1 + x + x^2 + \cdots + x^n = \frac{x^{n+1}-1}{x-1}$.

Tvrzení. *Pro libovolné* $x \in \mathbb{R}$, $n \in \mathbb{N}$ *platí* $\binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n = (x+1)^n$.

Jediný nekonečný součet, který budeme do začátku potřebovat znát, je součet nekonečné geometrické řady.[1]

Tvrzení. *Pro všechna* $x \in (-1, 1)$ *platí* $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$.

[1] Samozřejmě se hodit i další; my si ale užijeme dost zábavy i tak.

V případě $x = 0$ v předchozím tvrzení přitom používáme konvenci $0^0 = 1$. A když už jsme se dostali k těm nekonečným součtům, bylo by dobré vědět, co taková nekonečná řada $\sum_{n=0}^{\infty} a_n x^n$ vlastně je. Na takovou řadu se lze dívat dvěma způsoby. Předně se na $\sum_{n=0}^{\infty} a_n x^n$ můžeme dívat jenom jako na *formální řadu*, tj. posloupnost jejích koeficientů $a_0, a_1, a_2, \ldots$, za kterými jsou symboly x^n. Takovéto formální řady si můžeme sčítat i násobit jako by to byly polynomy. To odpovídá kombinatorické straně naší teorie.

Zároveň by se nám ale mohlo chtít za x dosazovat. Pokud by to šlo, odpovídala by řada $\sum_{n=0}^{\infty} a_n x^n$ nějaké funkci $f(x)$, která číslu x přiřadí onen nekonečný součet. O řadě bychom pak říkali, že *konverguje*. To ale bohužel nefunguje vždycky – pokud se koeficienty a_i chovají nepěkně, takový součet vůbec nemusí dávat smysl.

Tvrzení. *Konverguje-li řada $f(x) = \sum_{n=0}^{\infty} a_n x^n$ pro všechna $x \in (-\varepsilon, \varepsilon)$ pro nějaké dostatečně malé $\varepsilon > 0$, pak jsou její koeficienty jednoznačně určeny hodnotami funkce $f(x)$.*

Koeficienty a_n se pak dají zrekonstruovat pomocí derivování jako $a_n = \frac{f^{(n)}(0)}{n!}$.

Protože nás ale zajímá spíš kombinatorická strana mince, konvergencemi se moc zabývat nebudeme. K tomu, aby řada konvergovala na nějakém $(-\varepsilon, \varepsilon)$ například bohatě stačí, aby pro všechna $n \in \mathbb{N}$ platilo $a_n < K^n$ pro nějaké pevné číslo K. Jakmile tedy koeficienty a_n rostou dostatečně pomalu, jsou jednoznačně určeny funkcí $f(x)$. V takovém případě sčítání a násobení těchto funkcí odpovídá formálnímu sčítání a násobení původních řad.[2]

Definice.[3] Ať $a_0, a_1, a_2, \ldots$ je posloupnost reálných čísel. Její *generující* (často též *vytvořující*) funkcí rozumíme mocninnou řadu

$$\sum_{n=0}^{\infty} a_n x^n.$$

Pointa je následující. Máme-li nějakou posloupnost čísel, která nás zajímá, můžeme z ní vytvořit příslušnou generující funkci. Tu ale s trochou štěstí dokážeme vyjádřit v uzavřeném tvaru, třeba tak jako to umíme udělat pro nekonečné geometrické řady. Kombinatorické či algebraické vlastnosti původní posloupnosti jsou pak uschovány ve velmi kompaktním tvaru, ve kterém s nimi umíme jednoduše manipulovat – a pokud příslušné řady konvergují, umíme se kdykoli beztrestně vrátit zpět.

[2] Pokud Tě řady zajímají, určitě se o nich dočteš v každé knížce o matematické analýze.

[3] Lze uvažovat i jiné druhy generujících funkcí, které se hodí k jiným účelům – my si ale vystačíme s těmito.

Seznámení

Cvičení 3. Kolika způsoby lze číslo $n \in \mathbb{N}$ zapsat jako součet k přirozených čísel, jestliže záleží na jejich pořadí?

Cvičení 4. Jakou generující funkci má posloupnost $a_0, a_1, a_2, \ldots$, kde a_n odpovídá počtu způsobů, jak zaplatit n korun pomocí korunových, dvoukorunových a pětikorunových mincí? Umíte ji napsat v uzavřeném tvaru?

Cvičení 5. Mějme posloupnosti $a_0, a_1, a_2, \ldots$ a $b_0, b_1, b_2, \ldots$ a jejich generující funkce $a(x)$, $b(x)$. Dokážete pomocí nich vyjádřit generující funkci posloupnosti, jejíž i-tý člen je $s_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0$?

Cvičení 6. Posloupnost $a_0, a_1, a_2, \ldots$ má generující funkci $g(x)$. Jakou generující funkci pak bude mít posloupnost částečných součtů $a_0, a_0 + a_1, a_0 + a_1 + a_2, \ldots$?

Úložky

Začneme několika pěknými úlohami, které nevyužívají žádnou komplikovanou teorii – jenom trikovou práci s posloupnostmi a jejich generujícími funkcemi. Ačkoli se může hodit znát postupy z dalších částí přednášky, právě nyní bychom mohli pochopit, o co vlastně jde, a naučit se generující funkce intuitivně používat.

Úloha 7. Pro $n \in \mathbb{N}$ spočtěte $\sum_{i=0}^{n} (-1)^i \binom{n}{i}^2$.

Úloha 8. Máme pytel jablek, hrušek, pomerančů a banánů. Chceme vyrobit salát z n kusů ovoce, aby

(1) počet jablek byl sudý,
(2) počet hrušek byl dělitelný pěti,
(3) byly v něm nejvýše 4 pomeranče,
(4) byl v něm nejvýše jeden banán.

Kolika způsoby to lze udělat?

Úloha 9. *Hrací kostka* je krychle, jejíž stěny jsou popsané nějakými přirozenými čísly. Navrhněte dvojici kostek, jejichž hození je ekvivalentní hodu dvojicí běžných kostek, tj. aby se všechny možné součty se objevovaly stejně často. A dokážete určit, kolik takových dvojic kostek existuje?

Úloha 10. Pro $x \in \mathbb{R}$, $|x| < 1$ dokažte

$$\frac{1}{1-x} = (1+x)(1+x^2)(1+x^4)(1+x^8)\cdots,$$

kde napravo vystupuje nekonečný součin.

Úloha 11. Přirozená čísla jsme disjunktně prokryli n aritmetickými posloupnostmi s diferencemi $r_1, r_2, \ldots, r_n$. Dokažte, že $\frac{1}{r_1} + \frac{1}{r_2} + \cdots + \frac{1}{r_n} = 1$.

Úloha 12. *Rozkladem* čísla $m \in \mathbb{N}$ rozumíme rozložení čísla m na součet přirozených čísel, jejichž pořadí nás nezajímá. Dokažte, že počet rozkladů čísla m na různá čísla je stejný jako počet rozkladů m na lichá čísla.

Úloha 13. Po celých číslech skáče kobylka. Začíná v čísle 1 a pokaždé se náhodně rozhodne zda skočí na číslo o jedna menší či na číslo o dvě větší. S jakou pravděpodobností se někdy dostane do 0?

Úloha 14. Pro sudé $n \in \mathbb{N}$ dokažte rovnost

$$\sum_{k=0}^{\frac{n}{2}} (-1)^k \binom{n+2}{k} \binom{2(n-k)+1}{n+1} = \frac{(n+1)(n+2)}{2}.$$

(VJIMC 2014)

Úloha 15. Je dáno rostoucí posloupnost $a_0, a_1, a_2, \ldots$ v $\mathbb{N}_0$ taková, že každé $m \in \mathbb{N}_0$ lze vyjádřit právě jedním způsobem jako $a_i + 2a_j + 4a_k$. Určete a_{1998}.
(IMO Shortlist 1998)

Úloha 16. Najděte všechny disjunktní rozklady $\mathbb{N}_0 = A \cup B$ takové, že pro každé $n \in \mathbb{N}_0$ má rovnice $x + y = n$, $x < y$ stejně řešení v $A \times A$ jako v $B \times B$.

Úloha 17. Existuje podmnožina přirozených čísel X taková, že všechna dostatečně velká přirozená čísla lze vyjádřit jako součet dvou prvků z X stejným počtem způsobů?

Úloha 18. Vrcholy pravidelného n-úhelníku jsou obarveny několika barvami. Vrcholy každé barvy navíc opět tvoří pravidelný mnohoúhelník. Dokažte, že dva z nich mají stejný počet vrcholů.

Úloha 19. Dokažte, že $\sum \binom{k}{n-k} = F_{n+1}$, kde na levé straně sčítáme přes všechna smysluplná k a F_i značí i-té Fibonacciho číslo.

Derivace

Jedním ze šikovných způsobů, jak si ulehčit práci, je derivování a integrování. Jeli totiž řada $\sum_{n=0}^{\infty} a_n x^n$ konvergentní na nějakém neprázdném intervalu, jejím zderivováním dostaneme řadu $\sum_{n=0}^{\infty} (n+1) a_{n+1} x^n$. Zintegrováním původní řady naopak získáme řadu $c + \sum_{n=0}^{\infty} \frac{1}{n} a_{n-1} x^n$ pro nějaké reálné c.

Úloha 20. Pro $n \in \mathbb{N}$ spočtěte hodnotu $\sum_{k=0}^{n} k \binom{n}{k}$.

Úloha 21. Přirozená čísla jsme disjunktně prokryli n aritmetickými posloupnostmi s diferencemi po řadě $r_1, r_2, \ldots, r_n$ a počátečními členy po řadě $a_1, a_2, \ldots, a_n$. Dokažte, že $\frac{a_1}{r_1} + \frac{a_n}{r_2} + \cdots + \frac{a_n}{r_n} = \frac{n-1}{2}$.

Umět řady derivovat a integrovat se společně s dalšími postupy hodí docela často. Předchozí dvě úlohy tvořily jen lehkou ochutnávku – v dalších částech přednášky nabyté znalosti znovu využijeme.

Rekurence

Pomocí generujících funkcí lze přímočaře řešit různé rekurence. Pro různé speciální druhy rekurencí existují přehlednější způsoby řešení, generující funkce lze ale použít dost obecně.

Úloha 22. Definujme $a_0 = 0$, $a_{i+1} = 2a_i + 1$ pro $i \geq 1$. Vyjádřete explicitně a_n.

S použitím stejného přístupu a trochy hrubé síly lze vyjádřit i členy jiných rekurentně zadaných posloupností. Často je přitom ale potřeba rozkládat všelijaké racionální funkce na parciální zlomky. Předveďme si to na několika příkladech. Ačkoliv je třeba trochu počítat, není se čeho bát.

Úloha 23. (Fibonacciho čísla) Ať $F_0 = 1$, $F_1 = 1$ a $F_n = F_{n-1} + F_{n-2}$ pro $n \geq 2$. Vyjádřete explicitně F_n.

Vytvořující funkce ale začnou být skutečně potřeba, jakmile rekurence přestanou být lineární. Samozřejmě pokud řešení umíme tipnout, typicky je triviální řešení dokončit indukcí. Takový tip ale vůbec nemusí být lehký – a generující funkce ho umí udělat samy.

Úloha 24. Spočtěte explicitně členy posloupnosti splňující $x_{n+2} - 6x_{n+1} - 9x_n = = 2^n + n$ pro $n \in \mathbb{N}_0$, přičemž $x_1 = x_0 = 0$.

Ponaučením z této části by tedy mělo být, že počítání členů mnoha rekurentních posloupností jde jednoduše převést do jazyka generujících funkcí, které pak řešíme jako „běžné rovnice“. Pokud nám přitom přeje štěstí a máme zkušenosti, z vyjádření generujících funkcí zvládneme zpětně vyčíst hledanou posloupnost. Až budeme mít více znalostí, vyřešíme si i pár zajímavějších rekurencí.

Zobecněná binomická věta

Definice 25. Pro libovolné $r \in \mathbb{R}$, $k \in \mathbb{N}$ označme $\binom{r}{k} = \frac{r(r-1)\cdots(r-k+1)}{k!}$. Nazýváme ho *zobecněné kombinační číslo*.

Tvrzení 26. *Pro $x \in (-1, 1)$ platí* $(1+x)^r = \binom{r}{0} + \binom{r}{1}x + \binom{r}{2}x^2 + \cdots$

Pro $r \in \mathbb{N}$ je tedy předchozí tvrzení běžná binomická věta. Pro $r \in \mathbb{Z}$ nebo obecněji $r \in \mathbb{Q}$ ale dostáváme nové rovnosti, ve kterých najednou napravo vystupují nekonečné řady. Kromě součtu nekonečné geometrické řady tedy explicitně známe další druh součtu, díky čemu se umíme mnohem lépe vypořádat s některými dalšími generujícími funkcemi.

Jakmile tedy při výpočtech dospějeme ke generujícím funkcím, kde se výrazy $(1+x)^r$ vyskytují ve jmenovatelích či dokonce v odmocninách, už z nich budeme umět explicitně vyjádřit členy příslušné posloupnosti. V mnoha případech se samozřejmě dá zobecněné binomické větě vyhnout, často ale podstatným způsobem pomůže.

Úloha 27. V košíku je 30 modrých, 40 červených a 50 bílých míčků. Kolika způsoby lze vybrat 70 míčků?

Úloha 28. Vyjádřete explicitně součet $1^2 + 2^2 + \cdots + n^2$.

Pokud se nudíte, postup předchozí úlohy lze bez problému použít na zjištění součtů tvaru $1^3 + 2^3 + \cdots + n^3$, nebo i jakékoli vyšší mocniny, kterou si předem vyberete.

Úloha 29. S jakou pravděpodobností padne při hodu 12-ti hracími kostkami přesně 30?

Úloha 30. Kolik existuje slov z písmen a, b, c, d délky n, ve kterých se nikde vedle sebe nevyskytují písmena a, b?

Úloha 31. (Catalanova čísla) Máme čtverec $n \times n$ rozdělený na jednotkové čtverce. Ať c_n značí počet cest z levého dolního do pravého horního rohu původního čtverce, které vedou po hranách menších čtverečků směrem doprava či nahoru a zůstávají celou dobu pod diagonálou (můžou se jí dotknout). Spočtěte c_n.

Návody

1. Tento koeficient se dá kombinatoricky vyjádřit jako $\binom{20}{1} \cdot \binom{19}{2} = \frac{20 \cdot 19 \cdot 9}{2} = 3420$.

2. Násobte $(1 + x + x^2)(1 + x + x^2)(1 + x + x^2 + x^3)$, koeficient u x^4 je 8.

3. $\binom{n+k-1}{k-1}$

4. $\frac{1}{(1-x)(1-x^2)(1-x^5)}$

5. $a(x) \cdot b(x)$

6. $\frac{1}{(1-x)} \cdot g(x)$

7. Člen u x^n v $(x+1)^n(x-1)^n$.

8. Jsou to koeficienty řady $\frac{1}{(1-x)^2}$, salát z n kusů ovoce lze proto připravit $n+1$ způsoby.

9. Rozložte polynom $f = x + x^2 + x^3 + x^4 + x^5 + x^6$, jak jen to jde. Součty po hodu dvěma kostkami pak odpovídají polynomu f^2.

10. Jednoznačné vyjádření čísel ve dvojkové soustavě.

11. Rozepište do rovnosti geometrických řad, vynásobte $(x-1)$ a dosaďte 1.

12. Nahlédněte, že počet rozkladů má generující funkci danou nekonečným součinem geometrických řad $\prod_{n=0}^{\infty} \frac{1}{1-x^n}$. Pomocí stejných metod převeďte úlohu na ověření nějaké rovnosti nekonečných součinů.

13. Označme a_i počet posloupností skoků začínajících v 0, které se dostanou do 0 poprvé po i skocích. Dále ať b_i značí stejný počet pro posloupnosti začínající v čísle 3. Všimněte si vztahu mezi generujícími funkcemi.

14. Nejprve si všimněte rovnosti $\frac{1}{(1-x)^m} = \sum_{j=0}^{\infty} \binom{m+j-1}{m-1} x^j$. Interpretujte levou stranu zadání jako nějaký koeficient součinu dvou vhodných řad.

15. Uvažte funkci $\sum_{i=1}^{\infty} x^{a_i}$. Zkuste si hrát s dosazením $x = y^{2^k}$ a nekonečnými součiny.

20. Derivujte binomickou větu, dosaďte 1. Vyjde $n2^{n-1}$.

21. Zderivujte, dosaďte 1 a použijte identitu pro součet převrácených hodnot diferencí.

22. Vyjde $2^n - 1$.

23. Po delším výpočtu vyjde $(1 + x + x^2)(x + x^2 + x^3)(1 + x)(1 + x)$.

28. Vezměte geometrickou řadu. Derivujte, derivujte!

31. Nahlédněte rekurentní vztah $c_n = c_0c_{n-1} + \cdots + c_{n-1}c_0$, se kterým pak pracujte v řeči generujících funkcí.

Literatura a zdroje

[1] Titu Andreescu, Gabriel Dospinescu: *Problems from the Book*

[2] Pavel Šalom: *Vytvořující funkce*

[2] Robert Šámal: *Generující funkce*

[3] AoPS *Art of Problem Solving*

Teleskopické součty a součiny

Anna Mlezivová

Abstrakt. Příspěvek se zabývá metodou teleskopických součtů a součinů a obsahuje několik příkladů na její procvičení.

Princip metody teleskopických součtů a součinů je založen na cíleném rozšíření daného součtu nebo součinu několika čísel takovým způsobem, aby jej následně bylo možné výrazně zjednodušit.

Úmluva. V celém příspěvku budeme počítat s $n > 1$.

Při metodě teleskopických součtů se obvykle snažíme každý ze sčítanců přepsat ve tvaru rozdílu tak, že většina členů takto upraveného součtu se nakonec navzájem odečte.

Úloha. Určete hodnotu výrazu $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\cdots+\dfrac{1}{n\cdot(n+1)}$.

Úloha. Určete hodnotu výrazu $1!\cdot 1+2!\cdot 2+\cdots+n!\cdot n$.

Při teleskopických součinech chceme jednotlivé členy upravit tak, aby se jich co nejvíc zkrátilo a zůstal nám pouze jednoduchý výraz.

Úloha. Dokažte, že $\left(1+\dfrac{1}{1\cdot 3}\right)\cdot\left(1+\dfrac{1}{2\cdot 4}\right)\cdots\left(1+\dfrac{1}{(n-1)\cdot(n+1)}\right)<2$.

