Kombinatorické štruktúry

prof. RNDr. Martin Škoviera, PhD.

25. januára 2024

Obsah

Úvod

Cieľom tvorby tohto textu je urobiť prehľad o kľúčových pojmoch a tvrdeniach z teórie kombinatorických štruktúr a pomôcť tak pri príprave na skúšku. Daný text nie je náhradou absolvovania prednášok[1]. Vety, ktorých dôkazy sú nad našu úroveň, sú označené hviezdičkou.

Tento text je písaný na základe prednášok z predmetu Kombinatorické štruktúry v zimnom semestri akademického roku 2016/17, 2018/19 a 2020/21. Na tvorbe textu sa podieľali Askar Gafurov, Mário Lipovský, Jozef Rajník, Andrej Korman, Martin Pašeň, Ivan Agarský a Jitka Muravská.

Zdrojový kód nájdete tu: `https://github.com/japdlsd/komb_str_syllabus`. Pull requesty sú vítané!

[1] a ani náhradou pestrej stravy :)

Kapitola 1

Latinské štvorce

Latinský štvorec, s ktorým budeme túto kapitolu pracovať predstavuje štvorcovú tabuľku rozmerov $n \times n$ vyplnenú n rôznymi symbolmi, napríklad číslami od 1 po n tak, že v každom riadku a v každom stĺpci sa každý symbol vyskytuje práve raz. Latinské štvorce nachádzajú uplatnenie vo viacerých oblastiach ako štatistika, lineárna algebra, kódovanie alebo aj pri rôznych logických úlohách a hlavolamoch.

Jednoduchou ilustráciou latinských štvorcov je napríklad Sudoku, ktoré je vlastne zosilnený latinský štvorec o požiadavky na štvorcové bloky 3×3.

1.1 Definícia, základné vlastnosti

Okrem formálnej definície latinského štvorca, pripomenieme definíciu permutácie a jej základných vlastností. Riadky a stĺpce latinského štvorca si vieme predstaviť ako permutácie prvkov $1, \ldots, n$, čo neskôr využijeme na alternatívnu definíciu latinského štvorca.

Def 1.1. Tabuľka rozmerov $n \times n$ s prvkami z $\{1, \ldots, n\}$ je latinský štvorec rádu n, ak platí:

1. v každom riadku sa vyskytuje všetkých n rôznych symbolov
2. v každom stĺpci sa vyskytuje všetkých n rôznych symbolov

Úloha 1. Zostrojte latinský štvorec rádu 5.

Úloha 2. Zostrojte latinský štvorec rádu 7.

Úloha 3. Napíšte program na generovanie latinských štvorcov, ktorý bude generovať štvorec po riadkoch preberaním všetkých možností.

Príklad 1.1. Zostrojovať a generovať latinské štvorce je príjemná úloha na precvičenie definície, no môžeme sa aj zamyslieť načo by nám mohli byť užitočné. Predstavme si nasledujúci problém: *Sme vlastník farmy a chceme rozšíriť produkciu o vajíčka. Máme na výber z troch druhov sliepok s_1, s_2 a s_3. Chceme samozrejme vybrať tie, čo znesú najviac vajec za nejaké obdobie, napríklad 3 mesiace - apríl, máj a jún.*

Na takéto porovnanie môžeme navrhnúť jednoduchý experiment:

- Kúpime 3 polia p_1, p_2, p_3 pre pasenie sliepok.
- Umiestnime druh s_1 na pole p_1, druh s_2 na pole p_2 a druh s_3 na pole p_3.

- Spočítame počet znesených vajec za tri mesiace pre jednotlivé druhy sliepok a vyberieme druh, ktorý zniesol najviac.

Tento nápad má však zjavný problém, jeden druh testujeme iba na jednom poli. Teda produkcia vajec daného druhu nemusí záležať len od vlastností daného druhu, ale aj od poľa, na ktorom sa pásli. Napríklad pole p_1 je vystavené väčšiemu hluku, pole p_2 je bližšie k lesu, kde žije veľa líšok a pole p_3 je podmývané.

Lepším riešením by bolo testovať všetky druhy na všetkých poliach, na každom aspoň mesiac. Aby sme nemuseli kupovať ďalšie polia alebo nerealizovali experiment dlhšie, navrhneme rozpis, na ktorom poli bude, v ktorom mesiaci, ktorý druh sliepok. Tento rozpis môžeme reprezentovať a zostrojiť ako latinský štvorec, kde riadky budú polia, stĺpce mesiace a v bunkách budú druhy sliepok.

Def 1.2. Dvojica $S_n = (P, \circ)$ je grupa permutácií rádu n, kde P je množina všetkých permutácii veľkosti n (t.j. množina všetkých bijektívnych zobrazení z množiny $\{1, \ldots, n\}$ na ňu samu) a $\circ$ je binárna operácia skladania zobrazení, definovaná nasledovné:

$$\forall \phi, \psi \in S_n \forall x \in \{1, \ldots, n\} : (\phi \circ \psi)(x) = \phi(\psi(x)).$$

Pre krátkosť zápisu budeme symbol skladania vynechávať, t.j. $\phi\psi \stackrel{def}{\equiv} \phi \circ \psi$. Neutrálny prvok grupy S_n (t.j. identické zobrazenie) budeme označovať 1.

Def 1.3. Nech $\phi, \psi \in S_n$ sú permutácie veľkosti n. Potom vzdialenosť $\mathrm{dist}(\phi, \psi)$ dvoch permutácií definujeme ako počet prvkov, ktoré dané permutácie zobrazia rôzne. Formálne,

$$\mathrm{dist}(\phi, \psi) := |\{x \mid x \in \{1, \ldots, n\} \wedge \phi(x) \neq \psi(x)\}|$$

Def 1.4. Nech $\phi \in S_n$ je permutácia veľkosti n. Potom $Fix(\phi)$ je množina všetkých pevných bodov permutácie ϕ. Formálne,

$$Fix(\phi) := \{x \mid x \in \{1, \ldots, n\} \wedge \phi(x) = x\}$$

Úloha 4. Dokážte, že platí $\forall \phi \in S_n : Fix(\phi) = Fix(\phi^{-1})$.

Veta 1.1. *Nech $\phi, \psi \in S_n$ sú permutácie veľkosti n. Potom platí:*

1. $\forall \lambda \in S_n : \mathrm{dist}(\phi\lambda, \psi\lambda) = \mathrm{dist}(\lambda\phi, \lambda\psi) = \mathrm{dist}(\phi, \psi)$
2. $\mathrm{dist}(\phi, \psi) = \mathrm{dist}(1, \phi^{-1}\psi) = n - |Fix(\phi^{-1}\psi)|$

Dôkaz. Začneme dôkazom prvého tvrdenia. Dokážeme rovnosť $\mathrm{dist}(\phi\lambda, \psi\lambda) = \mathrm{dist}(\phi, \psi)$, druhú rovnosť prenechávame čitateľovi ako samostatné cvičenie (úloha 5).

Chceme ukázať, že vzdialenosti dvoch párov permutácií sú rovnaké. To znamená, že počty prvkov, v ktorých sa ich hodnoty líšia, je rovnaký. Prvú množinu prvkov označíme ako A, druhú ako B. Formálne, nech

$$A := \{x | x \in \{1, \ldots, n\} \wedge \phi(x) \neq \psi(x)\}$$

(t.j. $\mathrm{dist}(\phi, \psi) = |A|$ z definície vzdialenosti 1.3) a

$$B := \{y | y \in \{1, \ldots, n\} \wedge \phi(\lambda(y)) \neq \psi(\lambda(y))\}$$

(t.j. $\mathrm{dist}(\phi\lambda, \psi\lambda) = |B|$ z definície vzdialenosti 1.3).

Najprv ukážeme, že platí $|A| \geq |B|$, následne $|B| \geq |A|$. Z toho už platnosť prvého tvrdenia z vety bude očividná.

Nech $x \in A$. Z definície množiny A vyplýva, že $\phi(x) \neq \psi(x)$. Nech $y := \lambda^{-1}(x)$. Potom platí, že $\phi(\lambda(y)) \neq \psi(\lambda(y))$, čiže $y \in B$ z definície množiny B. Keďže λ^{-1} je permutácia, tak je injektívnym zobrazením. To znamená, že rôzne hodnoty x premietne do rôznych hodnôt y. Z toho vyplýva, že veľkosť množiny B je aspoň tak veľká, ako množiny A, t.j. $|A| \leq |B|$.

Ukážeme teraz druhú nerovnosť. Nech $y \in B$. Potom (z definície množiny B) platí $\phi(\lambda(y)) \neq \psi(\lambda(y))$. Teda, z definície množiny A, $\lambda(y) \in A$. Analogicky (z injektivity permutácie λ) vyplýva, že $|B| \leq |A|$. Týmto je dôkaz prvého tvrdenia z dokazovanej vety ukončený.

Dôkaz druhého tvrdenia z vety prenechávame čitateľovi ako samostatné cvičenie (úloha 6). □

Úloha 5. Dokážte, že $\forall \phi, \psi, \lambda \in S_n : \mathrm{dist}(\lambda\phi, \lambda\psi) = \mathrm{dist}(\phi, \psi)$.

Úloha 6. Dokážte tvrdenie 2 z vety 1.1 (*hint: použite prvé tvrdenie z tejto vety*).

Úloha 7. Dokážte, že $\forall \phi, \psi \in S_n : \mathrm{dist}(\phi, \psi) = \mathrm{dist}(\phi^{-1}, \psi^{-1})$.

