Konečné projektívne roviny a latinské štvorce

Peter „πtr“ Korcsok

Abstrakt. V tejto prednáške sa zoznámime s konceptom konečných projektívnych rovín a latinských štvorcov a ukážeme si, ako tieto objekty navzájom súvisia. V druhej časti prednášky si predstavíme ich aplikáciu pri takzvaných samoopravných kódoch. Tieto kódy sa využívajú pri prenose informácií menej spoľahlivým spôsobom, kde môže dochádzať k zmene niektorých z prenášaných znakov.

Kde sa to tu vzalo?

Už okolo roku 300 pred naším letopočtom napísal Euklides dielo *Základy*, v ktorom v trinástich knihách uviedol vtedajšie poznatky o geometrii a číslach formou axiómov a vecí z nich odvodených. V prvej z týchto kníh zaviedol aj päť postulátov (axiómov), ktoré následne tvorili základ množstva geometrických dôkazov.

Piaty postulát – najznámejší asi v podaní od Playfaira „pre daný bod a priamku ním neprechádzajúcu existuje maximálne jedna rovnobežka prechádzajúca daným bodom“ – je odlišný od zvyšných, preto sa ho mnoho matematikov snažilo dokázať s využitím iba predchádzajúcich štyroch. Všetky tieto pokusy ale boli neúspešné, dnes je už dokonca známe, že taký dôkaz ani existovať nemôže.

Miesto toho sa v geometrii zostrojil nový „model“ – predpokladá platnosť prvých štyroch postulátov, ten posledný je nahradený predpokladom „pre ľubovoľný bod a priamku ním neprechádzajúcu existujú aspoň dve rovnobežky prechádzajúce daným bodom“. Takýto systém priamok a bodov zvyknú matematici označovať ako *hyperbolickú rovinu*, tou sa ale na tejto prednáške nebudeme zaoberať.

Podobne sa ale môžeme dopracovať k *projektívnej* alebo aj *eliptickej rovine*, ktorá využíva mierne voľnejšie Euklidove postuláty, pričom posledný je nahradený podmienkou „každé dve rôzne priamky sa pretínajú“.

Pomoooc! Čo to je?!

Už sme zistili, prečo sa začali projektívne roviny skúmať. Aby sme ich mohli lepšie spoznať, musíme si ich trochu presnejšie popísať.

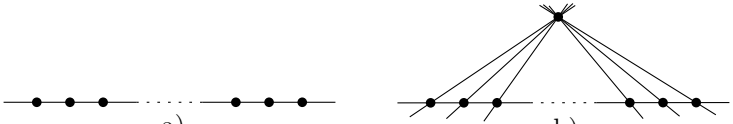
Definícia. *Projektívnou rovinou* budeme nazývať množinový systém $(B, \mathcal{P})$, kde $\mathcal{P} \subseteq 2^B$ a platia nasledujúce axiómy:

(1) $(\forall P, Q \in \mathcal{P},\ P \neq Q)\ |P \cap Q| = 1$,
(2) $(\forall x, y \in B,\ x \neq y)\ (\exists! P \in \mathcal{P})\ x, y \in P$,
(3) $(\exists \check{S} \subseteq B, |\check{S}| = 4)\ (\forall P \in \mathcal{P})\ |P \cap \check{S}| \leq 2$.

Prvky množiny B potom nazývame *bodmi PR*, prvky $\mathcal{P}$ sú tiež *priamky PR*. Ak navyše platí, že B má len konečne veľa bodov, hovoríme o *konečnej projektívnej rovine*.

Poznámka. Axióm (3) môžeme ekvivalentne nahradiť ľubovoľným z nasledujúcich dvoch:

(3′) $(\forall P, Q \in \mathcal{P})\ B \setminus (P \cup Q) \neq \emptyset$,
(3″) $(B, \mathcal{P})$ netvorí systém ako na obrázku:



Cvičenie. Nájdite najmenšiu projektívnu rovinu.

Tvrdenie. *Majme KPR $(B, \mathcal{P})$, potom všetky priamky $P \in \mathcal{P}$ obsahujú rovnako veľa bodov.*

Definícia. *Rádom KPR* $(B, \mathcal{P})$ budeme rozumieť hodnotu $|P| - 1$ pre $P \in \mathcal{P}$.

Tvrdenie. *Nech $(B, \mathcal{P})$ je KPR rádu n. Potom platia nasledujúce vlastnosti:*

(0) $(\forall P \in \mathcal{P})\ |P| = n + 1$,
(1) $(\forall x \in B)\ |\{P \in \mathcal{P}; x \in P\}| = n + 1$,
(2) $|B| = n^2 + n + 1$,
(3) $|\mathcal{P}| = n^2 + n + 1$.

Kde to rastie?

V predchádzajúcej časti sme si popísali, čo to konečné projektívne roviny sú a aké sú ich základné vlastnosti, v cvičení sme si dokonca skúsili nejakú KPR aj nájsť. Je ale možné, že je to jediný exemplár, ktorý spĺňa našu definíciu? Na to sa teraz pozrieme.