Úloha. Dokažte, že $\left(1-\dfrac{1}{4}\right)\cdot\left(1-\dfrac{1}{9}\right)\cdots\left(1-\dfrac{1}{n^2}\right)=\dfrac{n+1}{2n}$.

Příklady

Příklad 1. Určete hodnotu výrazu $\dfrac{1}{1\cdot 2\cdot 3}+\dfrac{1}{2\cdot 3\cdot 4}+\cdots+\dfrac{1}{n\cdot(n+1)\cdot(n+2)}$.

Příklad 2. Dokažte, že platí $\dfrac{1}{2^2}+\dfrac{1}{3^2}+\cdots+\dfrac{1}{n^2}<1$.

Příklad 3. Dokažte, že platí $\dfrac{1}{\sqrt{1}+\sqrt{2}}+\cdots+\dfrac{1}{\sqrt{99}+\sqrt{100}}=9$.

Příklad 4. Dokažte, že $1+\dfrac{1}{1+2}+\dfrac{1}{1+2+3}+\cdots+\dfrac{1}{1+2+\cdots+n}<2$.

Příklad 5. Dokažte, že platí $\dfrac{1}{1\cdot 5}+\dfrac{1}{3\cdot 7}+\cdots+\dfrac{1}{(2n-1)\cdot(2n+3)}<\dfrac{1}{3}$.

Příklad 6. Dokažte, že

$$\left(1+\frac{1}{2}-\frac{1}{4}-\frac{1}{8}\right)\left(1+\frac{1}{3}-\frac{1}{9}-\frac{1}{27}\right)\cdots\left(1+\frac{1}{n}-\frac{1}{n^2}-\frac{1}{n^3}\right)=\frac{(n+1)^2}{4n}.$$

Příklad 7. Dokažte, že $\dfrac{3}{1!+2!+3!}+\dfrac{4}{2!+3!+4!}+\cdots+\dfrac{2019}{2017!+2018!+2019!}<\dfrac{1}{2}$.

Příklad 8. Určete hodnotu $\sqrt{1+1+\dfrac{1}{4}}+\sqrt{1+\dfrac{1}{4}+\dfrac{1}{9}}+\cdots+\sqrt{1+\dfrac{1}{n^2}+\dfrac{1}{(n+1)^2}}$.

Příklad 9. Zjednodušte

$$\frac{1}{(1+1)\cdot\sqrt{1}+1\cdot\sqrt{1+1}}+\frac{1}{(2+1)\cdot\sqrt{2}+2\cdot\sqrt{2+1}}+\cdots+\frac{1}{(n+1)\cdot\sqrt{n}+n\cdot\sqrt{n+1}}.$$

Příklad 10. Dokažte, že $\dfrac{2^3+1}{2^3-1}\cdot\dfrac{3^3+1}{3^3-1}\cdots\dfrac{n^3+1}{n^3-1}<\dfrac{3}{2}$.

Příklad 11. Určete hodnotu $\displaystyle\sum_{n=2}^{\infty}\frac{F_n}{F_{n-1}\cdot F_{n+1}}$.

Příklad 12. Určete hodnotu $\displaystyle\sum_{n=2}^{\infty}\frac{1}{F_{n-1}\cdot F_{n+1}}$.

Literatura a zdroje

Tento příspěvek je z velké části převzatý z přednášky Adély Kostelecké, které bych tímto chtěla poděkovat.

[1] Adéla Kostelecká: *Teleskopické součty a součiny*, Lipová-lázně, 2016.

[2] Andreescu, Gelca: *Mathematical Olympiad Challenges*, 2000.

[3] Jaroslav Švrček: *O teleskopických součtech a součinech*, *https://is.muni.cz/el/1431/jaro2010/MA572/um/didmat2.pdf*

[4] Brilliant: *Telescoping Series – Sum*, *https://brilliant.org/wiki/telescoping-series/*

Konečné automaty

Viki Němeček

Abstrakt. Jedním z hlavních objektů, které zkoumá teoretická informatika, jsou Turingovy stroje. Protože o Turingových strojích je ale za jednu přednášku obtížné dokázat cokoli zajímavého, podíváme se na jejich (o několik stupňů) slabší brášky – konečné automaty.

V teoretické informatice často řešíme, jak složité je pro různé množiny řetězců rozhodnout, který řetězec do nich patří a který ne. Abychom ale mohli mluvit o řetězcích, musíme nejprve nadefinovat terminologii.

Definice. Konečné množině znaků budeme říkat *abeceda* a budeme ji značit Σ. Abeceda může být například $\{a, b, c, \ldots, z\}$, ale taky třeba množina obsahující #, @, § a !. My však budeme nejčastěji používat binární abecedu $\{0, 1\}$, či dokonce unární abecedu obsahující pouze nulu nebo pouze jedničku. Prvkům abecedy budeme říkat *znaky abecedy*, nebo prostě *znaky*. *Řetězec* pak bude konečná (klidně prázdná) posloupnost znaků. *Délkou řetězce* w budeme rozumět počet jeho znaků a budeme ji značit $|w|$. Řetězec délky 0 budeme značit ε. Máme-li řetězce u a v, budeme uv nebo $u \cdot v$ značit jejich zřetězení, tedy řetězec w takový, že $|w| = |u| + |v|$ a ve w jsou nejprve všechny znaky u v tom samém pořadí jako v u a potom obdobně všechny znaky v. Podobně budeme u^k pro $k \in \mathbb{N}_0$ značit řetězec u k-krát zřetězený sám za sebe (tedy například zápisem $1(10)^3$ budeme rozumět řetězec 1101010). Pro řetězec u budeme u^R značit ten samý řetězec pozpátku. Máme-li řetězec w, tak pro $k \in \mathbb{N}, k \leq |w|$ budeme $w[k]$ značit k-tý znak řetězce w.

Dále budeme potřebovat terminologii a značení mluvící o množinách řetězců. Dovolíme si jistou formální nepřesnost a budeme tam, kde to dává smysl, volně zaměňovat řetězec s jednoprvkovou množinou, která obsahuje právě tento řetězec.[1]

Dovolíme si podobně, jako zřetězujeme řetězce, zřetězovat i množiny. Tedy například $\{0, 1\} \cdot \{2, 3\} = \{02, 03, 12, 13\}$. Dále pokud M je množina řetězců, M^* budeme značit libovolný počet opakování něčeho z M, tedy

$$M^* = \{\varepsilon\} \cup M \cup M^2 \cup M^3 \cup \ldots$$

Například Σ^* je tedy množina všech možných konečných řetězců nad abecedou Σ. $\{01, 02\}^*$ obsahuje například ε, 01, 01020102, ale ne 010.

[1] Také budeme zaměňovat znak a řetězec délky jedna obsahující právě tento znak.

Definice. *Jazykem* nad abecedou Σ budeme značit množinu $L \subseteq \Sigma^*$. Jejím prvkům budeme říkat *slova* jazyka L.

Příkladem jazyka nad abecedou $\{0, 1\}$ může být například množina všech řetězců, které reprezentují ve dvojkové soustavě číslo menší než 42. Nebo množina všech řetězců, které reprezentují prvočíslo. Nyní však již konečně máme vše, co potřebujeme, abychom nadefinovali konečný automat.

Definice. *Konečný automat* je pětice $(S, \Sigma, \sigma, s, A)$, kde:

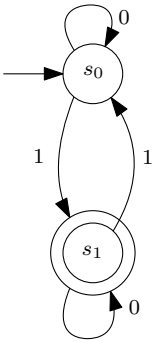
- S je konečná množina stavů,
- Σ je konečná abeceda,
- $\sigma : S \times \Sigma \to S$ je přechodová funkce,
- $s \in S$ je počáteční stav,
- $A \subseteq S$ je množina přijímajících stavů.

Výpočet konečného automatu nad řetězcem w probíhá následovně: Automat začne v počátečním stavu s. Poté přečte první znak řetězce $w[1]$ a přejde do stavu $s_1 = \sigma(s, w[1])$ (ne nutně různého od s). Dále přečte znak $w[2]$ a přejde do stavu $s_2 = \sigma(s_1, w[2])$. Tak pokračuje, dokud nepřečte poslední znak w a nepřejde do stavu $s_{|w|}$. Pak řekneme, že automat řetězec w přijal, pokud výpočet ukončil v přijímajícím stavu, tedy pokud $s_{|w|} \in A$.

Jazyk $L(A)$ *přijímaný automatem* A je množina všech slov z Σ^*, které automat přijme.

Průběh výpočtu si tedy můžeme představit tak, že automat čte řetězec znak po znaku a do svého stavu si ukládá nějakou informaci o tom, co už přečetl. Ve většině případů si však například nemůže uložit celou část řetězce, kterou už přečetl, protože jeho stav může nabývat jen konečně mnoha různých hodnot, kdežto řetězce můžou být obecně libovolně dlouhé.

Protože takovýto zápis automatu je (obzvlášť u větších automatů) velmi nepřehledný, často se používá ilustrace automatu pomocí orientovaného grafu, kde vrcholy odpovídají stavům automatu a orientované hrany označené znaky abecedy přechodové funkci. Mějme například automat nad abecedou $\{0, 1\}$, který má množinu stavů $\{s_0, s_1\}$,kde s_0 je počáteční stav a s_1 jediný přijímající stav. Přechodová funkce říká, že při přečtení nuly zůstaneme v témže stavu a při přečtení jedničky přejde do druhého z možných stavů. Tento automat by též šel popsat následujícím obrázkem:



Příklad 1. Jaký jazyk automat na obrázku vlastně přijímá?

Příklad 2. Nakreslete konečný automat nad abecedou $\{0, 1\}$, který přijímá právě ta slova, která reprezentují binární zápis sudého čísla. Co čísla dělitelná trojkou?

Příklad 3. Nakreslete konečný automat nad abecedou $\{0, 1\}$, který přijímá právě slova se sudým počtem nul. Pak nakreslete automat, který přijímá ta, v nichž je počet jedniček dělitelný třemi. Nakonec najděte automaty, které přijímají slova splňující alespoň jednu z těchto vlastností, respektive obě tyto vlastnosti.

Definice. O jazyku řekneme, že je *regulární*, pokud existuje konečný automat, který přijímá právě tento jazyk.

Příklad 4. Dokažte, že pro libovolné dva regulární jazyky L_1, L_2 nad abecedou Σ jsou jazyky $L_1 \cup L_2$, $L_1 \cap L_2$ a $\Sigma^* \setminus L_1$ také regulární.

Příklad 5. Rozmyslete si, že libovolný konečný jazyk je regulární.

Pumping lemma

Doteď jsme pouze konstruovali automaty, ale chyběly nám prostředky, jak dokázat, že nějaký jazyk regulární není. K tomu nám poslouží pumping lemma.

Věta. (Pumping lemma) *Pro každý regulární jazyk L existují konstanty k a ℓ, takové, že pro každé slovo $u \in L$, kde $|u| \geq \ell$, existují řetězce w, x a y, takové, že:*

- $u = w \cdot x \cdot y$,
- $|w \cdot x| \leq k$,
- $|x| \geq 1$,
- *pro každé $n \in \mathbb{N}_0$ je slovo $w \cdot x^n \cdot y$ také v jazyce L.*

Myšlenka důkazu. Máme-li regulární jazyk, pak existuje konečný automat, který ho přijímá. Tento automat má $|S|$ stavů a je nad $|\Sigma|$-prvkovou abecedou, takže pokud má slovo alespoň $|S| \cdot |\Sigma| + 1$ znaků, musí se z Dirichletova principu nějaká kombinace

čteného znaku a stavu stroje zopakovat (dokonce již mezi prvními $|S|\cdot|\Sigma|+1$ znaky). Část slova mezi těmito opakováními je ale možné vynechat či naopak libovolněkrát zopakovat, protože pokud stroj čte týž znak a je v témže stavu, bude se vždy chovat stejně bez ohledu na to, co již přečetl.

Úloha. Rozhodněte, zda jazyk $L = \{0^j \mid j \text{ je mocnina dvojky}\}$ je regulární.

Řešení. Jazyk regulární není. Pro spor připusťme, že by regulární byl. Pak existují k a ℓ s vlastnostmi ze znění pumping lemmatu. Najdeme n takové, že $2^{n-1} > \max(k, \ell)$. Pak slovo 0^{2^n} lze rozdělit na slova w, x a y podle pumping lemmatu. Protože ale $k < 2^{n-1}$, tak $1 \leq |x| < 2^{n-1}$, tedy $w \cdot y = w \cdot x^0 \cdot y$ je v L, ale současně $2^{n-1} < |w \cdot y| < 2^n$, což je ve sporu s definicí L. Jazyk L tedy není regulární.

Příklad 6. O následujících jazycích rozhodněte, zda jsou regulární: (Prostředky, které k tomu máte, jsou jednak pumping lemma a jednak uzavřenost regulárních jazyků na doplněk, průnik a sjednocení.)

(1) $L_1 = \{0^p \mid p \text{ je prvočíslo}\}$,
(2) $L_2 = \{0^n \cdot 1^m \mid n, m \in \mathbb{N}\}$,
(3) $L_3 = \{0^n \cdot 1^n \mid n \in \mathbb{N}\}$,
(4) $L_4 = \{0^n \cdot 1^m \mid n, m \in \mathbb{N}, n > m\}$,
(5) $L_5 = \{0^n \cdot 1^m \mid n, m \in \mathbb{N}, n \neq m\}$,
(6) $L_6 = \{w \cdot w^R \mid w \in \{0,1\}^*\}$.

Nedeterminismus

Doteď jsme měli pouze konečné automaty, které vždy věděly, co mají dělat. Co kdybychom jim ale dali na výběr?

Definice. *Nedeterministický konečný automat* je pětice $(S, \Sigma, \sigma, s, A)$, kde:

- S je konečná množina stavů,
- Σ je konečná abeceda,
- $\sigma : S \times (\Sigma \cup \{\lambda\}) \to \mathcal{P}(S)$ je přechodová funkce,
- $s \subseteq S$ je množina startovních stavů,
- $A \subseteq S$ je množina přijímajících stavů.

Výpočet konečného automatu nad řetězcem w probíhá následovně: Automat začne v nějakém počátečním stavu ze s. Poté přečte první znak řetězce $w[1]$ a přejde do nějakého stavu $s_1 \in \sigma(s, w[1])$ (ne nutně různého od s). Případně může také nečíst znak, ale přejít do nějakého stavu z množiny $\sigma(s, \lambda)$ (a v příštím kroku opět číst první znak; tomu říkáme, že automat využil λ přechod). Takto pokračuje ve výpočtu, dokud nepřečte poslední znak a případně ještě nevyužije nějaké λ přechody. Pak řekneme, že automat řetězec w přijímá, pokud existuje výběr počátečního stavu a stavů v průběhu výpočtu takový, že automat skončí v nějakém stavu z A.

Pokud během výpočtu nastane situace, že je automat ve stavu s, čte znak z a $\sigma(s, z) = \emptyset$, výpočet se považuje za nepřijímající.

Věta. *Pro každý nedeterministický konečný automat existuje deterministický konečný automat, který přijímá ten samý jazyk.*

Myšlenka důkazu. Nejprve si rozmyslíme, že λ přechody umíme odstranit poměrně jednoduše. Potom sestrojíme konečný automat, jehož stavy jsou všechny podmnožiny množiny stavů původního nedeterministického automatu. Rozmyslete si, jak nadefinovat přechodovou funkci.

Příklad 7. Nechť K_1 a K_2 jsou regulární jazyky. Pak rozhodněte, zda jsou následující jazyky regulární (pro každou volbu K_1 a K_2):

(1) $L_1 = \{w \mid w^r \in K_1\}$,
(2) $L_2 = \{w^* \mid w \in K_1\}$,
(3) $L_3 = K_1^*$ – tento příklad se od předchozího liší tím, že v předchozím případě se požaduje, aby w bylo pořád stejné, zde se za sebe můžou řetězit různá slova K_1,
(4) $L_4 = \{w \cdot v \mid w \in K_1, v \in K_2\}$,
(5) $L_5 = \{w \cdot v \mid v \cdot w \in K_1\}$.

Návody

4. Jazyky L_1 a L_2 jsou regulární, tedy máte konečné automaty, které je přijímají. Zkuste z nich tedy vyrobit automat, který by přijímal jazyky $L_1 \cup L_2$ a $L_1 \cap L_2$. Bude se vám hodit rozmyslet si, jak vypadá „kartézský součin“ dvou automatů.

6. Jazyk L_2 je jediný regulární. V části (5) si uvědomte, že doplněk L_5 je jazyk všech řetězců, které vypadají jinak, než nějaké nuly a pak jiný počet jedniček. Kdyby ale L_5 byl regulární, je regulární i jeho doplněk a následně průnik jeho doplňku s L_2, což je přesně L_3. V části (6) si můžeme vzít například $w = 0^n \cdot 1$ pro nějaké dostatečně vysoké n.

7. Jazyk L_2 není regulární, myšlenka důkazu je podobná L_6 ze cvičení 6. Ostatní regulární jsou, popište konstrukci nedeterministického automatu.

Jensenova nerovnost

Tomáš Novotný

Abstrakt. Jensenova nerovnost je jedním z velmi silných nástrojů pro řešení nerovností. Její účinné použití je však často založeno na volbě správné konvexní či konkávní funkce. V příspěvku se podíváme na techniky, které lze pro hledání těchto funkcí využít, a procvičíme si je na důkazech jiných standardních nerovností a několika skutečných příkladech.

Konvexní kombinace

Definice. Nechť $x_1, \ldots, x_n \in \mathbb{R}$, $\lambda_1, \ldots, \lambda_n \in \langle 0, 1\rangle$ a navíc $\lambda_1 + \cdots + \lambda_n = 1$. Pak číslo $\lambda_1 x_1 + \cdots + \lambda_n x_n$ nazýváme *konvexní kombinací* čísel $x_1, \ldots, x_n$.

Cvičení. Rozmyslete si, že pokud je x_1 nejmenší a x_n největší z čísel $x_1, \ldots, x_n$, leží každá konvexní kombinace těchto čísel v intervalu $\langle x_1, x_n\rangle$.

Pro práci s Jensenovou nerovností je klíčové porozumět konvexním kombinacím (bodů) v rovině.

Definice. Nechť $[x_1, y_1], \ldots, [x_n, y_n]$ jsou souřadnice n bodů v rovině, $\lambda_1, \ldots, \lambda_n \in \langle 0, 1\rangle$ a $\lambda_1 + \cdots + \lambda_n = 1$. Pak bod o souřadnicích

$$[\lambda_1 x_1 + \cdots + \lambda_n x_n, \lambda_1 y_1 + \cdots + \lambda_n y_n]$$

nazýváme *konvexní kombinací* bodů $[x_1, y_1], \ldots, [x_n, y_n]$.