Veta 1.2. *Funkcia* $\mathrm{dist}(\phi, \psi)$ *je metrikou priestoru* S_n*, t.j. ona spĺňa nasledujúce podmienky:*

1. $\forall \phi, \psi \in S_n : \mathrm{dist}(\phi, \psi) = 0 \Leftrightarrow \phi = \psi$
2. $\forall \phi, \psi \in S_n : \mathrm{dist}(\phi, \psi) = \mathrm{dist}(\psi, \phi)$ *(symetria)*
3. $\forall \phi, \psi, \lambda \in S_n : \mathrm{dist}(\phi, \psi) + \mathrm{dist}(\psi, \lambda) \geq \mathrm{dist}(\phi, \lambda)$ *(trojuholníková nerovnosť)*

Dôkaz. Prvé dve tvrdenia sú očividné a nepotrebujú špeciálny dôkaz. Pozrime sa teda na tretie tvrdenie o trojuholníkovej nerovnosti.

Nech $\phi_1, \phi_2, \phi_3 \in S_n$. Treba dokázať, že[1]

$$\mathrm{dist}(\phi_1, \phi_2) + \mathrm{dist}(\phi_2, \phi_3) \stackrel{?}{\geq} \mathrm{dist}(\phi_1, \phi_3).$$

Z vety 1.1 táto nerovnosť je ekvivalentná s nerovnosťou[2]

$$(n - |Fix(\phi_1^{-1}\phi_2)|) + (n - |Fix(\phi_2^{-1}\phi_3)|) \stackrel{?}{\geq} n - |Fix(\phi_1^{-1}\phi_3)|.$$

Ak komplement množiny A (vzhľadom na základnú množinu $\{1, \ldots, n\}$) označíme ako $\overline{A}$, tak túto nerovnosť môžeme prepísať do ďalšieho ekvivalentného tvaru[3]:

$$|\overline{Fix(\phi_1^{-1}\phi_2)}| + |\overline{Fix(\phi_2^{-1}\phi_3)}| \stackrel{?}{\geq} |\overline{Fix(\phi_1^{-1}\phi_3)}|.$$

Dokážeme si pomocné tvrdenie[4]:

$$\overline{Fix(\phi_1^{-1}\phi_2)} \cup \overline{Fix(\phi_2^{-1}\phi_3)} \stackrel{?}{\supseteq} \overline{Fix(\phi_1^{-1}\phi_3)}.$$

[1] tu a ďalej: otázniky nad znakmi rovnosti, nerovnosti alebo iných relácií označujú ten fakt, že dané tvrdenia ešte nie sú dokázané v rámci textu. Používame túto notáciu najmä v prípadoch, keď robíme úpravy nad práve dokazovanými tvrdeniami

[2] väčšina učebnicových dôkazov má veľmi jednoduchú schému: skúšame použiť postupne všetky doteraz dokázané vety. V danom prípade prehľadávanie je uľahčené tým faktom, že toto je ešte len druhá veta

[3] pozor, v tretej kapitole si podobným symbolom budeme označovať uzáver množiny v matroide

[4] niektorí ľudia v týchto okamihoch zvyknú nahlas povedať "Heuréka!"

Všimnite si, že ak daná inklúzia platí, tak z nej vyplývajú aj predchádzajúce tvrdenia (kvôli $A \cup B \supseteq C \implies |A \cup B| \geq |C| \implies |A| + |B| \geq |C|$). Môžeme toto tvrdenie prepísať do ekvivalentného tvaru, odstrániac znaky komplementu:

$$Fix(\phi_1^{-1}\phi_2) \cap Fix(\phi_2^{-1}\phi_3) \overset{?}{\subseteq} Fix(\phi_1^{-1}\phi_3).$$

Túto inklúziu dokážeme priamo. Nech $x \in Fix(\phi_1^{-1}\phi_2) \cap Fix(\phi_2^{-1}\phi_3)$. Potom $x = \phi_1^{-1}(\phi_2(x))$ a $x = \phi_2^{-1}(\phi_3(x))$. Dosadením druhej rovnosti do prvej dostaneme $x = \phi_1^{-1}(\phi_2(\phi_2^{-1}(\phi_3(x)))) = \phi_1^{-1}(\phi_3(x))$, čiže x je aj pevným bodom permutácie $\phi_1^{-1}\phi_3$, t.j. $x \in Fix(\phi_1^{-1}\phi_3)$. Týmto je dôkaz pomocného tvrdenia, a s tým aj celej vety, ukončený. □

Def 1.5. Latinský obdĺžnik rozmerov $k \times n$ je postupnosť $L = [\phi_1, \phi_2, \ldots, \phi_k]$ permutácií z S_n takých, že všetky sú vo vzdialenosti n. Formálne,

$$\forall i, j \in \{1, \ldots, n\} : i \neq j \Rightarrow \text{dist}(\phi_i, \phi_j) = n$$

Def 1.6. (Iná definícia latinských štvorcov) Latinský štvorec rádu n je latinský obdĺžnik typu $k \times n$ s maximálnou dĺžkou postupnosti. Inak povedané, latinský štvorec rádu n je postupnosť n permutácií z S_n, ktoré sú od seba vzdialené n.

Úloha 8. Nech $l = [\phi_1, \ldots, \phi_k]$ je latinský obdĺžnik typu $k \times n$ a $\lambda \in S_n$ je permutácia rádu n. Dokážte, že $[\lambda\phi_1, \ldots, \lambda\phi_k]$ a $[\phi_1\lambda, \ldots, \phi_k\lambda]$ sú tiež latinskými obdĺžnikmi typu $k \times n$.

Def 1.7. Nech X je množina a $\mathcal{X} = \{X_1, \ldots, X_k\}, \forall i \in \{1, \ldots, k\} : X_i \subseteq X$ je systém jej podmnožín. Systém rozličných reprezentantov pre $\mathcal{X}$ je postupnosť $x_1, \ldots x_k, \forall i \in \{1, \ldots, k\} : x_i \in X_i$ a zároveň sú všetky jej prvky rôzne, teda $\forall i, j \in \{1, \ldots, k\} : i \neq j \Rightarrow x_i \neq x_j$.

Lema 1.3. *(Hallova veta o párení, 1935) Nech $G = (A \cup B, E)$, kde $E \subseteq A \times B$, je konečný bipartitný graf s partíciami A a B. Nech $N_G(W)$ je okolie množiny vrcholov $W \subseteq A$. Formálne, $N_G(W) := \{y \in B | \exists x \in W : (x, y) \in E\}$ Potom graf G má úplné párenie práve vtedy keď*

$$\forall W \subseteq A : |N_G(W)| \geq |W|.$$

Neformálne povedané, ak každá podmnožina vrcholov z A má dostatočný počet kandidátov na spárovanie.

Dôkaz tejto lemy môžete nájsť v knihe *Graph Theory* (Diestel, 2000)[5].

Veta 1.4. *(Hallova veta pre množiny) Nech $\mathcal{X}$ je systém podmnožín množiny X. Ak $\forall \mathcal{Y} = \{Y_1, \ldots, Y_m\} \subseteq \mathcal{X} : |\bigcup_{Y \in \mathcal{Y}} Y| > m$ tak pre $\mathcal{X}$ existuje systém rozličných reprezentantov.*

Dôkaz. Cez Hallovu vetu pre bipartitné grafy. Vytvoríme bipartitný graf, ktorého partícia A obsahuje jeden vrchol pre každú množinu z $\mathcal{X}$ a partícia B obsahuje jeden vrchol pre každý prvok z X. Každý vrchol množiny spojíme s vrcholmi prvkov, ktoré obsahuje, teda $(X_i, x_j) \in E(G) \Leftrightarrow x_j \in X_i$. Z Hallovej vety o párení potom existuje párenie pokrývajúce všetky vrcholy A, ak z každej podmnožiny vrcholov A veľkosti m vychádza aspoň m hrán. □

Úloha 9. Napíšte polynomiálny algoritmus na nájdenie systému rozličných reprezentantov.

[5] alebo na Wikipédii: https://en.wikipedia.org/wiki/Hall's_marriage_theorem

Veta 1.5. *Každý latinský obdĺžnik sa dá doplniť na latinský štvorec.*

Dôkaz. Pomocou Hallovej vety dokážeme, že do každého latinského obdĺžnika $k \times n, k < n$ vieme pridať ďalší riadok. Pre i-ty stĺpec obdĺžnika definujeme množinu kandidátov X_i ako prvky, ktoré sa v stĺpci nenachádzajú. Z latinskej vlastnosti vyplýva, že do každého stĺpca sa dá doplniť práve $n-k$ prvkov, teda $\forall i \in \{1, \ldots, n\} : |X_i| = n - k$. Opačne, každý prvok sa dá doplniť do $n - k$ stĺpcov. Bipartitný graf zodpovedajúci $\mathcal{X} = \{X_1, \ldots X_n\}$ je teda $(n-k)$-regulárny. Z každej množiny stĺpcov veľkosti m tak vychádza $m(n - k)$ hrán, ktoré musia v druhej partícii vchádzať do m vrcholov. Keďže je splnená Hallova podmienka, existuje systém reprezentantov $\mathcal{X}$, ktorý vieme použiť ako $(k + 1)$-vý riadok latinského obdĺžnika. □

Úloha 10. Napíšte polynomiálny algoritmus na generovanie alebo doplňovanie latinských štvorcov (*hint: použite algoritmus z úlohy 9*).

1.2 Ortogonálne latinské štvorce

Def 1.8. Nech $l = [\phi_1, \ldots, \phi_n]$ a $l' = [\psi_1, \ldots, \psi_n]$ sú latinské štvorce rádu n. Hovoríme, že l a l' sú ortogonálne (značíme ako $l \perp l'$), ak platí:

$$\forall i, j, k, l \in \{1, \ldots, n\} : (i, j) \neq (k, l) \Longrightarrow (\phi_i(j), \psi_i(j)) \neq (\phi_k(l), \psi_k(l)).$$

Inak povedané, ak z prvkov na rovnakých pozíciách vytvoríme dvojice, tak sa každá dvojica z $\{1, \ldots, n\}^2$ objaví práve raz.