Jednou z možností je využitie vhodných algebraických telies:

Tvrdenie. *Pre každé $n = p^k$, kde p je prvočíslo a $k \in \mathbb{N}$, existuje KPR rádu n.*

Hypotéza. *KPR rádu n existuje práve pre $n = p^k$ pre nejaké prvočíslo p a $k \in \mathbb{N}$.*

Druhú možnosť nám dávajú tzv. *latinské štvorce*:

Definícia. *Latinským štvorcom rádu* n budeme označovať maticu $L \in [n]^{n\times n}$ spĺňajúcu podmienku

$$(\forall\, i \neq i', j \neq j' \in [n])\ L_{i'j} \neq L_{ij} \neq L_{ij'},$$

kde $[n] = \{1, \ldots, n\}$. Pre $k < n$ nazveme *latinským obdĺžnikom* maticu tvaru $k \times n$ spĺňajúcu predchádzajúcu podmienku pre každú dvojicu $i \neq i' \in [k]$

Tvrdenie. *Každý latinský obdĺžnik je možné doplniť na latinský štvorec.*

Cvičenie. Z balíčka kariet vyberte všetky štyri esá, kráľov, dámy aj chlapcov a rozmiestnite ich do mriežky 4×4 tak, aby žiadny riadok ani stĺpec neobsahoval dve karty rovnakej farby alebo hodnoty.

Definícia. Latinské štvorce L a L' rádu n nazveme *ortogonálnymi* ($L \perp L'$), ak platí podmienka

$$(\forall\, i, i', j, j' \in [n])\ (i,j) \neq (i',j') \Rightarrow (L_{i,j}, L'_{i,j}) \neq (L_{i',j'}, L'_{i',j'}).$$

Skupinu latinských štvorcov rovnakého rádu nazveme *navzájom ortogonálnymi*, ak každé dve z nich sú ortogonálne.

Príklad. Nasledujúci príklad ilustruje dve ortogonálne latinské štvorce rádu 3:

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{bmatrix}$$

Tvrdenie. *Nech $L_1, \ldots, L_m$ sú NOLŠ rádu n. Potom $m \leq n-1$.*

Veta. *Pre $n > 2$ existuje KPR rádu n, práve keď existuje $n-1$ NOLŠ rádu n.*

Dá sa to jesť?

Už sme si ukázali, ako vieme niektoré konečné projektívne roviny, prípadne latinské štvorce tvoriť, poďme sa teda zamyslieť, aký majú význam v bežnom živote.

Definícia. *Slovom w dĺžky n nad abecedou* Σ ($w \in \Sigma^n$) nazveme ľubovoľnú postupnosť n znakov z danej abecedy Σ. Vo väčšine prípadov sa používa $\Sigma = \{0,1\}$, prípadne obecnejšie $\Sigma = \{0, \ldots, q\}$ pre nejaké $q \in \mathbb{N}$.

Definícia. *Hammingovu vzdialenosť* dvoch slov $u, v \in \Sigma^n$ definujeme nasledovne:

$$d_H(u,v) = |\{i \in [n];\ u_i \neq v_i\}|\,.$$

Definícia. Podmnožinu $K \subseteq \Sigma^n$, $|K| = |\Sigma|^k$, kde platí $d_H(u,v) \geq d$ pre ľubovoľné $u \neq v \in K$, nazveme (n,k,d)-*kódom* a hovoríme o kóde dĺžky n, veľkosti $|\Sigma|^k$ a vzdialenosti d.

Pozorovanie. *(n, k, d)-kód dokáže rozpoznať až $d - 1$ a opraviť až $\lfloor \frac{d-1}{2} \rfloor$ chýb.*

Tvrdenie. *Ak existuje (n, k, d)-kód pre $d \geq 2$, potom existuje aj $(n - 1, k, d - 1)$-kód.*

Tvrdenie. *Ak existuje KPR rádu n, potom existuje aj kód nad abecedou $\Sigma = \{0, 1\}$ dĺžky $n^2 + n + 1$, veľkosti $n^2 + n + 2$ a vzdialenosti $2n$.*

Problém. Akú najväčšiu veľkosť môže mať kód nad abecedou $\Sigma = \{0, \ldots, q\}$ dĺžky 4 a vzdialenosti 3?

V nasledujúcich tvrdeniach budeme predpokladať abecedu $\Sigma = \{0, \ldots, q\}$.

Tvrdenie. *Pre každý $(4, k, 3)$-kód určite platí $k \leq 2$.*

Tvrdenie. *$(4, 2, 3)$-kód existuje práve vtedy, ak existujú dve ortogonálne latinské štvorce rádu q.*

A teraz trochu obecnejšie:

Tvrdenie. *Pre každý (n, k, d)-kód určite platí $k \leq n - d + 1$.*

Tvrdenie. *$(n, 2, n - 1)$-kód existuje práve vtedy, ak existuje $n - 2$ NOLŠ rádu q.*

Dôsledok. *$(n, 2, n - 1)$-kód nad abecedou $\Sigma = \{0, \ldots, n - 1\}$ existuje pre každé $n = p^k + 1$, kde p je prvočíslo a $k \in \mathbb{N}$. Ak by platila spomínaná hypotéza, takýto kód pre žiadne iné n neexistuje.*

Literatúra a zdroje

Pri príprave tejto prednášky som čerpal prevažne z nasledujúcich materiálov:

[1] Connelly, Robert. *Classical Geometries* (texty k prednáške). Cornell University, Ithaca, NY, 2010. *www.math.cornell.edu/∼web4520/*

[2] Bartlett, Padraic. *Latin Squares* (texty k prednáške). Mathcamp 2012. *www.its.caltech.edu/∼padraic/mathcamp_2012/mathcamp_2012.html*

[3] zápisky z prednášok *Kombinatorika a grafy I*, *Kombinatorika a grafy II* a *Kombinatorické struktury* na MFF UK