Cvičení. Co je množinou všech konvexních kombinací daných dvou (tří, čtyř, atd.) bodů v rovině? A co v prostoru?

Konvexní a konkávní funkce

Definice. Nechť $I \subseteq \mathbb{R}$ je interval a $f\colon I \to \mathbb{R}$ je funkce. Pokud pro každou dvojici $x, y \in I$ a každé $\lambda \in \langle 0, 1\rangle$ platí

$$f(\lambda x + (1 - \lambda)y) \leq \lambda f(x) + (1 - \lambda) f(y),$$

řekneme, že f je *konvexní* na I.

Duálně (s opačnou nerovností) definujeme *konkávní* funkci. Pokud pro $\lambda \in (0,1)$ platí ostrá varianta uvedené nerovnosti, mluvíme o *ryze konvexní* (resp. *ryze konkávní*) funkci.

Cvičení. Rozmyslete si, co nerovnost definující konvexitu (resp. konkavitu) znamená geometricky.

Cvičení. Zjistěte, které z elementárních funkcí jsou na některých intervalech konvexní (resp. konkávní). Jaký je vztah mezi konvexností a konkávností funkce f a $-f$?

Nyní můžeme konečně přejít k samotné nerovnosti.

Jensenova nerovnost

Věta. (Jensenova nerovnost) *Nechť f je konvexní funkce na intervalu I. Potom pro libovolná $x_1, \ldots, x_n \in I$ a $\lambda_1, \ldots, \lambda_n \in \langle 0, 1\rangle$ taková, že $\lambda_1 + \cdots + \lambda_n = 1$, platí*

$$\lambda_1 f(x_1) + \cdots + \lambda_n f(x_n) \geq f(\lambda_1 x_1 + \cdots + \lambda_n x_n).$$

Často nám bude stačit speciální případ, ve kterém jsou si všechny λ_i rovny:

$$\frac{f(x_1) + \cdots + f(x_n)}{n} \geq f\left(\frac{x_1 + \cdots + x_n}{n}\right).$$

Cvičení. Interpretujte obě strany nerovnosti geometricky pomocí konvexních kombinací bodů a uvědomte si, že tvrzení se tím stává téměř triviálním.

Cvičení. Rozmyslete si, kdy v Jensenově nerovnosti nastává rovnost.

Nyní si můžeme blahopřát, neboť jsme téměř zadarmo získali velmi obecně vyhlížející nerovnost, která se ukáže být silnou zbraní. Ke správnému použití Jensenovy nerovnosti je třeba umět rozhodnout, zda je daná funkce konvexní (resp. konkávní). K tomu se v praxi používá následující lemma.

Lemma. *Má-li funkce f na intervalu I nezápornou (resp. nekladnou) druhou derivaci, je f na I konvexní (resp. konkávní).*

Pokud jste o derivaci (natož nějaké druhé derivaci) neslyšeli, nezoufejte. U jednoduchých funkcí se dá konvexita/konkávnost dobře odhadnout z grafu, případně lze použít vhodný matematický software. Přísně korektní zdůvodnění se v tomto případě nevyžaduje ani v MO. O jednoduchých funkcích se považuje za známé, zda jsou konvexní či konkávní. Konvexní jsou například $\frac{1}{x}$, $\frac{1}{\sqrt{x}}$ na $\mathbb{R}^+$ nebo sudé mocniny x na $\mathbb{R}$. Typické konkávní funkce jsou $\sqrt{x}$ nebo $\log(x)$ na $\mathbb{R}^+$.

Motivační příklady

Konečně se dostáváme k úlohám. Začneme zlehka:

Příklad. Ukažte, že pro každé reálné $x > 1$ platí:

$$\frac{1}{x-1} + \frac{1}{x} + \frac{1}{x+1} \geq \frac{3}{x}.$$

Řešení. Použijeme Jensenovu nerovnost pro funkci $f(x) = 1/x$, která je konvexní na $\mathbb{R}^+$, a konvexní kombinaci kladných čísel $x-1$, x, $x+1$ s koeficienty

$$\lambda_1 = \lambda_2 = \lambda_3 = \frac{1}{3}.$$

Dostáváme

$$\frac{1}{3}\left(\frac{1}{x-1} + \frac{1}{x} + \frac{1}{x+1}\right) \geq \frac{1}{\frac{x-1}{3} + \frac{x}{3} + \frac{x+1}{3}} = \frac{1}{x} \;\Rightarrow\; \frac{1}{x-1} + \frac{1}{x} + \frac{1}{x+1} \geq \frac{3}{x}.$$

Jistě by vám nedělalo problém tuto nerovnost dokázat zcela přímočaře roznásobením. Zkusíme tedy něco těžšího – zástupce typické skupiny úloh řešitelných Jensenovou nerovností:

Příklad. Jsou-li α, β, γ velikosti úhlů v trojúhelníku, dokažte

$$\sin\alpha + \sin\beta + \sin\gamma \leq \frac{3\sqrt{3}}{2}.$$

Řešení. Jensenovu nerovnost aplikujeme na funkci $f(x) = \sin x$, která je konkávní na intervalu $(0, \pi)$. Platí $\alpha, \beta, \gamma \in (0, \pi)$, tedy

$$\frac{1}{3}\sin\alpha + \frac{1}{3}\sin\beta + \frac{1}{3}\sin\gamma \leq \sin\left(\frac{\alpha+\beta+\gamma}{3}\right) = \frac{\sqrt{3}}{2}.$$

U této nerovnosti bychom již přímočařejší přístup hledali těžko. Jensenova nerovnost je pro dokazování nerovností pro úhly v trojúhelníku často užitečná, neboť známe jejich součet (a tedy i tu nejjednodušší konvexní kombinaci).

Logaritmus

Občas se při používání Jensenovy nerovnosti setkáme s logaritmem. Užitečný pro nás bude zejména tím, že svým způsobem převádí násobení na sčítání a mocnění na násobení. Přesněji o tom hovoří následující poznámka.

Poznámka. Nechť je reálné číslo $a > 1$. Funkce $f(x) = \log_a(x)$ definovaná na $\mathbb{R}^+$ jako inverzní funkce k $g(x) = a^x$ má následující vlastnosti:

(i) f je rostoucí ryze konkávní funkce na $\mathbb{R}^+$,

(ii) $f(xy) = f(x) + f(y)$,

(iii) $f\left(\frac{1}{x}\right) = -f(x)$,

(iv) $f(x^y) = yf(x)$.

Jensenova nerovnost je ve skutečnosti velmi silná metoda – lze s ní například dokázat většinu běžně používaných nerovností:

Věta. (trojúhelníková nerovnost) *Pro reálná čísla $x_1, x_2, \ldots, x_n$ platí:*

$$|x_1| + |x_2| + \cdots + |x_n| \geq |x_1 + x_2 + \cdots + x_n|.$$

Věta. (AH nerovnost) *Pro kladná čísla $x_1, x_2, \ldots, x_n$ platí:*

$$\frac{x_1 + \cdots + x_n}{n} \geq \frac{n}{\frac{1}{x_1} + \cdots + \frac{1}{x_n}}.$$

Věta. (AG nerovnost) *Pro nezáporná čísla $x_1, x_2, \ldots, x_n$ platí:*

$$\frac{x_1 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 \ldots x_n}.$$

Věta. (Cauchy-Schwarzova nerovnost) *Pro libovolná reálná čísla $x_1, x_2, \ldots, x_n$, $y_1, y_2, \ldots, y_n$ platí:*

$$\left(x_1^2 + \cdots + x_n^2\right)\left(y_1^2 + \cdots + y_n^2\right) \geq \left(x_1 y_1 + \cdots + x_n y_n\right)^2.$$

Nápověda: Dokažte nerovnost pro nenulová y_i. Rozmyslete si, kdy nastává rovnost.

Nyní už víme dost, abychom se mohli pustit do řešení skutečných úloh. Nezapomeňte, že Jensenova nerovnost platí pro každou konvexní (resp. konkávní) funkci, takže pokud kýžená nerovnost hned napoprvé nevyjde, není důvod házet Jensena do žita – prostě zkuste jinou funkci. Tak hurá do toho!

Úlohy na rozehřátí

Úloha 1. Ukažte, že pro libovolná reálná čísla $a, b \in \langle -1, 1\rangle$ platí

$$\sqrt{1-a^2} + \sqrt{1-b^2} \leq \sqrt{4-(a+b)^2}.$$

Úloha 2. Dokažte, že pro kladná reálná čísla a, b splňující $a+b=1$ platí

$$\left(a+\frac{1}{a}\right)^2 + \left(b+\frac{1}{b}\right)^2 \geq \frac{25}{2}.$$

Úloha 3. Dokažte, že pro všechna přípustná $x \in \mathbb{R}$ platí

$$\sqrt{x+1} + \sqrt{2x-3} + \sqrt{50-3x} \leq 12.$$

Úloha 4. Pro α, β, γ úhly v trojúhelníku dokažte nerovnosti

(i) $\sin\frac{\alpha}{2} + \sin\frac{\beta}{2} + \sin\frac{\gamma}{2} \leq \frac{3}{2}$,

(ii) $\cos\frac{\alpha}{2} + \cos\frac{\beta}{2} + \cos\frac{\gamma}{2} \leq \frac{3\sqrt{3}}{2}$,

(iii) $\operatorname{tg}\frac{\alpha}{2} + \operatorname{tg}\frac{\beta}{2} + \operatorname{tg}\frac{\gamma}{2} \geq \sqrt{3}$,

(iv) $\sin\alpha\sin\beta\sin\gamma \leq \frac{3\sqrt{3}}{8}$.

Úloha 5. Ukažte, že pro úhly α, β, γ, δ v tětivovém čtyřúhelníku platí

$$4\sin\frac{\alpha}{4} + 3\sin\frac{\beta}{3} + 2\sin\frac{\gamma}{2} + \sin\delta \leq 3 + 2\sqrt{2}.$$

Úloha 6. Pro kladná a, b, c dokažte

$$\sqrt[4]{27\,(a^7+b^7+c^7)} \geq \sqrt[4]{a^7} + \sqrt[4]{b^7} + \sqrt[4]{c^7}.$$

Úloha 7. Kladná reálná čísla x, y splňují $x+y=1$. Dokažte

$$\frac{x}{1+y} + \frac{y}{1+x} \geq \frac{1}{1+2xy}.$$

Pořádné úlohy

Úloha 8. Ukažte, že v ostroúhlém trojúhelníku platí

$$a+b+c \geq \sqrt{2bc\cos\alpha} + \sqrt{2ac\cos\beta} + \sqrt{2ab\cos\gamma}.$$

Úloha 9. Pro kladná a, b, c dokažte

$$\frac{a}{(b+c)^2} + \frac{b}{(c+a)^2} + \frac{c}{(a+b)^2} \geq \frac{9}{4(a+b+c)}.$$

Úloha 10. Pro $a, b \geq 0$ dokažte

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

(MO 63–III–6)

Úloha 11. Pro $a, b, c > 0$ dokažte

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

Úloha 12. Pro reálná $x_1, \ldots, x_n \geq 1$ dokažte

$$\frac{1}{x_1+1} + \cdots + \frac{1}{x_n+1} \geq \frac{n}{\sqrt[n]{x_1 \cdots x_n}+1}.$$

(IMO Shortlist 1998)

Úloha 13. Pro kladná a, b, c dokažte

$$\frac{a}{\sqrt{a^2+8bc}} + \frac{b}{\sqrt{b^2+8ac}} + \frac{c}{\sqrt{c^2+8ab}} \geq 1.$$

(IMO 2001)

Návody

4. V podúloze (iv) využijte buďto funkci $\log(\sin x)$, nebo jen $\log x$ a dříve dokázané tvrzení.

8. Použijte kosinovou větu a substituci $a = \sqrt{x+y}$, $b = \sqrt{y+z}$, $c = \sqrt{z+x}$.

9. Použijte funkci $\dfrac{1}{x^2}$.

11. Platí, že $f(x) = x \log x$ je pro $x > 0$ konvexní.

12. Všimněte si, že pro $x_i \leq 1$ tvrzení neplatí. Hodí se substituce $y_i = \log x_i$.

13. Použijte funkci $\dfrac{1}{\sqrt{x}}$.

Zdroje

Příspěvek je z větší části založen na dřívějších přednáškách Davida Hrušky a Martina Töpfera. K těžším úlohám byly přidány hinty a změněna byla především část o standardních nerovnostech a goniometrických úlohách.

AG nerovnost

Marian Poljak

Abstrakt. V příspěvku jsou obsažena základní i pokročilá užití AG nerovnosti.

Účinné používání nerovností patří k základním dovednostem člověka účastnícího se matematických soutěží. Přestože je tento text zaměřen primárně na řešení nerovností, soustavy rovnic jsou s jejich pomocí také často hračka a silné odhady nezřídka vyřeší i nealgebraickou úlohu. Jednou ze (dvou) stěžejních nerovností je nerovnost mezi aritmetickým a geometrickým průměrem (zkráceně AG nerovnost). V této dvojpřednášce se s ní seznámíme a ukážeme si všechny možné nekalé triky, které s ní můžeme provádět.

Věta. (AG nerovnost) *Pro libovolná nezáporná čísla* $x_1, x_2, \ldots, x_n$ *platí*

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 \cdot x_2 \cdots x_n}.$$

Poznámka. Rovnost nastává právě tehdy, když $x_1 = x_2 = \cdots = x_n$.

Příklad.

(1) $a^2 + b^2 \geq 2ab$,
(2) $(a + b + c)(\frac{1}{a} + \frac{1}{b} + \frac{1}{c}) \geq 9$,
(3) $2x^3 + y^3 \geq 3x^2y$.

Cvičení. (Základní fígle.) Pro x, y, z kladná dokažte:

(1) $\frac{a}{b} + \frac{b}{a} \geq 2$,
(2) $x^3 + y^3 + z^3 \geq 3xyz$,
(3) $x^2 + \frac{2}{x} \geq 3$,
(4) $\frac{x^3}{yz} + y + z \geq 3x$,
(5) $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} \geq 3$,
(6) $2(x + y + z)(x^2 + y^2 + z^2) \geq x^3 + y^3 + z^3 + 15xyz$,
(7) $\frac{z}{x} + \frac{x}{y+z} + \frac{y}{z} \geq 2$.

Příklad. Nechť a, b jsou kladná reálná čísla taková, že $a > b$. Najděte minimum výrazu

$$a + \frac{1}{b(a-b)}.$$

Příklad. Najděte všechna kladná reálná řešení (a, b, c, d) splňující $a+b+c+d = 12$ a $abcd = 27 + ab + ac + ad + bc + bd + cd$.

Sčítání AG nerovností a míchání členů

Jak jste si možná všimli, většina dosud dokazovaných nerovností měla společnou jednu věc – členů na jedné straně nerovnosti bylo hodně, zatímco na druhé straně jeden. To samozřejmě (při letmém pohledu na AG nerovnost) není náhoda. Co kdybychom ale chtěli AG utilizovat i pro boj s následující nerovností?

$$x^3 + y^3 + z^3 \geq x^2y + y^2z + z^2x$$

Není těžké ověřit, že nerovnost (konkrétně její trojnásobek) můžeme „namíchat“ součtem nerovnosti $2x^3 + y^3 \geq 3x^2y$ a jejích cyklických záměn.

Ukažme si, jak na správné namíchání přijít!

Příklad. Dokažte, že pro kladná reálná x, y, z platí

$$x^3y + y^3z + z^3x \geq x^2yz + y^2zx + z^2xy.$$

Cvičení. (Míchací.) Pro x, y, z kladná dokažte (a určete, kdy nastává rovnost):

(1) $x^2 + y^2 + z^2 \geq xy + yz + zx$,
(2) $x^4 + y^4 + z^4 \geq x^3y + y^3z + z^3x$,
(3) $x^4y + y^4z + z^4x \geq x^2y^2z + y^2z^2x + z^2x^2y$,
(4) $\frac{x^2}{y} + \frac{y^2}{z} + \frac{z^2}{x} \geq x + y + z$,
(5) $x^7 + 1 \geq x^4 + x^3$,
(6) $\frac{x^3}{y} + \frac{y^3}{z} + \frac{z^3}{x} \geq xy + yz + zx$.

Poslední cvičení ukázala, že rozložit nepříjemnou nerovnost na součet několika lehčích nerovností může často vést k řešení. Musíme si však dát pozor na to, aby tyto lehčí nerovnosti platily. Pojďme si techniku „Rozděl a panuj!“ ukázat na různorodějších příkladech!

Příklad. Dokažte, že pro kladná reálná x, y, z platí

$$a^3 + b^3 + c^3 + 6 \geq 3(a + b + c).$$

Příklad. Dokažte, že pro kladná reálná x, y, z platí

$$(x + y)(y + z)(z + x) \geq 8xyz.$$

Příklad. Pro $a, b, c > 0$ dokažte nerovnost

$$\frac{2}{3}(a+b+c) \geq \sqrt[3]{ab} + \sqrt[3]{bc} + \sqrt[3]{ca} - 1.$$

Poznámka. Pomaličku začíná přituhovat a budeme bojovat se složitějšími výrazy. Abychom se v úpravách neztratili, vyzbrojíme se znakem tzv. *cyklické sumy*. Funguje to nějak takto: $\sum_{cyc} a = a + b + c$, $\sum_{cyc} xy^2 = xy^2 + yz^2 + zx^2$. Například jedno z prvních cvičení lze zapsat následovně:

$$2\left(\sum_{cyc} x\right)\left(\sum_{cyc} x^2\right) \geq \sum_{cyc} x^3 + 15xyz.$$

Lehké odhady na těžké nerovnosti

Asi největší využití AG nerovnosti spočívá v tvorbě odhadů, „mezivýrazů“, které vypadají rozumněji než levá a pravá strana a které se mezi ně proto pokoušíme vklínit. Mnohdy je vztah mezi levou a pravou stranou nerovnosti natolik slabý, že i ne moc dobrý odhad úlohu vyřeší. U těžších nerovností jsou silné odhady často nutností (a jejich používání vyžaduje notnou dávku praxe). Obojí si ukážeme.

Příklad. Pro $a, b, c > 0$ dokažte nerovnost

$$\sum_{cyc} \frac{1}{a^3 + b^3 + abc} \leq \frac{1}{abc}.$$

Poznámka. (Nenápadná, ale důležitá.) Při dokazování neostrých nerovností má smysl používat pouze takové odhady, u kterých se zachovají případy rovnosti.