Úloha 11. Nájdite dva ortogonálne latinské štvorce rádu 5.

Úloha 12. Napíšte (nie nutne polynomiálny) program, ktorý pre daný latinský štvorec nájde jemu ortogonálny.

Veta 1.6. *Nech $l = [\phi_1, \ldots, \phi_n]$ a $l' = [\psi_1, \ldots, \psi_n]$ sú latinské štvorce rádu n. Zavedieme nasledovné značenia:*

- *Nech $\lambda \in S_n$, potom $\lambda l := [\lambda\phi_1, \ldots, \lambda\phi_n]$ (λl je tiež latinský štvorec).*
- *Nech kompozícia l a l' je definovaná ako $l \circ l' := [\phi_1\psi_1, \ldots, \phi_n\psi_n]$.*

Potom platí:

1. *$l \perp l' \Leftrightarrow [\psi_1\phi_1^{-1}, \ldots, \psi_n\phi_n^{-1}]$ je latinský štvorec*
2. *Ak $\lambda, \rho \in S_n$ a $l \perp l'$, tak aj $\lambda l \perp \rho l'$*
3. *$l \perp l' \Leftrightarrow$ existuje latinský štvorec l'' taký, že $l' = l'' \circ l$*

Dôkaz. Prvé tvrdenie je ekvivalenciou, označíme ľavú stranu ako A a pravú ako B. Dokazovať túto ekvivalenciu budeme postupne, obidve implikácie $A \Longrightarrow B$ a $B \Longrightarrow A$ samostatne. Obidve implikácie budeme dokazovať nepriamo, t.j. dokážeme tvrdenia $\neg A \Longrightarrow \neg B$ a $\neg B \Longrightarrow \neg A$.

$$\neg A \overset{(def.)}{\Longleftrightarrow} \exists i, j, k, l \in \{1, \ldots, n\} : (i, j) \neq (k, l) \wedge \phi_i(j) = \phi_k(l) \wedge \psi_i(j) = \psi_k(l)$$

$$\neg B \overset{(def.)}{\Longleftrightarrow} \exists I, J, X \in \{1, \ldots, n\} : I \neq J \wedge \psi_I\phi_I^{-1}(X) = \psi_J\phi_J^{-1}(X)$$

$\neg A \Longrightarrow \neg B$:

Nech platí $\neg A$ a nech i, j, k, l sú príslušné čísla z tvrdenia. Nech[6] $X := \phi_i(j) = \phi_k(l), I := i, J := k$. Treba ukázať, že $I \overset{?}{\neq} J$ a $\psi_I\phi_I^{-1}(X) \overset{?}{=} \psi_J\phi_J^{-1}(X)$. Začnime druhým:

$$\begin{aligned} \psi_I\phi_I^{-1}(X) &\overset{?}{=} \psi_J\phi_J^{-1}(X) && \text{dosadíme hodnoty } X, I, J \\ \psi_i\phi_i^{-1}(\phi_i(j)) &\overset{?}{=} \psi_k\phi_k^{-1}(\phi_k(l)) && \phi(\phi^{-1}(x)) = x \\ \psi_i(j) &\overset{\checkmark}{=} \psi_k(l) && \text{platí z predpokladu } \neg A \end{aligned}$$

Zostáva ešte ukázať, že $I \overset{?}{\neq} J$. Sporom: nech $I = J$, čiže $i = k$. Potom nutne $j \neq l$ (z predpokladu $\neg A$). Po dosadení do tvrdenia $\neg A$ dostávame $j \neq l \wedge \phi_i(j) = \phi_i(l)$, t.j. permutácia ϕ_i zobrazuje dva rôzne prvky j a l do toho istého prvku, čo je spor s tým, že ϕ_i je injektívne zobrazenie. Týmto je dôkaz prvej implikácie z prvého tvrdenia vety ukončený.

$\neg B \Longrightarrow \neg A$:

Nech platí $\neg B$ a I, J, X sú príslušné čísla z tvrdenia. Nech $i := I$, $k := J$, $j := \phi_I^{-1}(X)$, $l := \phi_J^{-1}(X)$. Treba ukázať, že $(i, j) \overset{?}{\neq} (k, l)$, $\phi_i(j) \overset{?}{=} \phi_k(l)$ a $\psi_i(j) \overset{?}{=} \psi_k(l)$.

Prvé tvrdenie je platné kvôli predpokladu $I \neq J \Longleftrightarrow i \neq k$.

Druhé tvrdenie:

$$\begin{aligned} \phi_i(j) &\overset{?}{=} \phi_k(l) \\ \phi_I(\phi_I^{-1}(X)) &\overset{?}{=} \phi_J(\phi_J^{-1}(X)) \\ X &\overset{\checkmark}{=} X \end{aligned}$$

Tretie tvrdenie:

$$\begin{aligned} \psi_i(j) &\overset{?}{=} \psi_k(l) \\ \psi_I(\phi_I^{-1}(X)) &\overset{\checkmark}{=} \psi_J(\phi_J^{-1}(X)) && \text{z predpokladu } \neg B \end{aligned}$$

Týmto je dôkaz druhej implikácie, a s tým aj prvého tvrdenia z vety celkovo ukončený. Dôkaz druhého a tretieho tvrdenia prenechávame čitateľovi ako samostatné cvičenie (úlohy 13 a 14). □

Úloha 13. Dokážte tvrdenie 2 z vety 1.6.

Úloha 14. Dokážte tvrdenie 3 z vety 1.6.

Def 1.9. Množinu vzájomne ortogonálnych latinských štvorcov budeme označovať $MOLS$ a množinu vzájomne ortogonálnych latinských štvorcov rádu n označíme $MOLS(n)$.

Veta 1.7. *Maximálna (vzhľadom na inklúziu) $MOLS(n)$ má najviac $n-1$ prvkov.*

Dôkaz. Sporom: nech dokazované tvrdenie neplatí, teda existuje n navzájom ortogonálnych latinských štvorcov $l_1, \ldots, l_n$ rádu n. Preusporiadajme stĺpce latinských štvorcov tak, aby prvý riadok v každom bol rovný $(1, \ldots, n)$ (z vety 1.6). Pozrime sa teraz na prvé políčko v druhom riadku všetkých n latinských štvorcov.

[6] indexy I a J sme zvolili tak, lebo sú to jediné permutácie ϕ_i, o ktorých niečo vieme. Podobne aj X, nakoľko vieme o špecifickom správaní daných permutácií len v tomto bode

Tieto políčka nesmú obsahovať 1, lebo v prvom stĺpci je už použitá. Zároveň však platí, že hodnoty v týchto políčkach musia byť navzájom rôzne, nakoľko sa páry typu (k, k) už vyskytujú pri prvom riadku v každom páre latinských štvorcov (z definície ortogonálnych latinských štvorcov, každá dvojica hodnôt, vytvorená z prvkov na rovnakých pozíciách, sa musí vyskytnúť práve raz). Nakoľko vybrať z $(n-1)$ hodnôt až n rôznych nie je možné, dostávame spor, čím je dôkaz ukončený. □

Def 1.10. Latinský štvorec je v normálnom tvare, ak prvý riadok tabuľky je rovný $(1, \ldots, n)$ a prvý stĺpec je rovný $(1, \ldots, n)^T$.

Def 1.11. Latinské štvorce l a l' sú izotopické, ak sa dajú permutáciou riadkov, stĺpcov a názvov prvkov previesť na rovnaký latinský štvorec v normálnom tvare.

Poznámka 1.1. Latinský štvorec v normálnom tvare zodpovedá tabuľke binárnej operácie kvazigrupy (kvazigrupa je množina Q s binárnou operáciou $\circ$, v ktorej pre každý prvok $a, b \in Q$ existuje práve jedno $x, y \in Q$ také, že platia rovnosti $a \circ x = b$ a $y \circ a = b$)[7].

Platí, že 2 kvazigrupy sú izomorfné práve vtedy, keď príslušné latinské štvorce sú izotopické.

Úloha 15. Nájdite dva neizotopické latinské štvorce rádu 5.

Úloha 16. Napíšte program, ktorý pre dva zadané latinské štvorce overí, či sú izotopické.

Def 1.12. Latinský štvorec si vieme predstaviť ako maximálnu (na inklúziu) množinu A trojíc $(r, c, s) \in \{1, \ldots, n\}^3$, kde r zodpovedá číslu riadku, c zodpovedá číslu stĺpca a s zodpovedá hodnote v políčku (i, j), takú, že platí:

- všetky dvojice (r, c) sú rôzne ("máme n^2 políčok")
- všetky dvojice (r, s) sú rôzne ("v každom riadku sa vyskytnú všetky hodnoty od 1 po n")
- všetky dvojice (c, s) sú rôzne ("v každom stĺpci sa vyskytnú všetky hodnoty od 1 po n")

Konjugáciou latinského štvorca voláme množinu trojíc A', ktorá vznikne z A permutáciou trojíc. Formálne, nech $\lambda \in S_3$ je permutácia veľkosti 3, potom

$$A' = \left\{(a_{\lambda(1)}, a_{\lambda(2)}, a_{\lambda(3)}) \mid (a_1, a_2, a_3) \in A\right\}$$

Latinské štvorce, ktoré sa dajú jeden z druhého dostať pomocou konjugácie, voláme *konjugované*. Latinské štvorce, ktoré sa dajú jeden z druhého dostať pomocou konjugácie a izotopie, voláme *paratopické*.

Úloha 17. Nájdite dva neparatopické latinské štvorce rádu 5.

Úloha 18. Napíšte program, ktorý pre dva zadané latinské štvorce rozhodne, či sú paratopické.