Příklad. Pro $a, b, c > 0$ dokažte nerovnost

$$(a^5 - a^2 + 3)(b^5 - b^2 + 3)(c^5 - c^2 + 3) \geq (a+b+c)^3.$$

(USAMO, 2004)

AG vs. zlomky

Na úlohy se zlomky je většinou silnou zbraní Cauchyho–Schwarzova nerovnost (ta druhá stěžejní nerovnost). Nicméně i AG lze na zlomky použít překvapivě dobře – stačí sečíst zlomek s jeho jmenovatelem (funguje zejména u slabších nerovností). Při řešení nezapomeňme na poznámku o rovnosti!

Příklad. Pro $a, b, c > 0$ dokažte nerovnost

$$\frac{a^3}{bc} + \frac{b^3}{ca} + \frac{c^3}{ab} \geq a + b + c.$$

Příklad. Dokažte, že pro každá $a, b, c > 0$ platí

$$\sum_{cyc} \frac{a^3}{(a+b)(a+c)} \geq \frac{a+b+c}{4}.$$

Příklad. Pro a, b, c kladná dokažte

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

Vážená verze AG nerovnosti

K jejímu důkazu je třeba vyššího matematického aparátu. Ale platí a její obecnost se může hodit.

Věta. (Vážená AG nerovnost) *Pro libovolná reálná nezáporná čísla x_1, x_2, …, x_n a reálná nezáporná w_1, w_2, …, w_n s kladným součtem w. Pak platí*

$$\frac{w_1x_1 + w_2x_2 + \cdots + w_nx_n}{w} \geq \sqrt[w]{x_1^{w_1}x_2^{w_2}\cdots x_n^{w_n}}.$$

Poznámka. Rovnost nastává právě tehdy, když všechny x_i, pro která je $w_i > 0$, mají stejnou hodnotu.

Poznámka. Pro $w_1 = w_2 = \cdots = w_n = \frac{1}{n}$ dostáváme klasickou AG nerovnost.

Příklad. Dokažte, že pro kladná reálná a, b, c splňující $a + b + c = 3$ platí

$$a^b b^c c^a \leq 1.$$

Úlohy na procvičení (triviální až středně obtížné)

Úloha 1. Anička našla 4 kladná reálná čísla – součet dvou z nich je 42 a součet druhých dvou je 4. Jaký nejvyšší může být součin všech těchto čtyř čísel?

Úloha 2. Určete všechna kladná reálná x, y, z splňující $x + y + z = 6$ a $xyz = 8$.

Úloha 3. Dokažte, že pro každé přirozené $n > 1$ platí

$$\left(\frac{1}{2} + \frac{2}{3} + \cdots + \frac{n}{n+1}\right)^n > \frac{n^n}{n+1}.$$

Úloha 4. Najděte minimum výrazu $\frac{9x^2 \sin x^2 + 4}{x \sin x}$ pro $0 < x < \pi$.

Úloha 5. Dokažte, že pro kladná reálná x, y, z platí

$$x^2 + y^2 + z^2 \geq x\sqrt{y^2 + z^2} + y\sqrt{x^2 + z^2}.$$

Úloha 6. Nechť $xyz = 32$, kde x, y, z jsou kladná reálná. Najděte minimum výrazu

$$x^2 + 4xy + 4y^2 + 2z^2.$$

Úloha 7. Dokažte, že pro $0 \leq a \leq b \leq c$ platí $(a + 3b)(b + 4c)(c + 2a) \geq 60abc$.

Úloha 8. Na každé straně čtverce o straně 1 zvolíme bod. Tyto body vytvoří čtyřúhelník o stranách a, b, c, d. Dokažte, že platí $2 \leq a^2 + b^2 + c^2 + d^2 \leq 4$ a $2\sqrt{2} \leq a + b + c + d \leq 4$.

Úloha 9. Dokažte, že pro kladná a, b, c platí

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

Úloha 10. Dokaž, že pro kladná a_1, a_2, …, a_n, jejichž součin je 1, platí

$$\frac{a_1}{1+a_1} + \frac{a_2}{(1+a_1)(1+a_2)} + \cdots + \frac{a_n}{(1+a_1)(1+a_2)\cdots(1+a_n)} \geq 1 - \frac{1}{2^n}.$$

Úloha 11. Dokažte, že pro $a, b, c > 0$ splňující $abc = 1$ platí

$$\sum_{cyc} \frac{a^3}{(1+a)(1+b)} \geq \frac{3}{4}.$$

Úloha 12. Dokažte, že pro $a, b, c > 0$ platí

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

Těžší úlohy

Úloha 13. Nechť $a, b, c > 0$ a $abc = 1$. Dokažte, že platí

$$a^4 + b^4 + c^4 + a + b + c + \frac{2a}{b^2 + c^2} + \frac{2b}{a^2 + c^2} + \frac{2c}{a^2 + b^2} \geq 9.$$

Úloha 14. Ukažte, že pro každou trojici kladných čísel a, b, c splňující $abc = 1$ platí

$$\sum_{cyc} \frac{ab}{a^5 + b^5 + ab} \leq 1.$$

(IMO shortlist, 1996)

Úloha 15. Pro a, b, c kladná platí $a+b+c=1$. Dokažte, že

$$\sqrt{a^{1-a}b^{1-b}c^{1-c}} \leq \frac{1}{3}.$$

(Rakousko, 2008)

Úloha 16. Nechť $n>2$ je přirozené číslo a $x_1, x_2, \ldots, x_n$ jsou kladná reálná čísla. Ukažte, že

$$\sum_{cyc} \frac{1}{x_i^3 + x_{i-1}x_ix_{i+1}} \leq \sum_{cyc} \frac{1}{x_ix_{i+1}(x_i+x_{i+1})}.$$

(6. série A3, 6. ročník iKS)

Úloha 17. Nechť $n>2$ a $a_2, a_3, \ldots, a_n$ jsou kladná reálná čísla splňující podmínku $a_2a_3\cdots a_n=1$. Dokažte, že platí

$$(1+a_2)^2(1+a_3)^3\cdots(1+a_n)^n > n^n.$$

(IMO 2, 2012)

Úloha 18. Nechť $a,b,c>0$ a $a+b+c=1$. Dokažte, že platí

$$\sum_{cyc} \frac{a^3+bc}{a^2+bc} \geq 2.$$

Úloha 19. Ukažte, že pro každé přirozené n a každou n-tici kladných reálných čísel $x_1, x_2, \ldots, x_n$ platí

$$(1+x_1)(1+x_1+x_2)\cdots(1+x_1+x_2+\cdots+x_n) \geq \sqrt{(n+1)^{n+1}x_1x_2\ldots x_n}.$$

(35. ročník MKS, finální myšmaš)

Úloha 20. Mějme ostroúhlý trojúhelník ABC a jemu opsanou kružnici se středem O a poloměrem R. Označme D druhý průsečík přímky AO s kružnicí opsanou BOC, E druhý průsečík přímky BO s kružnicí opsanou AOC a F druhý průsečík přímky CO s kružnicí opsanou AOB. Dokažte

$$|OD|\cdot|OE|\cdot|OF| \geq 8R^3.$$

Úloha 21. Nechť $a,b,c>0$ a $abc=1$. Dokažte, že platí

$$\frac{a}{2b+c^2} + \frac{b}{2c+a^2} + \frac{c}{2a+b^2} \leq \frac{a^2+b^2+c^2}{3}.$$

Úloha 22. Nechť $a, b, c > 0$ a platí

$$a + b + c = \frac{1}{a^2} + \frac{1}{b^2} + \frac{1}{c^2}.$$

Dokažte, že platí

$$2(a + b + c) \geq \sqrt[3]{7a^2b + 1} + \sqrt[3]{7b^2c + 1} + \sqrt[3]{7c^2a + 1},$$

a určete, pro které trojice (a, b, c) nastává rovnost.

Úloha 23. Nechť $a, b, c > 0$ a $a + b + c = 1$. Dokažte, že platí

$$\sum_{cyc} \frac{\sqrt{a^2 + abc}}{c + ab} \leq \frac{1}{2\sqrt{abc}}.$$

Návody

1. Dvě lehká AGčka, vyjde $\frac{441}{4}$.

2. Kdy nastává při AG nerovnosti rovnost? :)

3. Je to vlastně AG nerovnost.

4. Substituce $a = x \sin x$, pomůže, výsledek je 12.

5. $x^2 + (y^2 + z^2) \geq \ldots$

6. $(x + 2y)^2 \geq 8xy$, mělo by vyjít 96.

7. Podmínky je třeba využít – zkus po roznásobení zmenšit levou stranu tak, aby byl příklad ekvivalentní jediné AG nerovnosti.

8. Může se hodit $2(a^2 + b^2) \geq (a + b)^2$.

9. Roznásobit a dvě AGčka.

10. Dokaž indukcí, že levá strana je $\frac{(1+a_1)(1+a_2)\cdots(1+a_n)-1}{(1+a_1)(1+a_2)\cdots(1+a_n)}$.

11. Zkus v AGčku vyrušit jmenovatele – pozor, aby nastávala rovnost!

12. Po roznásobení se může hodit substituce $x = \frac{a}{b}$.

13. $\frac{2a}{b^2+c^2} + \frac{b^2+c^2}{2} + a^2 \geq \ldots$ je dobrý začátek. :)

14. Použij odhad $a^5 + b^5 \geq a^3b^2 + a^2b^3$.

15. Je třeba použít váženou AG nerovnost.

16. Použij úlohu 9 na odhad členů levé strany a upravuj.

17. Známá substituce umí odstranit podmínku. Potom např. $(x_2 + x_3)^3 = (\frac{x_2}{2} + \frac{x_2}{2} + x_3)^3 \geq \ldots$

18. Po úpravě do tvaru $\sum_{cyc} \frac{bc(1-a)}{a^2+bc} \geq 1$ jde roznásobit.

19.

$$(1+x_1+\cdots+x_i)^{n-i+2} \geq \frac{(n-i+2)^{n-i+2}}{(n-i+1)^{n-i+1}}(1+x_1+\cdots+x_{i-1})^{n-i+1}x_i.$$

20. Dokaž $\frac{|OD|}{\sin|\sphericalangle OBD|} = \frac{|BC|}{\sin|\sphericalangle BOC|}$, použij vzorec $\frac{|BC|}{2\sin\alpha} = R$ a trochu goniometrie. AGčko je až poslední krok.

21. Odhadnout jmenovatele, zatnout zuby a nebát se homogenizovat pro $a = x^9$.

22. $a + a + \frac{7b+\frac{1}{a^2}}{8} \geq \ldots$ Alternativně lze řešit pomocí tzv. *Hölderovy nerovnosti*.

23. Je ekvivalentní

$$\sum_{cyc} a(a+b)\sqrt{bc(a+c)(a+b)} \leq \frac{1}{2}(a+b+c)(a+b)(b+c)(c+a).$$

Odhadni odmocninu hezkým AGčkem, zatni zuby a pokračuj.

Literatura a zdroje

[1] Michal Rolínek, Pavel Šalom: *Zdolávání nerovností*, Univerzita J.E. Purkyně, 2012.

[2] Samin Riasat: *Basics of Olympiad Inequalities.*

Catalanova čísla

Martin Raška

Abstrakt. Catalanova čísla jsou vedle kombinačních čísel jedny z nejčastěji se vyskytujících posloupností čísel v kombinatorice. V tomto příspěvku si představíme, co to vlastně je, a podíváme se na překvapivé množství úloh, kde hrají roli.

Definice. *Obdélníkem* $m \times n$ rozumíme obdélník ve čtvercové mřížce, který je m políček vysoký a n políček široký. *Cestou* v obdélníku pak nazýváme trasu z levého dolního do pravého horního rohu, která vede po hranách mřížky, a to pouze doprava a nahoru.

Cvičení. Dokažte, že v obdélníku $m \times n$ existuje $\binom{m+n}{n}$ různých cest.

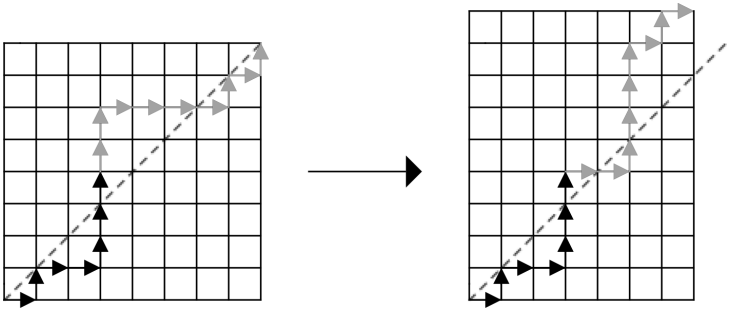
Definice. *Úhlopříčkou* ve čtverci $n \times n$ nazveme úsečku spojující levý dolní roh s pravým horním.

Definice. Symbolem C_n budeme značit n-té *Catalanovo číslo*, které si definujeme jako počet cest ve čtverci $n \times n$, které jsou celé pod úhlopříčkou (smí se jí dotýkat).

Tvrzení.

$$C_n = \binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1}\binom{2n}{n}$$

Důkaz. (náznak důkazu) Ve čtverci $n \times n$ spočítáme počet nevyhovujících cest, tj. takových cest, které překročí diagonálu, a tento počet pak odečteme od celkového počtu cest.



Mějme libovolnou nevyhovující cestu a podívejme se na místo, kde se poprvé dostane nad diagonálu. V momentě, kdy poprvé překročíme diagonálu a ujdeme krok směrem nahoru, zbytek cesty převrátíme, jak naznačuje obrázek (z cest nahoru se stanou cesty doprava a naopak). Nově vzniklá cesta bude obsahovat $n+1$ kroků směrem nahoru a $n-1$ kroků směrem doprava, bude tedy cestou v obdélníku $(n+1)\times(n-1)$. Překlopením nazpátek ve stejném místě dostaneme jednoznačně určenou původní cestu, tedy toto zobrazení je prosté.

Stejně tak můžeme z libovolné cesty v obdélníku $(n+1)\times(n-1)$ analogickým překlopením získat nevyhovující cestu v obdélníku $n\times n$ a toto zobrazení je rovněž prosté. Existuje tedy bijekce mezi cestami ve čtverci $n\times n$ překračujícími úhlopříčku a cestami v obdélníku $(n+1)\times(n-1)$, kterých je $\binom{2n}{n+1}$. □

Poznámka. Často se definuje i $C_0 = 1$. Prvních několik Catalanových čísel je postupně 1, 1, 2, 5, 14, 42, 132, 429, ...

Příklad 1. Kolik existuje různých cest v obdélníku $m\times n$, které jsou celé pod úhlopříčkou levého čtverce $m\times m$?

Rekurentní vzorec

Tvrzení. *Mějme posloupnost $(a_n)_{n\geq 0}$ splňující vztahy*

$$a_0 = 1,$$

$$a_{n+1} = \sum_{i=0}^{n} a_i a_{n-i}.$$

Pak $a_n = C_n$.

Úloha. Kolik existuje různých triangulací konvexního n-úhelníka[1]?

Zobecnění

Vrátíme-li se k původní definici Catalanových čísel, je přirozené se zeptat, jaká čísla dostaneme, pokud daný obdélník nebude čtverec. To vede k rozšíření Catalanových čísel.

Definice. Definujeme $C(n,k)$ pro $0\leq k\leq n$ jako počet cest v obdélníku $k\times n$, které vedou celé pod diagonálou levého čtverce $k\times k$. Volbou $k=n$ dostaneme právě C_n.

Rozšířením prvního důkazu identity charakterizující Catalanova čísla dostaneme podobný vztah, konkrétně

[1]Rozdělení na $n-2$ trojúhelníků, jejichž vrcholy jsou vrcholy původního n-úhelníka.

$$C(n,k) = \binom{n+k}{k} - \binom{n+k}{k-1}.$$

Přirozená struktura této konstrukce nám dovoluje vytvořit Catalanův trojúhelník, který je znázorněný na obrázku.

						132	⋯
					42	132	⋯
				14	42	90	⋯
			5	14	28	48	⋯
		2	5	9	14	20	⋯
	1	2	3	4	5	6	⋯
1	1	1	1	1	1	1	⋯

Číslo $C(n,k)$ je v $(n+1)$-ním sloupci a $(k+1)$-ním řádku. Catalanova čísla jsou přesně na diagonále.

Z faktu, že čísla jsou definována jako počet cest, není již těžké přejít k rekurentnímu vztahu $C(n,k) = C(n,k-1) + C(n-1,k)$ pro $0 < k < n$. Ten říká, že číslo v Catalanově trojúhelníku je součtem čísla pod ním a nalevo od něj, což jsou přesně místa odkud můžeme k danému vrcholu dojít námi definovanými cestami. Tento trojúhelník má, stejně jako ten Pascalův, množství pěkných vlastností. Například si lze všimnout, že součet každého sloupce dává Catalanovo číslo.

Konečně nějaké příklady

Příklad 2. Kolik existuje korektních uzávorkování n párů závorek?

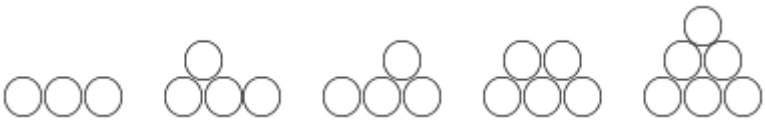
Příklad 3. Kolik existuje posloupností délky n splňujících $1 \le a_1 \le a_2 \le \cdots \le a_n$ a navíc $a_i \le i$?

Příklad 4. Kolika způsoby si může $2n$ lidí podat ruce přes stůl tak, aby se žádné dva páry rukou nekřížily (každý člověk podává právě jednu ruku jinému člověku)?

Příklad 5. Kolika způsoby lze vyplnit tabulku $2 \times n$ čísly 1 až $2n$ tak, aby čísla v obou řádcích i ve všech sloupcích byla rostoucí?

Příklad 6. Nechť n je přirozené číslo. Kolik existuje cest v kartézské soustavě souřadnic, které vedou z bodu $(0,0)$ do bodu $(2n,0)$, takových, že z libovolného bodu (x,y) cesta pokračuje buď do bodu $(x+1,y+1)$, nebo do bodu $(x+1,y-1)$? Kolik z těchto cest nikdy neklesne pod osu x?

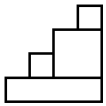
Příklad 7. Kolika způsoby je možné navršit mince na hromádku, je-li ve spodní řadě n mincí? Na obrázku jsou všechny možné hromádky pro $n = 3$.



Příklad 8. Kolik existuje binárních stromů[2] na n vrcholech? Rozlišujeme „pravé“ a „levé“ syny.

Příklad 9. Kolik existuje zakořeněných stromů (rozlišujeme pořadí synů) s n vrcholy?

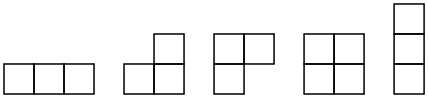
Příklad 10. Kolika způsoby je možno postavit schodiště o n schodech pomocí n obdélníků? Na obrázku je schodiště o 4 schodech postavené ze 4 obdélníků.



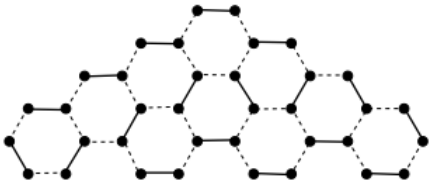
Příklad 11. Kolik je permutací množiny $\{1, \ldots, n\}$, které neobsahují klesající podposloupnost délky větší než 2?
(Označíme-li permutaci p, pak neexistují $i, j, k \in \{1, \ldots, n\}$ takové, že $i < j < k$ a zároveň $p(i) > p(j) > p(k)$.)

Příklad 12. Pro která n je C_n liché?

Příklad 13. Polyomino[3] nazveme *neklesající*, pokud je každý jeho sloupec souvislý (tj. není rozdělen na více částí oddělených prázdnými čtverečky), pozice horního čtverečku v každém sloupci se zleva doprava nesnižuje a obdobně se v každém sloupci nesnižuje pozice nejnižšího čtverečku zleva doprava. Kolik existuje *neklesajících* polyomin s obvodem délky $2n$? Obrázek zachycuje případ pro $n = 4$.



Příklad 14. Kolik existuje úplných párování vrcholů na šestiúhelníkové pyramidě šířky n? Úplné párování na šestiúhelníkové pyramidě šířky 4 může vypadat například takto:



[2]Pokud nevíš, co to znamená, neboj se zeptat přenášejícího!
[3]Útvar vzniklý sloučením několika jednotkových čtverců dotýkajících se hranou.

Návody

2. Převeď si to na počet cest pod diagonálou nebo rekurzí podle první korektní podposloupnosti.

3. Převeď na hledání cest pod diagonálou – dívej se na vodorovné hrany.

5. Bijekce na cesty pod diagonálou. Pořadí pohybu danými směry.

7. Rekurze, nejpravější mezera v druhé vrstvě odspodu.

9. Zakóduj si strom pomocí 1 a 0 (resp. závorek) a převeď na příklad 2.

10. Dvě různá políčka na úhlopříčce nemůžou být ve stejném obdélníku. Roh.

11. Zaznač si permutaci to tabulky $n \times n$ a najdi pomocí permutace cestu nad/pod diagonálou.

12. Použij rekurentní vztah a indukci.

13. Koukni se na horní a dolní trasu z levého dolního do pravého horního rohu polyomina. Poskládej pomocí nich trasu pod diagonálou čtverce.

14. Otoč si obrázek o 150° po směru hodinových ručiček. V každé vrstvě svislých hran je na párování použita právě jedna hrana. Po otočení jde vidět přirozená bijekce mezi volbou těchto hran a hledání cest pod uhlopříčkou.

Literatura a zdroje

Velká část příspěvku je převzatá z přednášek Martina Hory a Anči Chejnovské, jimž bych tímto chtěl poděkovat.

[1] Martin Hora, *Catalanova čísla*, 2012 Domašov

[2] Anča Chejnovská, *Catalanova čísla*, 2015 Staré Město

[3] Richard P. Stanley, *Exercises on Catalan and Related Numbers*, *http://www-math.mit.edu/~rstan/ec/catalan.pdf*

[4] Tom Davis, *Catalan Numbers*, *http://www.geometer.org/mathcircles/catalan.pdf*

Extremální princip

Martin Raška

Abstrakt. Příspěvek obsahuje několik příkladů vhodných na procvičení jedné ze základních důkazových metod – extremálního principu.

Extremální princip je základní důkazovou metodou. Spočívá v tom, že nalezneme něco, co je v nějakém slova smyslu maximální (nebo minimální), a zamyslíme se, co z toho vyplývá. Velmi často kombinujeme extremální princip s důkazem sporem. Například uvážíme nejdelší úsečku a ukážeme, že pak by musela existovat i nějaká delší, čímž získáme spor. Pojďme si ukázat použití extremálního principu na úloze.

Úloha. V nekonečných rovinatých tajgách Moravskoslezského kraje rostou v pravidelné čtvercové síti zakrslé smrky, přičemž výška každého je průměrem výšek všech čtyř kolem stojících stromů. Pokud výšky nabývají přirozených hodnot, ukažte, že jsou stromy stejně vysoké.

Řešení. (Náznak) Protože výšky stromů jsou přirozené, existuje (ne nutně jeden) strom s nejmenší výškou. Nějaký takový si vyberme a označme S. Všichni čtyři jeho sousedi musí mít výšku stejnou nebo vyšší. Kdyby byl ale nějaký vyšší, výška stromu S by nebyla průměrem výšek okolních stromů. Proto všichni jeho sousedi mají stejnou výšku jako S. Indukcí pak snadno ukážeme, že všechny stromy jsou stejně vysoké.

Nyní se můžeme pustit do samostatného počítání.

Příklady

Příklad 1. Lenička dokázala, že prvočísel je konečně mnoho. Ukažte, že se spletla.

Příklad 2. Michal žije v kraji, kde jsou města vystavena v takových rozestupech, že trojúhelník s vrcholy v libovolných třech městech má rozlohu menší než 390 000 km^2. Ukažte, že všechna města se vejdou na plochu menší, než má Mongolsko.[1]

Příklad 3. Eva si do sešitu nakreslila konečně mnoho bodů. Přišli k ní Martin s Albertem a všimli si, že každá přímka, která prochází skrz dva body, prochází i nějakým třetím bodem. Ukažte, že všechny body leží v jedné přímce.

[1] Poradím, že Mongolsko má rozlohu 1 566 500 km^2.

Příklad 4. Jonáš dal Vaškovi za úkol najít aspoň jedno celočíselné řešení rovnice $a^2 + b^2 = 3(c^2 + d^2)$. Pomozte mu a najděte dokonce všechna taková řešení.

Příklad 5. V Pszczynie jsou všechny silnice jednosměrné a každé dvě křižovatky jsou propojeny právě jednou silnicí. Ukažte, že existuje křižovatka, do které se dá dostat z každé jiné buď přímo, nebo po dvou silnicích.

Příklad 6. Na Petrově oslavě narozenin se každý pohádal s nejvýše třemi lidmi. Je možné účastníky slavnosti rozdělit do dvou skupin tak, aby každý měl ve své skupině nejvýše jednoho jiného člověka, se kterým se pohádal?

Příklad 7. Ondřej, Adam a jejich pět kamarádů sedí kolem kruhového stolu. Každý před sebou má pohár s mlékem. Dohromady mají mléka tři litry. Nejdřív první z nich vstane a rozdělí své mléko rovnoměrně mezi ostatní. Pak postupně proti směru hodinových ručiček totéž udělají i zbývající spolusedící. Když skončí, má každý z nich tolik mléka, kolik měl na začátku. Kolik to je?

Příklad 8. Pepa s Radkem hráli 3D šachy a přitom je napadla otázka, kolik nejméně věží je potřeba, aby ohrožovaly všechna políčka šachovnice $n \times n \times n$. Kolik to je?

Příklad 9. Města na Kubě neleží na jedné přímce. Ukažte, že pak existuje přímka, která prochází jen přes dvě z těchto měst. Platilo by to, i kdyby bylo měst nekonečně mnoho?

Příklad 10. Daniel dokázal, že prvočísel ve tvaru $6n-1$ je konečně mnoho. Ukažte, že se spletl.

Příklad 11. V Praze je n hradů a n studen takových, že žádné tři stavby neleží na jedné přímce. Adéla s Karolínou se shodly, že by bylo vhodné každý hrad spojit s jednou studnou přímou cestou aniž by se cesty křížily. Je možné to provést?

Příklad 12. Lucka si na zahrádce stoupla ke čtverečkovanému záhonu $n \times n$ a rozestavila na něj květináče s chryzantémami. Potom přišel Zdeněk a všiml si, že kdykoli máme v záhonu prázdný čtvereček, tak v řádku a sloupci, které daný čtvereček obsahují, je dohromady alespoň n chryzantém. Dokažte, že Lucka rozestavila alespoň $\frac{n^2}{2}$ chryzantém.

Příklad 13. Po drtivém útoku Humpolce na americký Pentagon byla podstava této budovy zdeformována do tvaru obecného konvexního pětiúhelníku. Matěj ukázal, že i tak z ní jde vybrat tři úhlopříčky, z nichž lze vytvořit trojúhelník. Ukažte to taky!

Příklad 14. Tomáš tvrdí, že každý mnohostěn má alespoň dvě stěny se stejným počtem hran. Petr mu to ale odmítá věřit. Kdo z chlapců má pravdu?

Příklad 15. Matej namaloval na rovinné plátno $n > 3$ přímek takových, že žádné dvě z nich nejsou rovnoběžné a průsečíkem každých dvou prochází i třetí přímka. Ukažte, že se pak všechny protínají v jednom bodě.

Příklad 16. Ostrava se dělí na obydlené a neobydlené části. Honzovi se zdálo, že spojíme-li úsečkou dvě obydlené části, bude tato úsečka obsahovat i neobydlenou část a naopak. Ukažte, že pak všechny části leží na přímce. Části vesnice považujeme za body a předpokládáme, že jich je konečně mnoho.

Úloha 17. Pomozte Majdě najít všechna kladná řešení dané soustavy rovnic:

$$x_1 + x_2 = x_3^2, \quad x_2 + x_3 = x_4^2,$$
$$x_3 + x_4 = x_1^2, \quad x_4 + x_1 = x_2^2.$$

Úloha 18. Lucka si do notýsku napsala kladná čísla taková, že součet součinů všech jejich dvojic byl roven jedné. Kačka se pak rozhodla, že ji trochu poškádlí a jedno číslo škrtne. Ukažte, že může škrtnout takové, aby součet zbylých čísel byl menší než $\sqrt{2}$.

Úloha 19. Klátra si vzala svých šest oblíbených kruhů a nakreslila je tak, aby se všechny protínaly v alespoň jednom společném bodě. Ukažte, že jeden z těchto kruhů obsahuje střed dalšího kruhu.

Literatura a zdroje

Tento příspěvek je téměř kopií příspěvku Martina Sýkory z jarního soustředění 2017, za což bych mu chtěl tímto poděkovat.

[1] Arthur Engel: *Problem-Solving Strategies*, Springer, 1997.

[2] Alča Skálová: *Extremální princip*, Blansko-Obůrka, 2011.

Apolloniova kružnice

Jáchym Solecký

Abstrakt. Tento příspěvek představuje Apolloniovu kružnici a její vlastnosti. Obsahuje pár úloh, které Apolloniovu kružnici využívají, a na konci uvádí některé další spojitosti s body v trojúhelníku.

Tvrzení. (Osa vnitřního úhlu) *Osa vnitřního úhlu u vrcholu A protíná protější stranu trojúhelníka ABC v bodě D tak, že platí*

$$\frac{|BD|}{|DC|} = \frac{|AB|}{|AC|}.$$

Tvrzení. (Osa vnějšího úhlu) *Je dán trojúhelník ABC takový, že $|AB| \neq |AC|$. Pak osa vnějšího úhlu u vrcholu A protíná přímku BC trojúhelníka ABC v bodě D tak, že platí*

$$\frac{|BD|}{|DC|} = \frac{|AB|}{|AC|}.$$

Úloha 1. V kartézské soustavě souřadnic jsou dány body $A = [5, 0]$ a $B = [20, 0]$. Najděte na přímce AB dva body, které jsou dvakrát blíže k A než k B. Zkuste najít další body mimo přímku AB. Dokázali byste je nějak popsat všechny?

Tvrzení. (Apolloniova kružnice) *V rovině jsou dány body A, B. Množina bodů X, pro které je poměr $|XA| : |XB|$ roven dané kladné konstantě $c \neq 1$ je kružnice se středem na přímce AB.*

Úloha 2. Body A, B, C jsou v tomto pořadí dány na přímce. Určete množinu bodů X, ze kterých jsou úsečky AB a BC vidět pod stejnými úhly.

Úloha 3. V rovině jsou dány čtyři různé body A, B, C, D neležící na stejné přímce. Sestrojte všechny body X, pro něž platí $\triangle ABX \sim \triangle CDX$.

Úloha 4. V rovině jsou dány čtyři různé body A, B, C, D ležící v tomto pořadí na jedné přímce. Sestrojte všechny body X, pro něž platí $|\sphericalangle AXB| = |\sphericalangle BXC| = |\sphericalangle CXD|$.

Úloha 5. Je dán trojúhelník ABC a dva různé body X, Y takové, že platí $|AX| : |BX| : |CX| = |AY| : |BY| : |CY|$. Dokažte, že přímka XY prochází středem O kružnice opsané trojúhelníka ABC.

Úloha 6. V rovině jsou dány body A, B, C neležící na jedné přímce. Zkonstruujte kružnici k procházející skrz body A, B takovou, že tečny z bodu C na ni svírají úhel $60°$.

Úloha 7. Na průměru kružnice k jsou dány body A, B. Vepište do kružnice k rovnoramenný trojúhelník tak, aby body A, B ležely na jeho různých ramenech.

Úloha 8. V rovině jsou dány dvě kružnice $k_1(S_1, r_1)$ a $k_2(S_2, r_2)$, kde $|S_1S_2| > r_1 + r_2$. Najděte množinu všech bodů X, které neleží na přímce S_1S_2 a mají tu vlastnost, že úsečky S_1X, S_2X protínají po řadě kružnice k_1, k_2 v bodech, jejichž vzdálenosti od přímky S_1S_2 se rovnají. (MO 63-A-II-2)

Úloha 9. V rovině je dána kružnice k a bod A mimo ni a její střed. Nechť A' je obraz bodu A přes kruhovou inverzi podle k. Ukažte, že kružnice k je Apolloniovou kružnicí kolem bodů A a A'.

Úloha 10. V rovině jsou dány body A, B, C neležící v přímce a je dána kladná konstanta $k \neq 1$. Nechť m je Apolloniova kružnice definovaná jako množina bodů X pro které $|XA| : |XB| = k$ a nechť n je kružnice opsaná trojúhelníku ABC. Označme T, U body, kde se m a n protínají. Dokažte, že tečny na m a n v bodě T, resp. U, jsou na sebe kolmé.

Úloha 11. (Izodynamické body) V rovině je dán trojúhelník ABC. Nechť k_a je Apolloniova kružnice kolem bodů B a C procházející bodem A, tj. množina bodů X takových, že $|XB| : |XC| = |AB| : |AC|$. Této kružnici se říká *A-Apolloniova kružnice*. Obdobně definujme k_b a k_c jako B-Apolloniovu kružnici a C-Apolloniovu kružnici. Ukažte, že k_a, k_b a k_c se potkávají ve dvou bodech.

Směs zajímavostí – Izodynamické body, Lemoinova a Brocardova přímka

Většinu těchto zajímavostí bohužel nejde snadno dokázat syntetickou geometrií a k důkazům se používají trilineární souřadnice, ale přijde mi pěkné ukázat, jak spolu všechno v trojúhelníku souvisí.

V poslední úloze jsme ukázali existenci tzv. *izodynamických bodů*. Označme je S a S'. Čím jsou tyto body zajímavé?

(1) Vzdálenosti od izodynamických bodů k jednotlivým vrcholům trojúhelníka jsou v inverzním poměru k délkám protilehlých stran, tj. $|SA| \cdot |BC| = |SB| \cdot |AC| = |SC| \cdot |AB|$ a $|S'A| \cdot |BC| = |S'B| \cdot |AC| = |S'C| \cdot |AB|$.

(2) Pokud z izodynamických bodů spustíme kolmice na jednotlivé strany trojúhelníku, dostaneme rovnostranný trojúhelník.

(3) Izodynamické body jsou si navzájem obrazem při kruhové inverzi podle kružnice opsané trojúhelníku ABC.

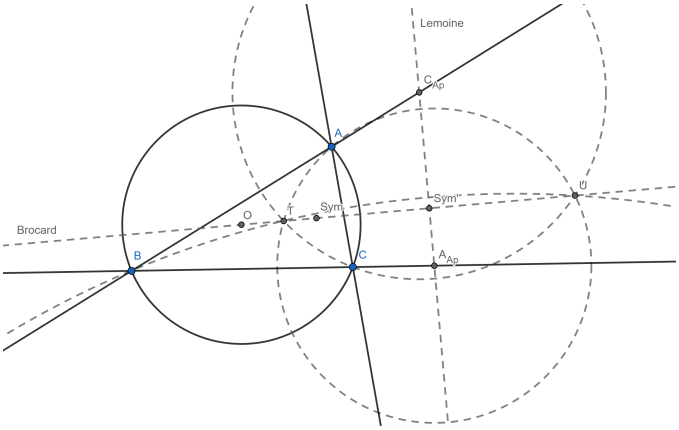
(4) Pokud pomocí kruhové inverze přes kružnici se středem v některém izodynamickém bodě převrátíme vrcholy A, B a C, dostaneme rovnostranný trojúhelník.

(5) Přímka, na které tyto body leží, se nazývá *Brocardova přímka*. Na této přímce leží kromě izodynamických bodů také střed kružnice opsané a Lemoinův bod (průsečík symedián trojúhelníka ABC).[1]

(6) Střed úsečky spojující oba izodynamické body je obrazem právě Lemoinova bodu při kruhové inverzi podle kružnice opsané trojúhelníku ABC.

(7) Protože se všechny Apolloniovy kružnice protínají v izodynamických bodech, jejich středy leží na jedné přímce. Tato přímka se nazývá *Lemoinova*, je kolmá na Brocardovu přímku a protíná ji v bodě popsaném výše.

(8) Izogonálními kamarády izodynamických bodů jsou tzv. *Fermatovy body*. Ty jsou zajímavé tím, že pokud z některého z nich povedeme přímky skrz vrcholy trojúhelníka ABC, tyto přímky budou svírat úhel 60°. To taky znamená, že ten Fermatův bod, který je uvnitř trojúhelníka ABC, je bodem s nejmenším součtem vzdáleností od vrcholů tohoto trojúhelníka.



Návody

2. Použijte tvrzení o ose vnitřního úhlu.

3. Známe poměr délek jedné dvojice odpovídajících si stran podobných trojúhelníků.

4. Použijte dvakrát úlohu 2.

5. Podívejte se na obrázek z pohledu bodů X a Y.

6. Zkonstruujte nejprve její střed O.

7. Čím bude v takovém trojúhelníku spojnice hlavního vrcholu se středem kružnice k?