Veta 1.8. *(Stevens, 1935) Ak $n = p^\alpha$, kde p je prvočíslo, tak maximálna $MOLS(n)$ má $n - 1$ prvkov.*

[7] dá sa to neformálne predstaviť ako klasickú grupu bez zaručenej asociativity

Konštrukcia. Číslo n je mocninou prvočísla, preto existuje konečné pole[8] $F := GF(n)$ príslušnej veľkosti. Očíslujeme prvky poľa F v ľubovoľnom poradí, ale nech $a_0 = 0$.

k-tý latinský štvorec si označme ako $l_k = \left(a_{ij}^{(k)}\right)$.

$a_{ij}^{(k)} := a_i a_k + a_j$

Dôkaz. Dôkaz pozostáva z dvoch častí. Najprv treba ukázať, že skonštruované l_k sú naozaj latinskými štvorcami, následne treba ukázať, že každá dvojica (l_a, l_b) je ortogonálna.

Latinský štvorec musí spĺňať podľa definície dve podmienky:

1. v každom riadku je práve raz každé z čísel $\{1, \ldots, n\}$, respektíve

$$\forall i, j_1, j_2 \in \{1, \ldots, n\} : j_1 \neq j_2 \Longrightarrow a_{ij_1}^{(k)} \neq a_{ij_2}^{(k)},$$

2. v každom stĺpci je práve raz každé z čísel $\{1, \ldots, n\}$, respektíve

$$\forall i_1, i_2, j \in \{1, \ldots, n\} : i_1 \neq i_2 \Longrightarrow a_{i_1 j}^{(k)} \neq a_{i_2 j}^{(k)}.$$

Sporom, nech prvá podmienka neplatí, čiže

$$\exists i, j_1, j_2 \in \{1, \ldots, n\} : j_1 \neq j_2 \wedge a_{ij_1}^{(k)} = a_{ij_2}^{(k)}.$$

Pozrieme sa bližšie na výraz $a_{ij_1}^{(k)} = a_{ij_2}^{(k)}$:

$$\begin{aligned} a_{ij_1}^{(k)} &= a_{ij_2}^{(k)} \\ a_i a_k + a_{j_1} &= a_i a_k + a_{j_2} \\ a_{j_1} &= a_{j_2} \qquad\qquad \text{SPOR} \end{aligned}$$

Dôkaz druhej podmienky sporom privedie ku výrazu $a_{i_1} a_k + a_j = a_{i_2} a_k + a_j$, ktorý taktiež vedie ku sporu.

Teraz zostáva dokázať $\forall k_1, k_2 \in \{1, \ldots, n\} : k_1 \neq k_2 \Longrightarrow l_{k_1} \perp l_{k_2}$. Sporom, nech $\exists k_1, k_2 : k_1 \neq k_2 \wedge l_{k_1} \not\perp l_{k_2}$, čiže

$$\exists i, j, k, l : (i, j) \neq (k, l) \wedge a_{ij}^{(k_1)} = a_{kl}^{(k_1)} \wedge a_{ij}^{(k_2)} = a_{kl}^{(k_2)}.$$

Prepíšeme tento výrok podľa konštrukcie a dostaneme:

$$(i, j) \neq (k, l) \wedge a_i a_{k_1} + a_j = a_k a_{k_1} + a_l \wedge a_i a_{k_2} + a_j = a_k a_{k_2} + a_l.$$

Po zopár algebraických úpravách dostaneme:

$$(i, j) \neq (k, l) \wedge (a_i - a_k) a_{k_1} = a_l - a_j = (a_i - a_k) a_{k_2}.$$

Ak $i \neq k$, tak $a_i - a_k \neq 0$, čiže $a_{k_1} = a_{k_2} \Longrightarrow k_1 = k_2$, čo je spor.

Ak $j \neq l$, tak $a_l - a_j \neq 0$, čiže $(a_i - a_k) a_{k_1} \neq 0 \Longrightarrow a_i \neq a_j \Longrightarrow a_{k_1} = a_{k_2} \Longrightarrow k_1 = k_2$, čo je spor.

Týmto je dôkaz správnosti konštrukcie ukončený.

□

[8] nie všetci vedia, ale konečné polia sa volajú tak kvôli tradičnému pokriku študentov informatiky "Konečne sú na niečo dobre!", ktorý im samovoľne vyletí z úst, keď prvýkrát zbadajú tieto štruktúry mimo druhého semestra vyššej algebry

Príklad 1.2. Povedzme, že chceme zostrojiť tri navzájom ortogonálne latinské štvorce. Budeme postupovať podľa konštrukcie z predchádzajúcej vety 1.8. Najprv teda potrebujeme zostrojiť konečné pole veľkosti 4. To sa dá napríklad faktorizáciou okruhu $\mathbb{Z}_2[x]$ podľa polynómu x^2+x+1, ktorý je ireducibilný nad $\mathbb{Z}_2$. Prvky $GF_4 = \mathbb{Z}_2[x]/(x^2+x+1)$ sú $\{0, 1, x, x+1\}$. Zostrojme multiplikačné tabuľky pre toto pole:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$*$	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

Očíslujeme prvky poľa GF_4 ako $a_0 = 0, a_1 = 1, a_2 = x, a_3 = x+1$. Teraz už máme všetko potrebné aby sme zostrojili požadované latinské štvorce. Prvý latinský štvorec bude mať prvky $a_{ij}^{(1)} = a_i a_1 + a_j$, pre $i, j \in \{0, 1, 2, 3\}$:

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}$$

Napríklad prvok štvorca v prvom riadku a druhom stĺpci (indexujúc od nuly) je $a_{12}^{(1)} = a_1 a_1 + a_2 = 1 \cdot x + 1 = x + 1 = a_3$. Druhý a tretí štvorec zostrojíme analogicky:

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{pmatrix}$$

Def 1.13. Množina $n-1$ vzájomne ortogonálnych latinských štvorcov rádu n sa nazýva úplná $MOLS(n)$.

Úloha 19. Napíšte program, ktorý pre zadané prvočíslo p zostrojí úplnú $MOLS(n)$.

Úloha 20. Napíšte program, ktorý pre zadané prvočíslo p a číslo α zostrojí úplnú $MOLS(p^\alpha)$.

Veta* 1.9. *(Bose, Parker, Schrickhande, 1960)*

$\forall n \geq 3 \wedge n \neq 6$: *existujú aspoň dva vzájomne ortogonálne latinské štvorce rádu* n.

Poznámka 1.2. Táto veta, má za sebou zaujímavý historický príbeh. Euler sa zaoberal problémom zostrojovania ortogonálnych latinských štvorcov ešte v 18. storočí. Katarína Veľká ho požiadala, aby navrhol ako usporiadať 36 dôstojníkov s 6 hodnosťami zo 6 plukov do štvorca tak, aby v každom riadku a každom stĺpci boli dôstojníci rôznej hodnosti a aj z rôznych plukov. Inými slovami aby zostrojil dva ortogonálne latinské štvorce rádu 6, v jednom by boli usporiadané hodnosti a v druhom pluky dôstojníkov. Ich prekrytie by tvorilo požadované usporiadanie dôstojníkov.

Eulerovi sa tento problém nepodarilo vyriešiť, ale počas svojho bádania navrhol postup pre zostrojovanie dvoch vzájomne ortogonálnych latinských štvorcov rádu n pre nepárne n a n, ktoré je násobkom 4. Popritom odpozoroval, že nie je možné zostrojiť dva vzájomne ortogonálne latinské štvorce rádu 2 a keďže nebol schopný

zostrojiť štvorce rádu 6, tak vyslovil hypotézu, že pre nepárne párne[9] $n \equiv 2 \pmod 4$ neexistujú vzájomne ortogonálne latinské štvorce rádu n.

V roku 1959 sa však podarilo zostrojiť dva vzájomne ortogonálne latinské štvorce rádu 10 pomocou hrubej sily a počítača, čo bolo jedno z prvých použití výpočtovej sily na riešenie matematických problémov. Neskôr v tom roku vydali Bose, Parker a Schrickhande článok, v ktorom dokázali, že vzájomne ortogonálne latinské štvorce existujú pre každé $n > 1$ okrem $n = 2$ a $n = 6$. Týmto definitívne vyvrátili Eulerovu hypotézu.

Euler teda spozoroval výnimku na dvoch prípadoch a mylne ju generalizoval na všetky nepárne párne rády štvorcov. No vyvrátiť jeho hypotézu trvalo približne 200 rokov.

Def 1.14. Nech $A \in \mathbb{R}^{n\times m}$ a $B \in \mathbb{R}^{p\times q}$ sú matice ľubovoľnej veľkosti. Potom matica $A \otimes B \in \mathbb{R}^{np\times mq}$ je Kronekerovym súčinom matíc A a B, ak platí:

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nm}B \end{bmatrix}$$

Príklad 1.3. Kroneckerov súčin môže byť napríklad:

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} 1\begin{bmatrix} 1 & 1 \\ -1 & 2 \end{bmatrix} & 2\begin{bmatrix} 1 & 1 \\ -1 & 2 \end{bmatrix} & 3\begin{bmatrix} 1 & 1 \\ -1 & 2 \end{bmatrix} \\ 4\begin{bmatrix} 1 & 1 \\ -1 & 2 \end{bmatrix} & 5\begin{bmatrix} 1 & 1 \\ -1 & 2 \end{bmatrix} & 6\begin{bmatrix} 1 & 1 \\ -1 & 2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 2 & 2 & 3 & 3 \\ -1 & 2 & -2 & 4 & -3 & 6 \\ 4 & 4 & 5 & 5 & 6 & 6 \\ -4 & 8 & -5 & 10 & -6 & 12 \end{bmatrix}$$

Veta* 1.10. *(Vlastnosti Kronekerovho súčinu)*

1. $(A \otimes B)^T = A^T \otimes B^T$
2. $(A + B) \otimes C = A \otimes C + B \otimes C$
3. $(AB) \otimes (CD) = (A \otimes C)(B \otimes D)$

Veta 1.11. $|MOLS(n_1)| \geq m \wedge |MOLS(n_2)| \geq m \Rightarrow |MOLS(n_1 n_2)| \geq m$

Konštrukcia. k-tý latinský štvorec rádu $n_1 n_2$ sa dá získať pomocou Kroneckerovho súčinu k-tých príslušných latinských štvorcov rádu n_1 a n_2.