[1] Pokud byste se o symediánách a Lemoinově bodu chtěli dozvědět více, doporučuji pročíst 3. díl seriálu z roku 2016/17 o Geometrii trojúhelníka (https://mks.mff.cuni.cz/archive/36/uvod3s.pdf).

8. Pokud jsou Y_1 a Y_2 body dotyku s kružnicemi k_1 a k_2, tak jsou trojúhelníky XS_1S_2 a XY_1Y_2 podobné.

9. Podívej se do Filipova příspěvku jak se definuje obraz bodu A.

10. Ukaž, že trojúhelníky OTA a OBT (kde O je střed kružnice m) jsou podobné.

11. Ukaž, že průsečík dvou těchto kružnic leží i na té třetí.

Zdroje a literatura

[1] Pavel Šalom, Pepa Tkadlec: Cèvova věta, seminář AoPS, 2014.

[2] Kimberling, Clark: Encyclopedia of Triangle Centers, http://faculty.evansville.edu/ck6/encyclopedia/ETC.html.

Náhodné procházky

Jáchym Solecký

Abstrakt. V tomto příspěvku se seznámíme s náhodnými procházkami a do detailů prozkoumáme příklad gamblerovy zkázy. Příspěvek je myšlen jako nadstavba na seriál z roku 2018/19 o pravděpodobnosti.

Motivace (a úlohy na procvičení ;))

Příklad 1. Kobylka skáče mezi vrcholy trojúhelníku, přičemž každým skokem přeskočí na jeden ze zbylých dvou vrcholů se stejnou pravděpodobností. Jaká je pravděpodobnost, že po n skocích bude kobylka na tom samém vrcholu, na kterém začala?

Příklad 2. Na řece mezi dvěma břehy leží 99 leknínů. Na 30. z nich (počítáno zleva) sedí žába, která každou minutu přeskočí na leknín doprava nebo doleva se stejnou pravděpodobností.

(1) Jaká je pravděpodobnost, že žába skočí na levý břeh řeky dřív, než skočí na pravý břeh?

(2) Jaká je střední hodnota počtu skoků, než žába na některý břeh skočí?

Příklad 3. Kolem kruhového jezera se nachází N měst označených od 0 do $N-1$. Turista, který se právě nachází ve městě 0, se každou hodinu přesune o město po směru nebo proti směru hodinových ručiček se stejnou pravděpodobností.

(1) Jaká je střední hodnota doby, za kterou turista projde všechny města na jezeře?

(2) Pro každé $k = 1, 2, \ldots, N-1$, jaká je pravděpodobnost, že město k je poslední turistou navštívené?

Příklad 4. (Gamblerova zkáza) Gambler opakovaně hraje hru, ve které vyhraje 1 korunu s pravděpodobností p a prohraje 1 korunu s pravděpodobností $q = 1 - p$ (nezávisle na ostatních hrách). Kasino opustí, když ztratí všechny peníze nebo bude mít M korun. Jaká je pravděpodobnost, že odejde s prázdnou, pokud má na začátku obnos n korun?

Všechny tyto úlohy jsou v principu stejné a představují příklady obecnější třídy náhodných procesů, kterým říkáme *náhodné procházky*[1]. Představme si blechu, která se náhodně pohybuje grafem. Při každém kroku (nebo skoku) se může posunout na některý jiný vrchol tohoto grafu, podle pravidel, které určují kam a s jakou pravděpodobností se z daného vrcholu může blecha posunout. Důležité je, že tato pravidla závisí pouze na tom, kde se blecha nachází právě teď, a nikoliv na jejích dřívějších pozicích.

Náhodné procházky pak můžeme použít k modelování mnoha situací z reálného světa, například pohybu částice v plynu nebo kapalině, cestě zvířete za jídlem nebo cenách na burze každé pondělí ráno. Na této přednášce se podrobně podíváme na příklad 4. – gamblerovu zkázu.

Pár definic na úvod

Definice. *Pravděpodobnostní prostor* je uspořádaná trojice $(\Omega, \mathcal{F}, \mathrm{P})$, kde Ω je množina elementárních jevů daného experimentu, $\mathcal{F}$ je množina jevů (tj. podmnožin Ω) a $\mathrm{P}\colon \mathcal{F} \to \langle 0, 1\rangle$ je funkce, která každému jevu přiřadí jeho pravděpodobnost.

Definice. Je dán pravděpodobnostní prostor $(\Omega, \mathcal{F}, \mathrm{P})$ a $A, B \in \mathcal{F}$ jsou jevy takové, že $\mathrm{P}(B) \neq 0$. *Podmíněnou pravděpodobnost* jevu A za podmínky, že nastal jev B, definujeme jako

$$\mathrm{P}(A|B) = \frac{\mathrm{P}(A \cap B)}{\mathrm{P}(B)}.$$

Věta. (O úplné pravděpodobnosti) *Je dán pravděpodobnostní prostor $(\Omega, \mathcal{F}, P)$ a disjunktní jevy $B_1, B_2, \ldots$ takové, že $B_1 \cup B_2 \cup \cdots = \Omega$ a $P(B_i) > 0$ pro všechna i. Potom pro libovolný jev A platí*

$$\begin{aligned} P(A) =& P(A \cap B_1) + P(A \cap B_2) + \cdots \\ =& P(B_1) \cdot P(A|B_1) + P(B_2) \cdot P(A|B_2) + \cdots . \end{aligned}$$

Této větě se také říká rozkladová věta, protože jevy B_i tvoří rozklad množiny Ω.

Definice. Mějme pravděpodobnostní prostor $(\Omega, \mathcal{F}, \mathrm{P})$. *Náhodná veličina* X na tomto prostoru je libovolná funkce z Ω do $\mathbb{R}$. Pak jev $\{\omega \in \Omega | X(\omega) = x\}$ značíme také $\{x = X\}$ a jeho pravděpodobnost $\mathrm{P}(X = x)$.

Definice. *Oborem hodnot* náhodné veličiny X myslíme množinu $\mathrm{Im}X = \{x \in \mathbb{R} | \mathrm{P}(X = x) > 0\}$[2].

Definice. Mějme náhodnou veličinu X definovanou pro prostor $(\Omega, \mathcal{F}, \mathrm{P})$. Potom *střední hodnotou* X myslíme výraz

$$\mathrm{E}(X) = \sum_{x \in \mathrm{Im}X} x \cdot \mathrm{P}(X = x).$$

[1] Občas taky celkem trefně používáme termín *opilcova procházka.*

[2] Označení Im pochází z anglického *image*.

Cvičení. Rozmyslete si, že pro konečnou množinu $\Omega = \{\omega_1, \omega_2, \ldots, \omega_n\}$ tato definice odpovídá definici v seriálu, tj. že

$$\mathrm{E}(X) = \mathrm{P}(\omega_1) \cdot X(\omega_1) + \mathrm{P}(\omega_2) \cdot X(\omega_2) + \cdots + \mathrm{P}(\omega_n) \cdot X(\omega_n).$$

Definice. Mějme náhodnou veličinu X definovanou pro prostor Ω. Potom *podmíněnou střední hodnotu* X za podmínky, že nastal jev B definujeme jako

$$\mathrm{E}(X|B) = \sum_{x \in \mathrm{Im}X} x \cdot \mathrm{P}(X = x|B).$$

Věta. (Rozkladová věta pro střední hodnotu) *Je dána náhodná veličina X definovaná pro prostor Ω a disjunktni jevy $B_1, B_2, \ldots$ takové, že $B_1 \cup B_2 \cup \cdots = \Omega$ (tj. tvořící rozklad prostoru Ω) a $P(B_i) > 0$ pro všechna i. Potom platí*

$$E(X) = E(X|B_1) \cdot P(B_1) + E(X|B_2) \cdot P(B_2) + \cdots .$$

Důkaz.

$$\begin{aligned}
\mathrm{E}(X) &= \sum_{x \in \mathrm{Im}X} x\mathrm{P}(X = x) \\
&= \sum_{x \in \mathrm{Im}X} x \left(\sum_i \mathrm{P}(X = x|B_i)\mathrm{P}(B_i) \right) \text{[dle věty o úplné pravděpodobnosti]} \\
&= \sum_{x \in \mathrm{Im}X} \sum_i x\mathrm{P}(X = x|B_i)\mathrm{P}(B_i) \\
&= \sum_i \mathrm{P}(B_i) \left(\sum_{x \in \mathrm{Im}X} x\mathrm{P}(X = x|B_i) \right) \\
&= \sum_i \mathrm{E}(X|B_i)\mathrm{P}(B_i).
\end{aligned}$$

Gamblerova zkáza

Příklad. Gambler opakovaně hraje hru, ve které vyhraje 1 korunu s pravděpodobností p a prohraje 1 korunu s pravděpodobností $q = 1 - p$ (nezávisle na ostatních hrách). Kasino opustí, když ztratí všechny peníze nebo bude mít M korun. Jaká je pravděpodobnost, že odejde s prázdnou, pokud má na začátku obnos n korun?

Označíme si tuto pravděpodobnost u_n a podle výsledků první hry můžeme díky větě o úplné pravděpodobnosti pozorovat:

$$\begin{aligned}
u_n = \mathrm{P}(\text{bankrot}|\text{výhra v 1. hře}) \cdot \mathrm{P}(\text{výhra v 1. hře}) + \\
+ \mathrm{P}(\text{bankrot}|\text{prohra v 1. hře}) \cdot \mathrm{P}(\text{prohra v 1. hře}).
\end{aligned}$$

Pokud gambler vyhraje první hru, tak díky *nezávislosti* jednotlivých her je nyní situace stejná jako kdyby gambler začínal s obnosem $\{n+1\}$ korun. Podobně pokud prohraje první hru, tak je to stejné jako kdyby začínal s obnosem $\{n-1\}$ korun. Z toho vyplývá, že

$$u_n = pu_{n+1} + qu_{n-1},$$

což platí pro $1 \leq n \leq M-1$. Zároveň máme také okrajové podmínky $u_0 = 1$ a $u_M = 0$.

Toto je příklad takzvaného rekurentního vztahu druhého stupně. Na konci této přednášky je nastíněný postup, kterým se takovéto vztahy řeší (je to velmi podobné např. diferenciálním rovnicím nebo rekurentním posloupnostem druhého stupně), ale to není hlavním předmětem této přednášky, takže my tento postup použijeme jen na náš vztah $pu_{n+1} - u_n + qu_{n-1} = 0$.

Charakteristická rovnice je v tomto případě

$$p\lambda^2 - \lambda + q = 0,$$

což se dá roznásobit na

$$(p\lambda - q)(\lambda - 1) = 0,$$

takže máme $\lambda = \frac{q}{p}$ nebo $\lambda = 1$.

Pokud $p \neq q$, tak

$$u_n = A + B\left(\frac{q}{p}\right)^n$$

pro nějaké konstanty A a B, které můžeme zjistit dosazením okrajových podmínek:

$$u_0 = 1 = A + B \quad \text{a} \quad u_M = 0 = A + B\left(\frac{q}{p}\right)^M,$$

což dává

$$A = -\frac{\left(\frac{1-p}{p}\right)^M}{1-\left(\frac{1-p}{p}\right)^M},\ B = \frac{1}{1-\left(\frac{1-p}{p}\right)^M}.$$

Takže

$$u_n = \frac{\left(\frac{1-p}{p}\right)^n - \left(\frac{1-p}{p}\right)^M}{1-\left(\frac{1-p}{p}\right)^M}.$$

Cvičení.[3] Zkontrolujte, že pro $p = q = \frac{1}{2}$ dostaneme

$$u_n = 1 - \frac{n}{M}.$$

[3]Toto je část (1) příkladu 2 v první kapitole.

Délka procházky

Příklad. Jaká je střední hodnota počtu her odehraných před tím, než gambler opustí kasino?

Stejně jako jsme použili rozkladovou větu pro sestavení rekurentního vztahu pro pravděpodobnost, použiijeme rozkladovou větu pro střední hodnotu k sestavení rekurentního vztahu pro očekávanou délku tohoto procesu.

Zavedeme si náhodnou veličinu X udávající počet kroků (v našem případě odehraných her) a označíme e_n střední hodnotu X, pokud gambler začínal s obnosem n korun. Pak platí

$$e_n = p \cdot \mathrm{E}(X|\text{výhra v 1. hře}) + q \cdot \mathrm{E}(X|\text{prohra v 1. hře}).$$

Zamysleme se teď nad podmíněnými středními hodnotamy v tomto výrazu. Pokud v první hře gambler vyhraje, pak *odehrál jednu hru* a následně je úloha stejná jako kdyby začal s obnosem $\{n+1\}$ korun. Takže dostaneme

$$\mathrm{E}(X|\text{výhra v 1. hře}) = 1 + e_{n+1}.$$

Podobně taky

$$\mathrm{E}(X|\text{prohra v 1. hře}) = 1 + e_{n-1}.$$

Takže dostaneme rekurentní výraz

$$e_n = p(1 + e_{n+1}) + q(1 + e_{n-1}),$$

který můžeme upravit na

$$pe_{n+1} - e_n + qe_{n-1} = -p - q = -1$$

s okrajovými podmínkami $e_0 = e_M = 0$. Všimněme si, že tento výraz je stejný, jako když jsme počítali pravděpodobnost, ale není homogenní. Obecné řešení homogenní rovnice je tedy stejné. Podíváme se na případ $p \neq q$, pro který:

$$w_n = A + B\left(\frac{q}{p}\right)^n$$

Jako partikulární řešení zkusme $v_n = Cn$ (zkoušet konstantu nemá smysl, protože každá konstanta je řešením homogenní rovnice), pak máme

$$pC(n+1) - Cn + qC(n-1) = -1,$$

takže $C = -1/(p-q)$. Dohromady dostáváme

$$e_n = A + B\left(\frac{q}{p}\right)^n - \frac{n}{p-q}.$$

Dosazením okrajových podmínek získáme

$$e_0 = 0 = A + B,\ e_M = 0 = A + B\left(\frac{q}{p}\right)^M - \frac{M}{p-q},$$

a po vyřešení pro A a B dostaneme výsledek

$$e_n = \frac{M}{p-q}\frac{1-(q/p)^n}{1-(q/p)^M} - \frac{n}{p-q}$$

pro $1 \leq n \leq M-1$.

Cvičení.[4] Najděte výraz pro střední hodnotu odehraných her v případě $p = q = \frac{1}{2}$.

Do nekonečna

Na závěr se podíváme, co se stane, když odebereme horní hranici na M. Uvažujeme tedy, že náš gambler opustí kasino jenom tehdy, když prohraje všechny své peníze. Nyní máme náhodnou procházku po celých číslech začínajíc na některém $n > 0$. Projde tato procházka nulou, anebo zůstane donekonečna v kladných číslech?

Matematicky můžeme odebrání této hranice docílit tak, že uvažujeme limitu pro M jdoucí do nekonečna. Pak dostaneme, že

$$u_n = \begin{cases} \lim\limits_{M\to\infty} \frac{\left(\frac{q}{p}\right)^n - \left(\frac{q}{p}\right)^M}{1-\left(\frac{q}{p}\right)^M}, & \text{pro } p \neq q \\ \lim\limits_{M\to\infty} 1 - \frac{n}{M}, & \text{pro } p = q = \frac{1}{2} \end{cases} = \begin{cases} \left(\frac{q}{p}\right)^n, & \text{pro } p > q. \\ 1, & \text{pro } p \leq q. \end{cases}$$

Po rigorózním zavedení pravděpodobnosti můžeme dokázat, že tato limita nám opravdu dá pravděpodobnost, že náhodná procházka po celých číslech projde nulou. To znamená, že procházka má nenulovou pravděpodobnost, že se udrží v kladných číslech, právě tehdy, když $p > q$.

Appendix: Rekurentní vztahy

Definice. *Rekurentní (nebo diferenční) vztah k-tého stupně* má tvar

$$\sum_{j=0}^{k} a_j u_{n+j} = f(n),$$

kde $a_0, \ldots, a_k$ jsou konstanty nezávislé na n a $a_0 \neq 0$ a $a_k \neq 0$. *Řešením* takového rekurentního vztahu je posloupnost $(u_n)_{n\geq 0}$ splňující vztah výše pro všechna $n \geq 0$.

[4] Toto je část (2) příkladu 2 v první kapitole.

Definice. Rekurentní vztah je homogenní, pokud $f(n) = 0$.

Při řešení rekurentních vztahů musíme nejprve najít obecné řešení $(w_n)_{n\geq 0}$ pro homogenní vztah

$$\sum_{j=0}^{k} a_j u_{n+j} = 0.$$

Pak najdeme jedno konkrétní, tzv. *partikulární*, řešení $(v_n)_{n\geq 0}$ našeho nehomogenního rekurentního vztahu a obecným řešením tohoto vztahu je pak posloupnost $u_n = v_n + w_n$.

Tvrzení. *Homogenní rekurentní vztah prvního stupně*

$$u_{n+1} = au_n$$

má obecné řešení tvaru

$$u_n = Aa^n,$$

kde A je konstanta.

Definice. Je dán homogenní rekurentní vztah druhého stupně $u_{n+1}+au_n+bu_{n-1} = 0$. Jeho *charakteristická rovnice* má tvar $\lambda^2 + a\lambda + b = 0$.

Tvrzení. *Je dán homogenní rekurentní vztah druhého stupně*

$$u_{n+1} + au_n + bu_{n-1} = 0.$$

Nechť λ_1, λ_2 jsou kořeny jeho charakteristické rovnice. Pokud $\lambda_1 \neq \lambda_2$, pak má obecné řešení tvar

$$u_n = A\lambda_1^n + B\lambda_2^n,$$

kde A, B jsou konstanty. Pokud $\lambda_1 = \lambda_2 = \lambda$, pak má obecné řešení tvar

$$u_n = (A + Bn)\lambda^n,$$

kde A, B jsou konstanty.

Pro hledání partikulárního řešení zkus postupně dosadit polynomy jednotlivých stupňů. Nejčastěji vyjde ten se stupněm o 1 vyšší, než jaké je obecné řešení homogenního vztahu.

Příklad. Najděte obecné řešení rekurentního vztahu

$$u_{n+1} - 2u_n + u_{n-1} = 1.$$

Řešení. Homogenní vztah je $u_{n+1} - 2u_n + u_{n-1} = 0$ s charakteristickou rovnicí $\lambda^2 - 2\lambda + 1 = 0$, která má jeden dvojitý kořen $\lambda = 1$. Takže obecné řešení homogenní rovnice má tvar

$$(A + Bn)1^n = A + Bn.$$

Z partikulárního řešení vidíme, že jakákoliv konstantní i lineární posloupnost je automaticky řešením homogenního vztahu, takže zkusíme kvadratickou posloupnost $v_n = Cn^2$. Dosazením dostaneme

$$C(n+1)^2 - 2Cn^2 + C(n-1)^2 = 1,$$

což dává $C = \frac{1}{2}$. Takže obecné řešení má tvar

$$A + Bn + \frac{1}{2}n^2.$$

Návody

1. Napiš si prvních pár pravděpodobností a zkus z toho vykoumat rekurentní vztah (a pak si ho odůvodnit :))

3.1. Jak vypadá množina navštívených měst těsně potom, co turista navštíví nové město?

3.2. Před tím, než turista navštíví město k, musí navštívit buď město $k-1$, nebo $k+1$. Co se muselo stát pak?

Literatura a zdroje

[1] James Martin: Prelims Probability. Oxford University Mathematical Institute, 2018.

[2] Danil Koževnikov, Václav Rozhoň: Pravděpodobnost, seriál MKS, 2018/19.

Asymetrické šifry

Michal Töpfer

Abstrakt. V dnešní době je naprosto normální, že se pomocí internetu přihlašujeme ke svému bankovnictví a uskutečňujeme platby. Málokdo ale ví, jak tyto věci opravdu fungují a jak je možné, že se k vašim datům, která bance posíláte, nedostane nikdo cizí. Za tím vším stojí matematika, konkrétně počítaní s 600 a více cifernými čísly. V tomto příspěvku se nejprve podíváme na obecný úvod do kryptografie a pak se zaměříme na protokol RSA a teorii čísel, která za ním stojí.

Kryptografická primitiva

Představte si následující situaci: Alice chce Bobovi posílat zprávy. Jenže všechny zprávy, které Alice pošle, si cestou může přečíst i Eva. Jak to Alice může zařídit, aby Bob její zprávy přečetl, ale Eva se nedozvěděla nic o tom, co se v nich píše?

Alice bude zprávy šifrovat. Pořídí si tedy nějaké krabičky E a D.[1] Krabička E udělá z původní zprávy zašifrovaný tex. Krabička D naopak ze zašifrovaného textu vyrobí původní zprávu. Protože dobrých šifrovacích algoritmů je málo, je vhodné je parametrizovat *klíčem*. Obecně je dobré uchovávat v tajnosti co nejméně informací, ideálně takové, které se dají snadno změnit.

Symetrické šifry

Symetrické šifry využívají pro šifrování i dešifrování stejný klíč. Je proto potřeba si tento klíč předat ještě před začátkem komunikace nějakou jinou cestou. Podstatnou výhodou symetrických šifer je jejich nízká výpočetní náročnost.

Jednoduchým příkladem symetrické šifry je Caesarova šifra. Její hlavní princip spočívá v tom, že každé písmeno zprávy posuneme o pevný počet pozic v abecedě. Tato šifra samozřejmě není příliš bezpečná, protože je velmi snadné zkusit všech 26 možných posunů a jedním z nich zprávu dešifrovat.

[1] Písmena jsou odvozena z anglických termínů *Encrypt* a *Decrypt*.

Asymetrické šifry

Pro asymetrické šifry platí, že využívají různé klíče pro šifrování a dešifrování. Šifrovací klíč je typicky veřejný, takže zprávy může zašifrovat kdokoliv. Naopak dešifrovací klíč si držíme v tajnosti, abychom zprávy mohli dešifrovat jen my. Všimněte si, že tímto odpadá nutnost znalosti společného tajemství pro posílání zpráv. Důležité je, aby z jednoho klíče nešlo efektivně odvodit druhý.

Asymetrické šifry se dají využít i opačně, čímž vznikne podpisové schéma. Jeho cílem není zašifrovat zprávu, aby si ji útočník nemohl přečíst, ale zařídit, aby ji cestou nemohl změnit. Představte si například, že Alice chce Bobovi poslat plán nějaké akce. Chceme zajistit, aby Bob dostal plán přesně v takové podobě, v jaké ho Alice poslala, a aby Eva plán nemohla po cestě nějak upravit. Alice proto zprávu s plánem *podepíše*. Podpis je odvozený ze zprávy, takže pokud by ji Eva nějak změnila, tak podpis nebude odpovídat. Bob tedy dokáže ověřit, jestli dostal původní zprávu beze změny.

Pro podpisové schéma budeme mít dešifrovací klíč veřejný a šifrovací soukromý. Potom můžeme soukromým klíčem zašifrovat zprávu a zveřejnit ji. Každý může zprávu dešifrovat a tím ověřit, že jsme ji opravdu zašifrovali my. Nikdo jiný než Alice nezná její soukromý klíč, takže nedokáže zprávu podepsat jejím jménem.

Hešovací funkce

Hešovací funkce umí z libovolného vstupu vytvořit výstup konstantní délky. Důležité je, aby z heše nešlo efektivně zjistit původní zprávu a ani najít zprávu, která bude mít stejný heš. Kolizím (zprávám se stejným hešem) nejde zabránit, neboť počet možných výstupů je omezený a počet vstupů není, ale důležité je, aby nebylo snadné je hledat.

Pojďme se podívat na konkrétní příklad velmi jednoduché hešovací funkce: poslední číslice ciferného součtu čísla. Z libovolně velkého čísla na vstupu nám jako heš vyjde vždy jedna číslice. Je vidět, že z heše není možné původní hodnotu čísla zrekonstruovat. Nicméně tato hešovací funkce je špatná, protože hledat kolize je snadné. Zkuste si nějaké sami najít.

Využít je můžeme k vylepšení podpisového schématu: Místo zprávy podepíšeme její heš a připojíme ho k původní zprávě. Jednak tím celý proces podepisování zrychlíme, protože počítání heše je (z bezpečnostních důvodů popsaných níže) daleko rychlejší než asymetrické šifrování, a jednak nebudeme muset řešit, jak celou zprávu rozdělit na dostatečně malé části, aby je asymetrická šifra zvládla. Navíc je pak možné původní zprávu přečíst i bez nutnosti dešifrování.

Kombinace primitiv

Ještě zmíníme, jak se dají kryptografická primitiva kombinovat. Poměrně časté je spojení symetrického a asymetrického šifrování. Symetrické šifry mají tu výhodu, že jsou mnohem méně náročné na výpočetní výkon než asymetrické. Asymetrické zase

tu, že nepotřebují předem dohodnutý tajný klíč, který by znaly obě strany. Dá se tedy udělat to, že pomocí asymetrické šifry si přeneseme klíč, který pak využijeme pro šifrování a dešifrování zpráv symetrickou šifrou. Přenesení klíče nezabere tolik času, protože jeho délka je obvykle výrazně menší než délka zprávy.

Samozřejmě je také časté kombinovat šifrování a podepisování. Tím si zajistíme jednak to, že naše zprávy si nikdo nemůže přečíst, a jednak to, že si dokážeme po přijetí ověřit, že je nikdo cestou nezměnil. Tady je důležité používat pro šifrování a podepisování různé klíče, jinak si vystavujeme velkému riziku jejich prolomení.

Cvičení

Příklad 1. Alice a Bob jsou ubytováni ve stejném hotelu v oddělených místnostech, které nemohou opustit. Jediná možnost, jak si mohou něco předat, je pomocí poslíčka Evy. Bob chce poslat Alici prstýnek, ale bojí se, že by ho Eva mohla ukrást. Oba milenci mají na svých pokojích několik trezorů, visacích zámků a odpovídajících klíčů. Zamčené trezory můžeme považovat za nedobytné a navíc víme, že Eva celé trezory nekrade. Jak to mají udělat, aby se prstýnek bezpečně dostal k Alici?

Teorie čísel a konstrukce asymetrických šifer

V této části přednášky si povíme něco o protokolu RSA. K jeho vybudování ale nejprve potřebujeme pár poznatků o dělitelnosti a prvočíslech.

Definice. *Největší společný dělitel* čísel m a n značíme $\gcd(m, n)$.
Pokud $\gcd(m, n) = 1$, řekneme, že čísla m a n jsou *nesoudělná*.

Definice. Nechť m je přirozené číslo. Jestliže dvě celá čísla a, b splňují $m \mid a - b$, pak říkáme, že a a b jsou *kongruentní modulo* m, což zapisujeme takto:

$$a \equiv b \pmod{m}.$$

Pokud jsou dvě čísla kongruentní modulo m, tak to znamená, že dávají stejný zbytek po dělení číslem m. Speciálně $m \mid a$ můžeme zapisovat jako $a \equiv 0 \pmod{m}$. S kongruencemi se dá až na výjimky pracovat stejně jako s normálními rovnicemi.

Věta. (Malá Fermatova) *Mějme prvočíslo p a a takové, že $p \nmid a$. Pak*

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

Důkaz. Uvažme množiny

$$A = \{1, 2, \ldots, p-1\},$$
$$B = \{1a, 2a, \ldots, (p-1)a\},$$

přičemž v množině B počítáme čísla modulo p. Protože $p \nmid a$ a pro žádné $b \in \{1, 2, \ldots, p-1\}$ neplatí $p \mid b$, tak ani $b \cdot a \not\equiv 0 \pmod{p}$, a tedy žádný prvek množiny B není 0.

Sporem ukážeme, že žádné dva prvky množiny B nejsou shodné. Předpokládejme $ax \equiv ay \pmod{p}$ pro nějaká $x, y \in \{1, 2, \ldots, p-1\}, x \neq y$. To znamená $p \mid a(x-y)$. Ale $p \nmid a$ a také zřejmě $x - y \not\equiv 0 \pmod{p}$.

Množiny tedy nutně obsahují právě stejné hodnoty, a proto i součin jejich hodnot je stejný:

$$1 \cdot 2 \cdot \ldots \cdot p-1 \equiv 1a \cdot 2a \cdot \ldots \cdot (p-1)a \pmod{p}.$$

Zkrácením rovnosti postupně čísly 1 až $p-1$ dostáváme požadovanou vlastnost: $1 \equiv a^{p-1} \pmod{p}$. □

Definice. (Eulerova funkce) *Eulerova funkce* $\varphi(n)$ je definovaná jako počet přirozených čísel k takových, že $1 \leq k \leq n$ a zároveň $\gcd(k, n) = 1$ (čísla jsou nesoudělná).

Cvičení 2. Rozmyslete si, že

(i) $\varphi(1) = 1$,
(ii) pro p prvočíslo je $\varphi(p) = p - 1$,
(iii) pro p prvočíslo a $m \in \mathbb{N}$ je $\varphi(p^m) = (p-1) \cdot p^{m-1}$,
(iv) pro n, m nesoudělná platí $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

RSA

Jednou z nejznámějších a nejpoužívanějších asymetrických šifer je protokol RSA. Je pojmenovaný po svých autorech, kteří ho v roce 1978 publikovali. Byli to pánové Ronald Rivest, Adi Shamir a Leonard Adleman.

Základní myšlenka je poměrně jednoduchá. Protokol využívá toho, že násobit dokážeme velmi rychle, ale pro opačný postup, tedy rozklad čísla na prvočinitele, není známý žádný efektivní algoritmus. Pokud máme zadaná čísla n a e, tak je velmi jednoduché spočítat pro m hodnotu $m^e \pmod{n}$. Ale udělat to naopak vůbec není snadné. Pokud ovšem neznáme prvočíselný rozklad čísla n. Pokud ho známe, pak můžeme hodnotu m z $m^e \pmod{n}$ najít poměrně snadno, jak si za chvíli ukážeme.

Formální zavedení RSA

Generování klíče

Nejprve si musíme zvolit délku klíče. V současné době se nejčastěji používají hodnoty $b = 2048$ nebo $b = 4096$.

(1) Zvolíme si (náhodně vygenerujeme) dvě velká prvočísla p a q (každé s $b/2$ ciframi).
(2) Spočítáme jejich součin $n = p \cdot q$.
(3) Spočítáme hodnotu Eulerovy funkce $\varphi(n) = (p-1)(q-1)$.

(4) Zvolíme číslo e menší než $\varphi(n)$ a nesoudělné s $\varphi(n)$.

(5) Najdeme číslo d, pro které platí $ed \equiv 1 \pmod{\varphi(n)}$.

Veřejným klíčem je dvojice $P = (n, e)$.

Soukromým klíčem je dvojice $S = (n, d)$.

V pátém bodě využijeme rozšířený Eukleidův algoritmus na hodnoty $\varphi(n)$ a e (kterým současně ověříme nesoudělnost požadovanou v bodě 4).

Algoritmus. (Rozšířený Eukleidův algoritmus)
Pro daná dvě čísla a, b nalezneme $\gcd(a, b)$ a také koeficienty x a y, pro které platí $ax + by = \gcd(a, b)$.[2]

Budeme postupně počítat členy posloupností $\{q_i\}$, $\{r_i\}$, $\{s_i\}$ a $\{t_i\}$, přičemž chceme zachovat platnost vztahu $r_i = s_i a + t_i b$.

Nastavíme $r_0 = a$, $r_1 = b$. Z toho nutně plyne $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, $t_1 = 1$.

Další členy definujeme rekurzivně:

$$\begin{aligned} q_i &= r_{i-2}/r_{i-1} \qquad \text{(celočíselné dělení)}, \\ r_i &= r_{i-2} - r_{i-1} \cdot q_i, \\ s_i &= s_{i-2} - s_{i-1} \cdot q_i, \\ t_i &= t_{i-2} - t_{i-1} \cdot q_i. \end{aligned}$$

Tento postup opakujeme, dokud $r_i \neq 0$. Ve chvíli, kdy $r_i = 0$, máme výsledek

$$\gcd(a, b) = r_{i-1} = s_{i-1} a + t_{i-1} b.$$

Podrobnější rozbor algoritmu naleznete například v [4].

V pátém bodě tedy aplikujeme rozšířený Eukleidův algoritmus na hodnoty $\varphi(n)$ a e, čímž dostaneme $\gcd(\varphi(n), e) = 1 = s_{i-1} \cdot \varphi(n) + t_{i-1} \cdot e \equiv t_{i-1} \cdot e \pmod{\varphi(n)}$. Vezmeme $d \equiv t_{i-1} \pmod{\varphi(n)}$.

Šifrování

$E_P(m) = m^e \pmod{n}$.

Dešifrování

$D_S(c) = c^d \pmod{n}$.

Příklad 3. Jistě jste si všimli, že v tuto chvíli můžeme jako zprávy posílat pouze celá čísla z rozsahu 0 až $n-1$. Jak to zařídit, abychom mohli posílat libovolné textové zprávy?

[2] Tato identita je známá jako Bézoutova rovnost.

Důkaz správnosti

Chceme ověřit, že $D_S\left(E_P(m)\right) = m$. Umíme posílat jen zprávy kratší než n, takže stačí pracovat modulo n. Víme, že

$$D_S\left(E_P(m)\right) = D_S(m^e) = m^{ed} \pmod{n}.$$

Z toho, jak jsme generovali klíč, máme $ed \equiv 1 \pmod{\varphi(n)}$, tedy existuje nějaké $k \in \mathbb{Z}$ tak, že $ed = 1 + k \cdot (p-1)(q-1)$. To můžeme dosadit:

$$m^{ed} = m \cdot m^{k(p-1)(q-1)} = m \cdot \left(m^{p-1}\right)^{k(q-1)}.$$

Pokud $p \nmid m$, můžeme použít Malou Fermatovu větu:

$$m^{p-1} \equiv 1 \pmod{p},$$
$$m^{ed} = m \cdot \left(m^{p-1}\right)^{k(q-1)} \equiv m \cdot (1)^{k(q-1)} \equiv m \pmod{p}.$$

V opačném případě dostaneme triviálně stejný výsledek: $m^{ed} \equiv 0 \equiv m \pmod{p}$.

Obdobně postupujeme i pro q:

$$m^{ed} = m \cdot m^{k(p-1)(q-1)} = m \cdot \left(m^{q-1}\right)^{k(p-1)} \equiv m \pmod{q}.$$

Nyní máme $p \mid m^{ed} - m$ a $q \mid m^{ed} - m$, z čehož nutně i $pq \mid m^{ed} - m$, protože p a q jsou nesoudělná. Tedy

$$m^{ed} \equiv m \pmod{pq}.$$

□

Ukázka použití

Nejprve si vygenerujeme klíče:

(1) $p = 5$, $q = 11$.
(2) $n = 5 \cdot 11 = 55$.
(3) $\varphi(55) = (5-1)(11-1) = 40$.
(4) $e = 3$.
(5) $\gcd(40, 3) = 1 = 1 \cdot 40 - 13 \cdot 3 \equiv -13 \cdot 3 \pmod{40}$, tedy $d = -13 \equiv 27$.

Jako veřejný klíč tedy zveřejníme dvojici $(55, 3)$ a sami si tajně uschováme soukromý klíč $(55, 27)$.

Řekněme, že nám chce někdo jako zprávu poslat číslo 18. Stačí, aby spočítal hodnotu $E_{(55,3)}(18) = 18^3 \pmod{55} = 2$. Tím zprávu zašifroval a může nám ji poslat.

My dostaneme číslo 2 a chceme z něj dešifrovat původní zprávu. To uděláme snadno: $D_{(55,27)}(2) = 2^{27} \pmod{55} = 18$. Tím jsme skutečně dostali původní zprávu a zároveň si ji cestou nikdo jiný nemohl přečíst.[3]

[3] No ...

Cvičení

Předpokládejte, že můj veřejný klíč je $(629, 17)$ a že pro kódování zpráv používám ASCII (tedy například písmena A až Z se kódují postupně na 65 až 90 a mezera se kóduje na 32).

Příklad 4. Zašifrujte zprávu „MKS“ (po písmenech).

Příklad 5. Zachytili jste zašifrovanou zprávu:

$$247, 337, 322, 463, 15, 73, 440, 15, 342, 323, 435.$$

Zkuste ji rozluštit.

Bezpečnost RSA a možné útoky

Obecně je algoritmus RSA při použití dostatečně velkého klíče považován za bezpečný. V dnešní době je vhodné používat **minimálně** 2048-bitové klíče. Bezpečnost algoritmu je založena na tom, že pro rozklad čísel na prvočinitele není známý žádný efektivní algoritmus.

Nicméně pokud je algoritmus použit špatně, existuje hned několik možností, jak ho prolomit. Zde zmíníme jen některé z nich:

(1) Pokud je použita nízká hodnota e a nízká hodnota m, může se stát, že výsledek m^e je menší než n. Pak je dešifrování snadné, protože stačí vzít e-tou odmocninu ze zašifrovaného textu.

(2) RSA je deterministická šifra, takže útočník může zkusit šifrovat pravděpodobné zprávy a porovnávat je se zašifrovaným textem. Také to znamená, že stejné zprávy se zašifrují stejně, takže útočník může poznat, že se zpráva opakuje.