Formálne, nech $l_1, \ldots, l_m$ sú ortogonálne latinské štvorce rádu n_1 a $l'_1, \ldots, l'_m$ sú ortogonálne latinské štvorce rádu n_2. Potom množina matíc $\{l_k \otimes l'_k \mid k \leq m\}$, kde $\otimes$ je Kroneckerov súčin matíc, je množina ortogonálnych latinských štvorcov rádu $n_1 n_2$.

Overenie správnosti tejto konštrukcie prenechávame čitateľovi ako samostatné cvičenie (úloha 21).

Dôsledok 1.11.1.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \Rightarrow |MOLS(n)| \geq \min_{i\leq r}(p_i^{\alpha_i} - 1)$$

Úloha 21. Dokážte správnosť konštrukcie z vety 1.11.

[9] Viac o nepárne párnych číslach sa dá dočítať na `https://en.wikipedia.org/wiki/Singly_and_doubly_even`

Veta 1.12.

$$n = 2m - 1 \Rightarrow |MOLS(n)| \geq 2$$

Konštrukcia. Pohybujeme sa v cyklickej grupe $(\mathbb{Z}_n, +) = \{0, \ldots, n-1\}$.

$$A := (a_{ij}),\ a_{ij} := m(i+j)\ (mod\ n)$$
$$B := (b_{ij}),\ b_{ij} := (i-j)\ (mod\ n)$$

Overenie správnosti tejto konštrukcie prenechávame čitateľovi ako samostatné cvičenie (úloha 22).

Úloha 22. Dokážte správnosť konštrukcie z vety 1.12.

1.3 Traverzály

Traverzála latínskeho štvorca je taký výber n políčok, že v každom riadku je vybraté práve jedno políčko, v každom stĺpci je vybraté práve jedno políčko a každý symbol je obsiahnutý v práve jednom políčku.

Def 1.15. Nech $A := (a_{ij})$ je latinský štvorec veľkosti n. n-tica $\{(i_1, j_1), (i_2, j_2), \ldots, (i_n, j_n)\}$ je traverzála latínskeho štvorca A p. v. k. $\{a_{i_1 j_1}, a_{i_2 j_2}, \ldots, a_{i_n j_n}\} = \{i_1, i_2, \ldots, i_n\} = \{j_1, j_2, \ldots, j_n\} = \{1, 2, \ldots, n\}$

Úloha 23. Nájdite jeden latinský štvorec, ktorý má traverzálu a jeden, ktorý nemá traverzálu.

Úloha 24. Nech $A := (a_{ij}), a_{ij} = i + j$ je latinský štvorec veľkosti n. Ukážte, že A nemá traverzálu.

Veta 1.13. *Nech $A := (a_{ij}), B := (b_{ij})$ sú kolmé latinské štvorce veľkosti n, $c \in \{1, 2, \ldots, n\}, T = \{(i, j) | a_{ij} = c\}$. Potom T je traverzála štvorca B.*

Dôkaz. Keďže A je latinský štvorec, tak platí, že veľkosť T je n a pre každé dva rôzne prvky $(i_1, j_1), (i_2, j_2) \in T$ platí $i_1 \neq i_2, j_1 \neq j_2$ z čoho vyplýva $\{i_1, i_2, \ldots, i_n\} = \{j_1, j_2, \ldots, j_n\} = \{1, 2, \ldots, n\}$.

Keďže A a B sú na seba kolmé, tak $b_{i_k j_k}$ a $b_{i_l j_l}((i_k, j_k), (i_l, j_l) \in T, (i_k, j_k) \neq (i_l, j_l))$ musia byť rôzne a teda $\{b_{i_1 j_1}, b_{i_2 j_2}, \ldots b_{i_n j_n}\} = \{1, 2, \ldots, n\}$. □

Dôsledok 1.13.1. *Latinský štvorec veľkosti n má kolmú dvojičku, práve vtedy keď sa dá pokryť n traverzálami.*

Kapitola 2

Blokové plány

Blokové plány sú kombinatorické štruktúry, pre ktoré existuje veľa využití v štatistike, dizajne experimentov, teórii kódovania, teórii grafov a ďalších oblastiach. Napríklad aj pri dizajne spoločenských hier :) Populárna hra Dobble je vlastne blokový plán, kde jednotlivé karty sú bloky a symboly na kartách sú objekty.

2.1 Symetrické blokové plány

Def 2.1. Nech $X =\subseteq x_1, \ldots, x_v$ je množina objektov a $\mathcal{B} = \{X_1, \ldots, X_v\} \subset \mathcal{P}(X)$ je množina podmnožín objektov (tieto podmnožiny voláme *bloky*), pričom sú splnené nasledujúce podmienky:

1. $|X_i| = k$ pre $i = 1, 2, \ldots, v$;
2. $|X_i \cap X_j| = \lambda$ pre $i \neq j$;
3. $0 < \lambda < k < v - 1$.

Potom systém blokov $\mathcal{B}$ voláme (v, k, λ) - *konfigurácia* (alebo symetrický blokový plán).

Def 2.2. Maticou incidencie (v, k, λ) - konfigurácie voláme $0, 1$-maticu $A = (a_{ij})$, kde $a_{ij} = 1$ práve vtedy, keď $x_j \in X_i$, inak $a_{ij} = 0$.

Veta 2.1. *Označme I jednotkovú maticu*[1] *rádu v a J maticu pozostávajúcu zo samých jednotiek rádu v. Ukážeme si teraz sériu vlastností (v, k, λ) - konfigurácie s maticou incidencie A, ktoré nám pomôžu v dokázaní ekvivalencie duálneho pohľadu na blokové plány.*

1. $AJ = kJ$
2. $AA^T = \lambda J + (k - \lambda)I$
3. $\det(AA^T) = (\det(A))^2 = (k + \lambda(v - 1))(k - \lambda)^{v-1}$
4. $k(k - 1) = \lambda(v - 1)$
5. $JA = kJ$
6. $AA^T = A^T A$

[1] jednotková matica je matica, ktorá má na diagonále jednotky a mimo diagonály nuly

Dôkaz. Dokážeme postupne jednotlivé body.

1. $AJ = kJ$.
   Riadok i matice A popisuje, ktoré objekty tvoriace i-ty blok. Všetky objekty v i-tom bloku sú zastúpené v i-tom riadku matice A jednotkami, ostatné objekty sú zastúpené nulami. Keďže každý blok má k prvkov a maticu J tvoria samé jednotky. Tak prvok matice AJ vznikne ako súčet k jednotiek a $v-k$ núl, teda každý prvok výslednej matice má hodnotu k a $AJ = kJ$.

2. $AA^T = \lambda J + (k-\lambda)I$.
   Prvok AA^T na pozícii i, j označme $c_{i,j}$ potom $c_{i,j} = \sum_{l=1}^{v} a_{il}a_{jl}$. Keďže a_{pq} je jedna v prípade, že $x_q \in X_p$, inak $a_{pq} = 0$, tak súčin $a_{il}a_{jl} = 1$ ak $x_l \in X_i \cap X_j$, inak $a_{il}a_{jl} = 0$. Z toho vyplýva, že:

   $$c_{ij} = |X_i \cap X_j| = \begin{cases} k & i = j \\ \lambda & i \neq j \end{cases}$$

   Teda:

   $$AA^T = \begin{pmatrix} k & \lambda & \dots & \lambda \\ \lambda & \ddots & & \vdots \\ \vdots & & \ddots & \lambda \\ \lambda & \dots & \lambda & k \end{pmatrix} = \lambda J + (k-\lambda)I.$$

3. $\det(AA^T) = (\det(A))^2 = (k + \lambda(v-1))(k-\lambda)^{v-1}$.

   $$\det(AA^T) = \begin{vmatrix} k & \lambda & \dots & \lambda \\ \lambda & \ddots & & \vdots \\ \vdots & & \ddots & \lambda \\ \lambda & \dots & \lambda & k \end{vmatrix} = \begin{vmatrix} k & \lambda-k & \lambda-k & \vdots & \lambda-k \\ \lambda & k-\lambda & 0 & \vdots & 0 \\ \vdots & 0 & k-\lambda & \vdots & \vdots \\ \vdots & 0 & \vdots & \vdots & 0 \\ \lambda & 0 & 0 & \vdots & k-\lambda \end{vmatrix} =$$

   $$\begin{vmatrix} \lambda(v-1)+k & 0 & \dots & \dots & 0 \\ \lambda & k-\lambda & 0 & \vdots & 0 \\ \vdots & 0 & k-\lambda & \vdots & \vdots \\ \vdots & 0 & \vdots & \vdots & 0 \\ \lambda & 0 & 0 & \vdots & k-\lambda \end{vmatrix} =$$

   $$(\lambda(v-1)+k)\begin{vmatrix} k-\lambda & 0 & 0 & \dots & 0 \\ 0 & k-\lambda & 0 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & \dots & 0 & k-\lambda \end{vmatrix} = (\lambda(v-1)+k)(k-\lambda)^{v-1}$$

4. $k(k-1) = \lambda(v-1)$.
   Vychádzajme z rovnosti $AA^T = \lambda J + (k-\lambda)I$. Ďalej počítajme:

   $$AA^T = \lambda J + (k-\lambda)I \quad /\dot{J}$$

   $$AA^T J = \lambda J^2 + (k-\lambda)J = \lambda v J + (k-\lambda)J = (k + \lambda(v-1))J$$

Pretože $0 < \lambda < k$ je podľa 3 matica A regulárna a podľa 1 platí $A^{-1}J = \frac{1}{k}J$. Z toho a rovnosti $AA^TJ = (k+\lambda(v-1))J$ vyplýva $A^TJ = (k+\lambda(v-1))A^{-1}J$

$$A^TJ = \frac{k+\lambda(v-1)}{k}J \quad /\text{transponujeme}$$

$$(A^TJ)^T = \frac{k+\lambda(v-1)}{k}J^T$$

$$J^TA^{TT} = \frac{k+\lambda(v-1)}{k}J^T$$

$$JA = \frac{k+\lambda(v-1)}{k}J \quad /\dot{J}$$

$$JAJ = \frac{v}{k}(k+\lambda(v-1))J$$

Ďalej z 1 vieme, že $AJ = kJ$, teda $JAJ = kJ^2 = vkJ$. Z toho vyplýva, že $vkJ = \frac{v}{k}(k+\lambda(v-1))J$ a teda $k = \frac{k+\lambda(v-1)}{k}$, čo je ekvivalentné s $k^2-k = \lambda(v-1)$ a teda $k(k-1) = \lambda(v-1)$.