(3) Platí, že součin zašifrovaných textů je roven zašifrování součinu původních zpráv: $m_1^e \cdot m_2^e \equiv (m_1 m_2)^e \pmod{n}$. Je tedy možné provést útok s výběrem původního textu. Pokud chceme rozluštit zprávu $c = m^e \pmod{n}$, můžeme adresáta požádat o dešifrování nevinně vypadající zprávy $f = cr^e \pmod{n}$ pro námi vybrané r. Dešifrování zprávy f je potom $mr \pmod{n}$, z čehož už zjistíme i m. Tento typ útoku se zdá na první pohled úplně nereálný, nicméně RSA se používá i pro podepisování zpráv, takže můžeme oběti zkusit podstrčit k podepsání námi vybranou zprávu. Proto byste nikdy neměli používat stejný klíč pro šifrování a podepisování!

(4) Pokud je stejná zpráva zašifrována pomocí e nebo více veřejných klíčů se stejným e, je možné ji rozluštit pomocí Čínské zbytkové věty.

Většině z těchto útoků dokážeme zabránit pomocí *paddingu*. Původní zprávu před zašifrováním doplníme nějakými náhodnými bity, takže třeba dvě stejné původní zprávy dostanou různý padding, a tedy se nezašifrují stejně. Paddingové schéma může vypadat třeba takto: `00 02 NAHODNE 00 ZPRAVA`. Dvojka před náhodnými

bity nám zajistí to, že budeme vždy šifrovat dostatečně velké číslo. Počet náhodných bitů můžeme volit tak, abychom délku celé zprávy zarovnali na námi požadovanou hodnotu.

Návody

4. Mělo by vám vyjít 247, 75, 440. Pro počítání hodnot použijte Wolfram Alpha.

5. $629 = 17 \cdot 37$. Pak postupujte jako při generování klíče a následně dešifrujte.

Literatura a zdroje

[1] Andrew D. Ker: *Computer Security*, Department of Computer Science, Oxford University, 2014.

[2] Dan Yasaki: *RSA Exercises*, The University of North Carolina at Greensboro.

[3] Filip Hlásek: *Komunikace přes nezabezpečený kanál*, Sklené, 2015.

[4] Brilliant: *Extended Euclidean Algorithm*, *https://brilliant.org/wiki/extended-euclidean-algorithm/*

[5] Wikipedia: *RSA (cryptosystem)*, *https://en.wikipedia.org/wiki/RSA_(cryptosystem)*

Fourierova transformace

Michal Töpfer

Abstrakt. Zajímalo vás někdy, jak funguje komprese zvuku a obrazu ve formátech MP3 a JPEG? Na pozadí se skrývá poměrně zajímavá matematická struktura zvaná Fourierova transformace. V tomto příspěvku se podíváme na to, co to Fourierova transformace je a jak ji (rychle) spočítat.

Připomenutí komplexních čísel

Definice. Množinou *komplexních čísel* rozumíme $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$.

Sčítání a násobení zavedeme přirozeně, přičemž využijeme $i^2 = -1$.

Definice. (Komplexně sdružené číslo) Pro $z = a+bi$ zavedeme *komplexně sdružené* číslo $\overline{z} = a - bi$.

Definice. (Absolutní hodnota) $|x| = \sqrt{x \cdot \overline{x}}$, tedy $|a + bi| = \sqrt{a^2 + b^2}$.

Definice. (Goniometrický tvar) $x = |x| \cdot (\cos\varphi + i \sin\varphi)$, pro nějaké $\varphi \in \langle 0, 2\pi)$.

Tvrzení. (Eulerova formule) $e^{i\varphi} = \cos\varphi + i \sin\varphi$.

Pošimněme si, že pokud necháme úhel φ běžet od 0 do 2π, pohybujeme se proti směru hodinových ručiček po jednotkové kružnici.

Odmocniny z jedničky

Odmocňování v komplexních číslech není jednoznačné. Vezměme například rovnici $x^4 = 1$, která má čtyři řešení: 1, -1, i, $-i$.

Podívejme se podrobněji na kořeny rovnice $x^n = 1$. Platí $|x^n| = |x|^n$, tedy nutně $|x| = 1$. Díky tomu víme $x = e^{i\varphi}$ pro nějaké φ. Nyní si rovnici zapíšeme v goniometrickém tvaru:

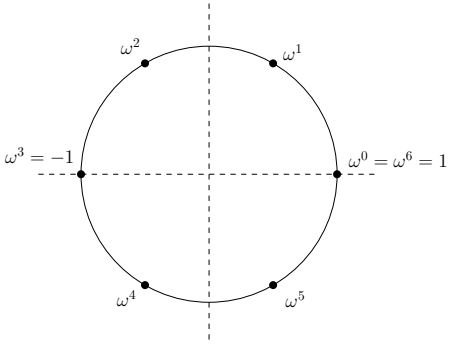
$$1 = x^n = e^{i\varphi n} = \cos\varphi n + i \sin\varphi n.$$

To platí pro $\cos\varphi n = 1$, tedy $\varphi n = 2k\pi$, kde $k \in \mathbb{Z}$.

Celkem dostáváme n různých n-tých odmocnin z jedné. Konkrétně

$$e^{\frac{2k\pi i}{n}} \text{ pro } k = 0, 1, \ldots, n-1.$$

Pokud řešení zakreslíme do Gaussovy roviny, tyto body tvoří vrcholy pravidelného n-úhelníku:



Definice. Komplexní číslo ω je *primitivní* n-tá odmocnina z 1, pokud $\omega^n = 1$ a žádné z čísel $\omega^1, \omega^2, \ldots, \omega^{n-1}$ není rovno 1.

Příklad 1. Které ze čtyř výše zmíněných odmocnin z 1 jsou primitivní?

Pro obecné $n > 2$ vždy existují alespoň dvě primitivní odmocniny z 1, konkrétně čísla $\omega = e^{i2\pi/n}$ a $\overline{\omega} = e^{-i2\pi/n}$. Platí totiž $\omega^j = e^{i2\pi j/n}$.

Úmluva. Ve zbytku textu budeme předpokládat, že ω je nějaká pevně zvolená primitivní n-tá odmocnina z 1.

Příklad 2. Rozmyslete si, že $\omega^j \neq \omega^k$ pro $0 \leq j < k < n$.

Příklad 3. Ukažte, že pro sudá n platí $\omega^{\frac{n}{2}} = -1$.

Diskrétní Fourierova transformace

Úmluva. Předpokládejme, že n je mocnina dvojky.

Úmluva. Pokud není uvedeno jinak, vektory mají n složek.

Definice. *Diskrétní Fourierova transformace (DFT)* je zobrazení $\mathcal{F} : \mathbb{C}^n \to \mathbb{C}^n$, které vektoru $\vec{x}$ přiřadí vektor $\vec{y}$ daný předpisem

$$y_j = \sum_{k=0}^{n-1} x_k \cdot \omega^{jk}.$$

Všimněme si, že tato definice přesně odpovídá maticovému násobení (je to lineární zobrazení). Pro ω primitivní n-tou odmocninu z 1 definujme matici Ω takto: $\Omega_{j,k} = \omega^{jk}$ (indexujeme od 0). Pak

$$\mathcal{F}(\vec{x}) = \Omega \cdot \vec{x}.$$

Toho využijeme při hledání inverzní Fourierovy transformace. Stačí najít inverzní matici k Ω. K tomu využijeme matici $\overline{\Omega}$, která vznikne stejně jako Ω, pouze s použitím $\overline{\omega}$ (tato matice obsahuje komplexně sdružená čísla k prvkům Ω).

Příklad 4. Ukažte, že $\frac{1}{n}\overline{\Omega}$ je inverzní maticí k Ω.

Příklad 5. Spočítejte Fourierovy obrazy následujících vektorů z $\mathbb{C}^n$:

a) $(x, \dots, x)$,

b) $(1, -1, 1, -1, ..., 1, -1)$,

c) $(2, 0, 2, 0, 2, 0, 2, 0)$,

d) $(\omega^0, \omega^1, \omega^2, \dots, \omega^{n-1})$,

e) $(\omega^0, \omega^2, \omega^4, \dots, \omega^{2n-2})$.

Příklad 6. Najděte pro každé j vektor, jehož Fourierův obraz má na j-tém místě jedničku a všude jinde nuly.

Odbočka ke spojité Fourierově transformaci

Fourierova transformace se dá zavést i spojitě, stačí místo sumy uvažovat integrál. DFT pak odpovídá tomu, že si poznamenáme hodnoty funkce jen v některých bodech a s nimi pak pracujeme. Následující definici uvádím spíše pro úplnost. d

Definice. Nechť $f : \mathbb{R} \to \mathbb{C}$ je integrovatelná funkce. Pak *Fourierova transformace funkce* f je

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \xi} dx,$$

pro libovolné reálné ξ.

Pro lepší pochopení toho, co Fourierova transformace znamená je dobré podívat se na izualizaci, kterou najdete na stránce *http://michal.topfer.matfyz.cz/fourier*. Uvnitř integrálu máme dva členy. Člen $e^{-2\pi i x \xi}$ zajišťuje pohyb po jednotkové kružnici po směru hodinových ručiček. To je tím, že argument tohoto komplexního čísla obsauje hodnotu x, podle které integrujeme, takže běží od mínus nekonečna do nekonečna. První člen v integrálu zajistí to, že vzdálenost od nuly odpovídá velikosti funkční hodnoty v příslušném bodě. Celkově si to tedy můžeme představit jako namotávání funkce dokola kolem počátku.

Následně nás zajímá, kde má tento namotaný graf těžiště. Jeho reálná a imaginární souřadnice je právě hodnotou Fourierovy transformace pro zadanou hodnotu ξ. V definici tedy ξ odpovídá frekvenci „namotávání“ a x je definiční obor původní funkce (čas).

Využití DFT

Fourierova transformace má poměrně široké uplatnění. Fyzikálně totiž odpovídá spektrálnímu rozkladu signálu na siny a cosiny o různých frekvencích.

Na tom jsou založeny například algoritmy pro filtrování zvuku. A souvisí s tím i komprese zvuku (MP3) a obrazu (JPEG). Zvuk se ukládá s nějakou vzorkovací frekvencí, pak se rozdělí na bloky (po řádově 1000 vzorcích). Na blok se aplikuje DFT a koeficienty se uloží s požadovanou přesností (různá přesnost pro různé frekvence – lidské ucho nevnímá všechny frekvence stejně). Při přehrávání se použije IFT, čímž dostaneme zvuk, který je velmi podobný tomu původnímu.

Dalším použitím je rychlé násobení polynomů, ale k tomu si nejdřív budeme muset ukázat, jak ji spočítat rychle.

Násobení polynomů

Definice. *Polynom* je výraz typu

$$P(x) = \sum_{i=0}^{n-1} p_i \cdot x^i,$$

kde x je proměnná a p_0 až p_{n-1} jsou *koeficienty* polynomu. Vektoru $(p_0, \ldots, p_{n-1})$ budeme říkat *vektor koeficientů*.

Definice. *Stupněm* polynomu nazveme nejvyšší mocninu s nenulovým koeficientem.

Všimněte si, že doplněním koeficientů p_n a vyšších nulami se hodnota polynomu nezmění.

Podívejme se nyní, jak se polynomy násobí.

$$R(x) = P(x) \cdot Q(x) = \left(\sum_{i=0}^{n-1} p_i \cdot x^i\right) \cdot \left(\sum_{j=0}^{n-1} q_j \cdot x^j\right) = \sum_{i,j} p_i q_j x^{i+j},$$

tedy koeficient $r_k = \sum_{i=0}^{k} p_i q_{k-i}$.

Pokud bychom polynomy násobili podle této definice, potřebujeme na to $\mathcal{O}(n^2)$ kroků.

Jiný pohled na polynomy

Rozmyslíme si, kdy polynomy považujeme za stejné. Můžeme se na ně dívat jako na výrazy. Pak o nich řekneme, že jsou *identické*, pokud mají po normalizaci stejné vektory koeficientů.

Druhá možnost je dívat se na polynomy jako na funkce. Polynomy P a Q jsou si rovny právě tehdy, když $\forall x \in \mathbb{R} : P(x) = Q(x)$. Identické polynomy jsou si rovné i jako funkce a platí to i naopak:

Věta. *Buďte P a Q polynomy stupně nejvýše d. Pokud platí $P(x_i) = Q(x_i)$ pro navzájem různá čísla $x_0, \dots, x_d$, pak P a Q jsou identické.*

Díky této větě můžeme polynom reprezentovat také pomocí vektoru funkčních hodnot, této reprezentaci říkáme *graf polynomu*. Pokud máme alespoň $\deg P + 1$ bodů, je polynom P grafem určen jednoznačně.

V grafové reprezentaci je násobení polynomů triviální: součin polynomů P a Q má v bodě x hodnotu $P(x) \cdot Q(x)$. Stačí tedy grafy vynásobit po složkách.

Pro převod do grafové reprezentace využijeme Fourierovu transformaci. Označme $\vec{p}$ vektor koeficientů polynomu P. Pak jeho Fourierova transformace $\mathcal{F}(\vec{p})$ je grafem tohoto polynomu v bodech $\omega^0, \dots, \omega^{n-1}$. Zbývá tedy ukázat, jak počítat Fourierovu transformaci efektivně.

Příklad 7. Pomocí Fourierovy transformace spočtěte součin polynomů $P(x) = x + 1$ a $Q(x) = 2x^2 + 1$.

Rychlá Fourierova transformace (FFT)

Pro výpočet využijeme metodu *Rozděl a panuj*. Budeme vyhodnocovat polynom P v n bodech, které si zvolíme tak, aby byly *spárované*, tedy aby tvořily dvojice lišící se znaménkem:

$$\pm x_0, \pm x_1, \dots, \pm x_{\frac{n}{2}-1}.$$

Polynom P pak můžeme rozložit na členy se sudým a lichým exponentem:

$$P(x) = (p_0 x^0 + p_2 x^2 + \cdots + p_{n-2} x^{n-2}) + (p_1 x^1 + p_3 x^3 + \cdots + p_{n-1} x^{n-1}).$$

A z druhé závorky vytkneme x:

$$P(x) = (p_0 x^0 + p_2 x^2 + \cdots + p_{n-2} x^{n-2}) + x \cdot (p_1 x^0 + p_3 x^2 + \cdots + p_{n-1} x^{n-2}).$$

Tím máme v obou závorkách pouze sudé mocniny, a tedy můžeme každou z nich považovat za vyhodnocení polynomu velikosti $n/2$ v bodě x^2:

$$P(x) = P_s(x^2) + x \cdot P_l(x^2),$$

kde P_s a P_l jsou polynomy se sudými a lichými koeficienty P. Navíc také snadno vypočteme hodnotu v bodě $-x$:

$$P(-x) = P_s(x^2) - x \cdot P_l(x^2).$$

Tím jsme vyhodnocení polynomu P v bodech $\pm x_0, \pm x_1, \dots, \pm x_{\frac{n}{2}-1}$ převedli na vyhodnocení dvou polynomů poloviční velikosti v bodech $x_0^2, x_1^2, \dots, x_{n/2-1}^2$. Toto vyhodnocení uděláme rekurzivně, čímž dohromady dostaneme časovou složitost $\mathcal{O}(n \log n)$[1].

[1] To plyne z Kuchařkové věty (Master Theorem).

Ale na jednu věc si musíme dát pozor! Pro správnou funkčnost rekurze potřebujeme, aby čísla $x_0^2, x_1^2, \ldots, x_{n/2-1}^2$ byla opět spárovaná. Přesně k tomu potřebujeme využít komplexní čísla.

Polynom budeme vyhodnocovat v bodech $\omega^0, \omega^1, \ldots, \omega^{n-1}$. Navíc platí, že ω^2 je primitivní $\frac{n}{2}$-tá odmocnina z jedničky, takže rekurzivní volání funguje.

Příklad 8. Ověřte, že jsou čísla $\omega^0, \omega^1, \ldots, \omega^{n-1}$ spárovaná.

FFT v konečných tělesech

Fourierovu transformaci nemusíme zavádět jen nad $\mathbb{C}$. Stačí nám libovolné těleso, ve kterém máme primitivní n-tou odmocninu z jedničky. V konečných tělesech $\mathbb{Z}_p$ pro p prvočíslo platí, že jejich multiplikativní grupa (množina nenulových prvků s operací násobení) je cyklická, tedy všech $p-1$ nenulových prvků tělesa lze zapsat jako mocniny nějakého čísla g (generátoru grupy). Mezi čísly $g^0, g^1, \ldots, g^{p-2}$ se každý nenulový prvek grupy vyskytuje právě jednou, takže g je primitivní $(p-1)$-ní odmocnina z jedničky.

Vhodné jsou například hodnoty $p = 2^{16}+1 = 65537$, $g = 3$. Takže můžeme využít $\omega = 3$ a $n = 2^{16}$.

Výhodou této varianty FFT je, že jsou méně zatížené zaokrouhlovacími chybami (komplexní odmocniny z jedničky mívají obě složky iracionální).

Návody

2. Uvědomte si, že $\frac{\omega^k}{\omega^j} = \omega^{k-j} \neq 1$.

3. Jaké jsou možné hodnoty $\omega^{\frac{n}{2}} = \sqrt{1}$?

4. Spočtěte $\left(\Omega \cdot \overline{\Omega}\right)_{j,k}$ a ukažte, že výraz je roven 0 pro $j \neq k$ a n pro $j = k$. Bude se vám hodit vzorec pro součet geometrické řady:

$$\sum_{k=0}^{n-1} q^k = \frac{q^n - 1}{q - 1}.$$

5.
a) Využijte podobnou myšlenku jako v předchozím příkladu,
b) je to kosinus s frekvencí $n/2$,
c) součet b) s konstantní 1,
d) $y_j = \sum_{k=0}^{n-1} \omega^k \omega^{jk} = \sum_{k=0}^{n-1} \left(\omega^{j+1}\right)^k$, což je nenulové pro $j \equiv -1 \pmod{n}$,
e) stejně jako d), akorát vyjde $j+2$.

6. Zobecněte poslední dvě podúlohy předchozího příkladu.

7. Všimněte si, že vám stačí $n = 4$. Asi nejpřehlednější je pro výpočet využít násobení maticemi Ω a $\overline{\Omega}$.

Literatura a zdroje

[1] Martin Mareš, Tomáš Valla: *Průvodce labyrintem algoritmů*, CZ.NIC, 2017.

[2] 3Blue1Brown: *But what is the Fourier Transform? A visual introduction.*, *https://www.youtube.com/watch?v=spUNpyF58BY*

Obsah