5. $JA = kJ$.
   Trochu upravíme naspäť vlastnosť 4:

$$k(k-1) = \lambda(v-1)$$

$$k-1 = \frac{\lambda(v-1)}{k}$$

$$k = \frac{k+\lambda(v-1)}{k}$$

   Tiež vieme, že $A^TJ = \frac{k+\lambda(v-1)}{k}J$, nahradíme $\frac{k+\lambda(v-1)}{k}$ za k, čím dostaneme $A^TJ = kJ$. Transponovaním dostaneme $J^TA = kJ^T$ a pretože J je symetrická, tak $J^T = J$ a teda $JA = kJ$.

6. $AA^T = A^TA$.
   Túto vlastnosť dokážeme priamo pomocou ekvivalentných úprav a vlastností, ktoré sme už dokázali.

$$AA^T = A^{-1}AA^TA \overset{2}{=} A^{-1}(\lambda J + (k-\lambda)I)A = \lambda A^{-1}JA + (k-\lambda)A^{-1}IA =$$

$$\lambda A^{-1}JA+(k-\lambda)I \overset{5}{=} \lambda A^{-1}kJ+(k-\lambda)I \overset{1}{=} \lambda A^{-1}AJ+(k-\lambda)I = \lambda J+(k-\lambda)I = AA^T$$

□

Poznámka 2.1. Tvrdenie z vlastnosti 5 sa dá ekvivalentne zapísať ako $\sum_{i=1}^{v} a_{ij} = k$, inými slovami súčet prvkov v stĺpci matice A je k, teda každý objekt je obsiahnutý v k blokoch. Podobne z vlastnosti 6 vyplýva, že:

$$\sum_{i=1}^{v} a_{ij}a_{il} = \begin{cases} k & i = j \\ \lambda & i \neq j \end{cases}$$

Čiže každá dvojica rôznych objektov sa vyskytuje v presne λ blokoch.

Týmto sme dokázali dualitu: Ľubovoľná dvojica blokov má práve k objektov spoločných, ak sú objekty rovnaké a práve λ objektov spoločných, ak sú rôzne. Duálne: Ľubovoľná dvojica objektov je obsiahnutá v presne k blokoch, ak sú objekty rovnaké a práve λ blokoch, ak sú rôzne.

Teda existuje dualita medzi pojmami objekt a blok.

2.2 Definícia, základné vlastnosti

Pojem symetrického blokového plánu vieme zovšeobecniť na blokové plány, kde sú mohutnosti množiny blokov a množiny objektov rôzne. Definujeme všeobecnejší pojem blokového plánu a ukážeme si niektoré vlastnosti.

Def 2.3. Vyvážený nekompletný blokový plán (angl. *balanced incomplete block design*) $BIBD(v, b, r, k, \lambda)$ je usporiadaná dvojica $(X, \mathcal{B})$, kde X je množina objektov a $\mathcal{B} \subset \mathcal{P}(X)$ je množina podmnožín objektov (tieto podmnožiny voláme *bloky*), pričom sú splnené nasledujúce podmienky:

1. $v = |X|$ je mohutnosť množiny objektov.
2. $b = |\mathcal{B}|$ je mohutnosť množiny blokov.
3. každý blok má mohutnosť k.
4. každý objekt je obsiahnutý v práve r blokoch.
5. každá dvojica objektov sa vyskytuje v práve λ blokoch.

Poznámka 2.2. Z definície vidno, že ak položíme $b = v$, získame symetrický blokový plán definovaný podľa duálneho pohľadu zo záveru predchádzajúcej podkapitoly.

Veta 2.2. *$\exists BIBD(v, b, r, k, \lambda) \iff$ λ-násobný kompletný multigraf rádu v λK_v sa dá rozložiť na b hranovo disjunktných klík rádu k (K_k).*

Dôkaz. Množina objektov X zodpovedá množine vrcholov multigrafu. Výskyt dvojice objektov v bloku zodpovedá hrane v multigrafe. Samotné bloky zodpovedajú kompletným klikám.

Formálna konštrukcia je z toho očividná. □

Veta 2.3. *Nech existuje $BIBD(v, b, r, k, \lambda)$. Potom:*

1. $vr = bk$
2. $\lambda(v - 1) = r(k - 1)$

Úloha 25. Dokážte vetu 2.3. *Hint: prvá rovnosť vyjadruje celkový počet bodov vo všetkých blokoch (s opakovaním), druhá rovnosť vyjadruje celkový počet hrán pre jeden vrchol v zodpovedajúcom multigrafe.*

Dôsledok 2.3.1. *Preto namiesto značenia $BIBD(v, b, r, k, \lambda)$ budeme často používať značenie $BIBD(v, k, \lambda)$, nakoľko zvyšné parametre vieme dorátať:*

$$r := \frac{\lambda(v-1)}{k-1}, \; b := \frac{\lambda v(v-1)}{k(k-1)}$$

Veta 2.4. *Nech existuje $BIBD(v, b, r, k, \lambda)$, kde $X = \{x_1, x_2, \ldots, x_v\}$ a $\mathcal{B} = \{B_1, \ldots, B_b\}$. Nech matica incidencie $A \in \{0, 1\}^{v \times b}$ je matica typu $v \times b$, kde $A_{ij} = 1$ práve vtedy, keď $x_i \in B_j$. Potom $AA^T = (r - \lambda)I_v + \lambda J_v$, kde I_v je matica identity rádu v a J_v je matica jednotiek typu $v \times v$.*

Dôkaz. Pozrieme sa na jednotlivé políčka matice AA^T:

$$(AA^T)_{ik} = \sum_{j=1}^{b}(A)_{ij}(A^T)_{jk} = \sum_{j=1}^{b}(A)_{ij}(A)_{kj} = \sum_{j=1}^{b}[x_i \in B_j][x_k \in B_j] = \sum_{j=1}^{b}[x_i \in B_j \wedge x_k \in B_j]$$

Slovne povedané, políčko $(AA^T)_{ik}$ sa rovná počtu blokov, kde sa naraz vyskytujú prvky x_i a x_k. V prípade, že $i = k$, $(AA^T)_{ik} = r$, nakoľko sa v blokovom pláne každý prvok vyskytuje v práve r blokoch. V opačnom prípade $(AA^T)_{ik} = \lambda$, nakoľko sa každá dvojica prvkov v blokovom pláne vyskytuje v práve λ blokoch.

Čiže matica AA^T má na diagonále číslo r a mimo diagonály číslo λ, čo presne vyjadruje vzorec $AA^T = (r - \lambda)I_v + \lambda J_v$. □

Lema 2.5. *Nech A je matica incidencie blokového plánu $BIBD(v, b, r, k, \lambda)$. Potom* $\det(AA^T) = (r - \lambda)^{v-1}(v\lambda - \lambda + r)$.

Dôkaz. Z lineárnej algebry vieme[2], že determinant matice je súčinom všetkých jej vlastných čísel (s násobnosťami). Takže treba nájsť všetky vlastné čísla matice $AA^T = (r - \lambda)I_v + \lambda J_v$. Číslo x je vlastným číslom matice M práve vtedy keď je riešením rovnice $\det(M - xI) = 0$. Napíšeme si túto rovnicu pre maticu AA^T:

$$\det((r - \lambda - x)I_v + \lambda J_v) = 0$$

Ak $r - \lambda - x = 0$, tak celá matica v determinante má hodnosť 1, čiže $x = r - \lambda$ je $(v - 1)$-násobným vlastným číslom matice AA^T. Čiže zostáva nájsť ešte jedno vlastné číslo násobnosti 1. Z toho vyplýva, že po dosadení x do rovnosti by sme dostali maticu hodnosti $(v - 1)$, čiže jediným prejavom lineárnej závislosti je lineárna kombinácia všetkých riadkov matice. Po chvíli rozmýšľania nás môže napadnúť rovnosť $(r - \lambda - x) = -v\lambda$, čím docielime, že súčet čísel v každom stĺpci je nula. Teda, číslo $x = r - \lambda + v\lambda$ je vlastným číslom matice AA^T s násobnosťou 1.

Z toho vyplýva, že $\det(AA^T) = (r-\lambda)^{v-1}(r-\lambda+v\lambda)$, čím je dôkaz ukončený. □

Dôsledok 2.5.1. *Ak $BIBD(v, b, r, k, \lambda)$ je blokový plán a $b = v$, tak matica incidencie A je regulárna a matici A^T tiež zodpovedá nejaký blokový plán.*

Veta 2.6. *(Fisherova nerovnosť) Nech existuje blokový plán $BIBD(v, b, r, k, \lambda)$. Potom $b \geq v$.*

Dôkaz. Zjavne $r \geq \lambda$, lebo sa každý prvok v rámci dvojice vyskytuje v práve λ blokoch, čiže aj počet výskytov každého prvku samostatne musí byť aspoň λ. Rozoberieme teraz dva prípady: $r = \lambda$ a $r > \lambda$.

Nech $r = \lambda$. Pozorujme prvok $x \in X$. BUNV sa prvok x nachádza v blokoch $B_1, \ldots, B_r$. Keďže sa každá dvojica (x, y) vyskytuje práve r krát, tak sa každý prvok $y \in X$ musí nachádzať v blokoch $B_1, \ldots, B_r$. Čiže, bloky $B_1, \ldots, B_r$ majú mohutnosť v, čiže $b = v$, čím je požadované tvrdenie dokázané.

Nech teraz $r > \lambda$. Potom z lemy 2.5 matica AA^T je regulárna, čiže $rank(AA^T) = v$. Z lineárnej algebry vieme, že hodnosť matíc je aspoň tak veľká ako hodnosť ich súčinu, t.j. $rank(A) \geq rank(AA^T) = v$. Na druhej strane, matica A je typu $v \times b$, čiže $b \geq rank(A)$. Syntézou dvoch nerovností dostaneme $b \geq rank(A) \geq v$, čím je dôkaz ukončený. □

Dôsledok 2.6.1. *Nech existuje blokový plán $BIBD(v, b, r, k, \lambda)$. Potom $r \geq k$.*

[2]respektíve *už* vieme :)

2.3 Cyklické blokové plány a diferenčné množiny

Def 2.4. Množina $D = \{d_1, \ldots, d_k\} \subsetneq \mathbb{Z}_v$ mohutnosti $k < v$ sa volá (v, k, λ)-diferenčnou množinou, ak pre každý nenulový prvok $a \in \mathbb{Z}_v$ existuje práve λ usporiadaných dvojíc $(d_i, d_j) \in D^2$ takých, že $d_i - d_j \equiv a \mod v$.

Poznámka 2.3. Množina $\{0, 1, 3\}$ je $(7, 3, 1)$-diferenčnou množinou.

Poznámka 2.4. Podobným spôsobom je možné definovať diferenčné množiny nad konečnými grupami rádu v.

Úloha 26. Nájdite bez pomoci počítača ďalšie dve $(7, 3, 1)$-diferenčné množiny.

Úloha 27. Napíšte program, ktorý overí, či zadaná na vstupe množina je (v, k, λ)-diferenčnou množinou pre nejaké parametre v, k, λ.

Úloha 28. Napíšte brute-force program na generovanie diferenčných množín so zadanými parametrami v, k, λ[3].

Lema 2.7. *Nech pre dané v, k a λ existuje (v, k, λ)-diferenčná množina. Potom platí*

$$k(k-1) = \lambda(v-1).$$

Dôsledok 2.7.1. *Pre každú (v, k, λ)-diferenčnú množinu platí $\lambda > k$.*

Def 2.5. Nech $D = \{d_1, \ldots, d_k\}$ je množina, a nech a je prirodzené číslo. Potom množinu $\{a + d_1, \ldots, a + d_k\} =: a + D$ voláme *transláciou* množiny D.

Lema 2.8. *Všetky translácie jednej diferenčnej množiny sú navzájom rôzne.*

Dôkaz. Nech je daná (v, k, λ)-diferenčná množina $D = \{d_1, \ldots, d_k\}$. Sporom, nech existuje dvojica rovnakých translácií. BUNV nech sú to D a $a + D$ pre nejaké nenulové a.

To je ekvivalentné existencii k-prvkovej permutácii $\phi \in S_k$ takej, že

$$\forall i \in \{1, \ldots, k\} : a = d_i - d_{\phi(i)}.$$

Čiže, pre daný nenulový prvok a existuje aspoň k spôsobov ako ho vyjadriť ako rozdiel dvoch čísel z diferenčnej množiny D. Teda platí, že $\lambda \leq k$, čo je spor s dôsledkom 2.7.1. □

Def 2.6. (v, k, λ)-BIBD je cyklický, ak existuje permutácia s cyklom dĺžky v taká, že zachováva bloky[4]. Formálne, blokový plán je cyklický, ak existuje permutácia $\phi \in S_v$ s cyklom dĺžky v taká, že

$$\mathcal{B} = \{\{\phi(x_1), \ldots, \phi(x_k)\} \mid \{x_1, \ldots, x_k\} \in \mathcal{B}\}$$

Veta 2.9. *Množina $D = \{d_1, \ldots, d_k\}$ je (v, k, λ)-diferenčná množina práve vtedy, keď $(X, \mathcal{B})$, kde $X = \mathbb{Z}_v$ a $\mathcal{B} = \{D + i \mid \forall i \in \mathbb{Z}_v\}$ ($D + i := \{d_1 + i, \ldots, d_k + i\}$), je cyklický (v, k, λ)-BIBD.*

Dôkaz. Dokazovať túto vetu budeme po implikáciách.

[3] na bežných strojoch jednoduchý program v Pythone zvláda generovať diferenčné množiny s parametrom $v \leq 25$ do niekoľkých sekúnd

[4] bijektívne zobrazenia množiny na ňu samu, ktoré zachovávajú vzťahy medzi objektami, sa všeobecne nazývajú *automorfizmy*

dif. množina $\Longrightarrow$ blokový plán: Treba ukázať, že dvojica $(\mathbb{Z}_v, \mathcal{B})$ spĺňa definíciu (v, k, λ)-BIBD a zároveň definíciu cyklickosti z definície 2.6. Cyklickosť blokov množiny $\mathcal{B}$ je zrejmá z jej definície, zodpovedajúcim automorfizmom je cyklický posun o jeden.

Definícia blokového plánu má päť podmienok, z toho prvé tri triviálne platia. Z vety 2.3 vyplýva, že v danom prípade $r = k$. Čiže ostáva dokázať dve tvrdenia: každý bod je obsiahnutý v práve k blokoch a každá dvojica bodov sa vyskytuje v práve λ blokoch.

Každý bod je obsiahnutý v práve k blokoch: Každé číslo $a \in \mathbb{Z}_v$ sa vyskytne práve v blokoch $(a - d_1) + D, (a - d_2) + D, \ldots, (a - d_k) + D$ postupne ako obraz čísel $d_1, d_2, \ldots, d_k$ v príslušnej translácii množiny D.

Každá dvojica bodov sa vyskytuje v práve λ blokoch: pre každú dvojicu rôznych čísel (a, b) z definície diferenčnej množiny existuje práve λ dvojíc $(i_1, j_1), \ldots, (i_\lambda, j_\lambda)$ takých, že $d_{i_1} - d_{j_1} = \ldots = d_{i_\lambda} - d_{j_\lambda} = a - b$, takže dvojica (a, b) sa určite vyskytuje v blokoch $(d_{i_1} - a) + D, \ldots, d_{i_\lambda} - a) + D$.

Zároveň platí, že ak sa dvojica (a, b) vyskytuje v bloku $x + D$, tak musí existovať taká dvojica bodov $(d_i + x, d_j + x)$, že $d_i + x = a$ a $d_j + x = b$, čiže $d_i - d_j = a - b$. Z toho vyplýva, že dvojica bodov (a, b) sa vyskytuje v práve λ blokoch.

Týmto je dôkaz tejto implikácie ukončený.

blokový plán $\Longrightarrow$ dif. množina: Dôkaz tejto implikácie prenechávame čitateľovi ako samostatné cvičenie (úloha 29). □

Úloha 29. Dokážte druhú implikáciu z vety 2.9.

Def 2.7. Nech F je konečné pole. Nech $V \cong F^{n+1}$ je vektorový priestor dimenzie $n + 1$ nad poľom F. Definujeme reláciu $\sim$ nad prvkami $V^* := V - \left\{\vec{0}\right\}$:

$$\forall \vec{a}, \vec{b} \in V^* : \left(\vec{a} \sim \vec{b} \overset{def}{\iff} \exists k \in F : \vec{a} = k\vec{b}\right)$$

Potom rozklad V^* na triedy ekvivalencie $\mathbb{P}^n(V) := {}^{V^*}\!/_{\sim}$ je n-rozmerná projektívna rovina nad F.

Projektívnu rovinu dimenzie n nad konečným poľom s $q = p^r$ prvkami označujeme ako $PG(n, q) := \mathbb{P}^n\left(\mathbb{Z}_p^r\right)$

Veta* 2.10. *(Typ S dif. množín — Singerove dif. množiny)*
Nech množina D obsahuje všetky nadroviny konečnej projektívnej roviny $PG(n, q)$ (nadrovina je faktorový obraz vektorového podriestoru dimenzie n). Potom D je (v, k, λ)-diferenčná množina s parametrami:

$$v = \frac{q^{n+1} - 1}{q - 1}, \quad k = \frac{q^n - 1}{q - 1}, \quad \lambda = \frac{q^{n-1} - 1}{q - 1}$$

Veta* 2.11. *(Typ Q dif. množín — kvadratické rezíduá, angl.* Paley-type*)*
Nech $F := GF(p^l)$ je konečné pole mohutnosti p^l, kde $p^l \equiv 3 \mod 4$. Nech $r \in F$ je generátor grupy $F^* := (F - \{0\}, *)$. Potom množina kvadratických rezíduí grupy F^* $QR(F^*) := \left\{r^a \mod p^l \mid a \in \left\{0, \ldots, p^l - 1\right\} \wedge a \text{ je párne}\right\}$ je (v, k, λ)-diferenčnou množinou s parametrami:

$$v = p^l = 4t - 1, \quad k = 2t - 1, \quad \lambda = t - 1$$

Veta* 2.12. *(Typ B dif. množín — bikvadratické rezíduá)*
Nech $F := GF(q)$ je konečné pole, kde $q = p^l$ a $p = 4x^2 + 1$ pre nepárne x. Nech r je generátor grupy $F = (GF(q), +)$. Potom množina bikvadratických rezíduí grupy F $BQR(F) := \{TODO\}$ je (v, k, λ)-diferenčnou množinou s parametrami:

$$v = p = 4x^2 + 1, \quad k = x^2, \quad \lambda = \frac{x^2 - 1}{4}$$

Veta* 2.13. *(Typ T dif. množín — Twin prime power dif. množiny)*
Nech je množina D v grupe $((GF(q), +) \times (GF(q+2), +), +)$, kde q aj $q+2$ sú mocniny prvočísel, definovaná nasledovne $D = \{(x, y) \mid y = 0$ alebo x aj y sú nenulové a oba sú súčasne štvorce alebo súčasne neštvorce$\}$. Potom D je (v, k, λ)-diferenčná množina s parametrami:

$$v = q^2 + 2q, \quad k = \frac{q^2 + 2q - 1}{2}, \quad \lambda = \frac{q^2 + 2q - 3}{4}$$

2.4 Hadamardove matice

Hadamardove matice sú štvorcové matice s prvkami ± 1, ktorých riadky stĺpce sú navzájom ortogonálne. Vďaka svojim vlastnostiam, z ktorých si niektoré predstavíme v tejto časti, sú užitočné vo viacerých oblastiach matematiky a informatiky. V štatistike sa používajú na odhad štatistickej odchýľky[5]. Asi najvýznamnejšie využitie je v teórii kódovania na konštrukciu samoopravných kódov a spracovania signálu. Napríklad v 70. rokoch boli využité na prenos fotiek Marsu z vesmírnej sondy *Mariner 9* späť na Zem[6].

Def 2.8. Matica $H \in \{-1, +1\}^{n \times n}$ je Hadamardovou maticou rádu n, ak $HH^T = nI_n$ (t.j. všetky riadky sú navzájom ortogonálne).

Veta 2.14. *Nech matica H je Hadamardova matica rádu n. Potom platí:*

1. *výmenou riadkov (stĺpcov) matice H dostaneme Hadamardovu maticu*
2. *vynásobením riadku (stĺpca) matice H číslom -1 dostaneme Hadamardovu maticu*
3. *matica H je normálna, t.j. $HH^T = H^T H$*

Dôkaz. Prvé dve tvrdenia vieme dokázať jednoduchým pozorovaním priamo z definície. Označme si riadkové vektory matice H ako $H_1, \ldots, H_n$. Rovnosť $HH^T = nI_n$ vieme ekvivalentne zapísať ako skalárny súčin vektorov H_i a H_j:

$$H_i \cdot H_j = \begin{cases} n & i = j \\ 0 & i \neq j \end{cases} \qquad \sum_{l=0}^{n} h_{i,l} h_{j,l} = \begin{cases} n & i = j \\ 0 & i \neq j \end{cases}$$

Je zrejmé, že táto rovnosť je invariantná voči zmene poradia riadkov a stĺpcov aj prenásobeniu riadka (stĺpca) číslom -1.

Tretie tvrdenie sa dá odvodiť pomocou zopár jednoduchých ekvivalentných maticových úprav.

[5] Viac o tejto metóde sa dá dočítať na wikipédii `https://en.wikipedia.org/wiki/Balanced_repeated_replication`

[6] Opäť viac sa dá dočítať na wikipédii `https://en.wikipedia.org/wiki/Hadamard_code`

Kľúčové pozorovanie je, že matice s ortogonálnymi riadkami (stĺpcami)[7] matice sú vždy regulárne, čiže majú inverznú maticu (pre Hadamardovu maticu H je to matica $n^{-1}H^T$). Pre nás však je dôležité, že násobenie regulárnou maticou pre maticové rovnice je ekvivalentnou úpravou[8].

$$\begin{aligned} HH^T &\stackrel{?}{=} H^TH && \text{vynásobiť zľava regulárnou maticou } H \\ H(HH^T) &\stackrel{?}{=} (HH^T)H && \text{asociativita a definícia H. matíc} \\ HnI_n &\stackrel{?}{=} nI_nH && \text{...} \\ H &\stackrel{\checkmark}{=} H \end{aligned}$$

Teda, pomocou ekvivalentných úprav sme sa dostali od pôvodného tvrdenia ku triviálne platnému, čiže aj pôvodné tvrdenie je nutne platné. □

Použitím prvých dvoch tvrdení vieme ľahko previesť ľubovoľnú Hadamardovu maticu do tvaru, kedy prvý riadok aj prvý stĺpec obsahujú iba jednotky. Tento tvar budeme nazývať *normálny tvar* Hadamardovej matice.

Def 2.9. Hadamardova matica je v normálnom tvare, ak prvý riadok aj prvý stĺpec obsahujú iba hodnoty +1.

Veta 2.15. *Nech H je Hadamardova matica rádu n. Potom* $\det H = \sqrt{n^n}$.

Úloha 30. Dokážte vetu 2.15 *(hint: z definície Hadamardovej matice).*

Veta* 2.16. *(Hadamardov odhad)*
Nech $M \in \mathbb{C}^{n\times n}$ je komplexná matica typu $n \times n$, kde $|(M)_{ij}| \leq 1$. Nech H je ľubovoľná Hadamardova matica rádu n. Potom platí:

$$\det M \leq \det H = \sqrt{n^n}$$

Veta 2.17. *Ak H je Hadamardova matica rádu n, tak n je buď* 1, 2 *alebo násobok* 4.

Dôkaz. Nech $n \geq 4$. BUNV Hadamardova matica H je v normálnom tvare. Pozrieme sa na prvé tri riadky matice H, a špeciálne na ich stĺpcové vektory. Stĺpcové vektory prvých troch riadkov Hadamardovej matice v normálnom tvare môžu byť štyroch typov:
$\begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\-1\end{pmatrix}, \begin{pmatrix}1\\-1\\1\end{pmatrix}$ a $\begin{pmatrix}1\\-1\\-1\end{pmatrix}$.
Označme si ich počty ako x, y, z a w a indexy stĺpcov daného typu ako I_1, I_2, I_3 a I_4. Súčet počtov všetkých typov sa musí rovnať počtu stĺpcov, t.j. $x+y+z+w = n$. Ďalej z vlastností Hadamardovej matice vyplýva, že všetky tri riadky sú navzájom kolmé. Rozpísaním skalárnych súčinov dvojíc riadkov dostaneme nasledovné rovnice:

$$h_1 \perp h_2 \iff \sum_i h_{1i}h_{2i} = 0 \iff \sum_{i\in I_1} 1 + \sum_{i\in I_2} 1 + \sum_{i\in I_3}(-1) + \sum_{i\in I_4}(-1) = x+y-z-w = 0$$

$$h_1 \perp h_3 \iff \sum_i h_{1i}h_{3i} = 0 \iff \sum_{i\in I_1} 1 + \sum_{i\in I_2}(-1) + \sum_{i\in I_3} 1 + \sum_{i\in I_4}(-1) = x-y+z-w = 0$$

[7] je nesprávne volať Hadamardovu maticu "ortogonálnou", pretože sa historicky tento pojem vyhradzuje pre matice, ktorých stĺpce sú *ortonormálne*, t.j. sú navzájom ortogonálne a zároveň majú dĺžku 1, t.j. sú normované.

[8] technicky, tento dôkaz sa dá napísať aj bez využitia ekvivalentných úprav, ale bolo by to menej intuitívne. Čitateľ je však vítaný otočiť poradie maticových úprav a tešiť sa z toho.

$$h_2 \perp h_3 \iff \sum_i h_{2i}h_{3i} = 0 \iff \sum_{i\in I_1} 1 + \sum_{i\in I_2}(-1) + \sum_{i\in I_3}(-1) + \sum_{i\in I_4} 1 = x - y - z + w = 0$$

Dostali sme sústavu lineárnych rovníc pre štyri neznáme, jediným riešením ktorej je $x = y = z = w = \frac{n}{4}$, čím je dôkaz tejto vety ukončený. □

Hypotéza 2.1. *(Hadamard)*
$\forall n \in \{1, 2\} \cup \{4k \mid k \in \mathbb{N}\} \implies$ *existuje Hadamardova matica rádu* n.

Veta 2.18. *(Hadamard, Sylvester)*
Ak H, H' *su Hadamardove matice, tak aj* $H \otimes H'$ *je tiež Hadamardova matica (*$\otimes$ *je Kroneckerov súčin matíc).*

Úloha 31. Dokážte vetu 2.18 *(hint: použite vlastnosti Kronekerovho súčinu z vety 1.10 pre overenie podmienok z definície Hadamardovej matice).*

Dôsledok 2.18.1. *Existuje aspoň jedna Hadamardova matica rádu* $n = 2^\alpha$, *pre* $\alpha \in \mathbb{N}$.

Dôkaz. Zoberme maticu $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, ktorá zjavne spĺňa definíciu Hadamardovej matice. Následne pomocou nej a Kronekerovho súčinu zostrojme maticu $H_{2^\alpha} = \underbrace{H_2 \otimes H_2 \otimes \ldots \otimes H_2}_{\alpha-krát}$. □

Dôsledok 2.18.2. *Ak je* H *je Hadamardova matica, tak aj* $\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$ *je Hadamardova matica.*

Dôkaz. Opäť zoberme maticu $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Potom $H_2 \otimes H = \begin{pmatrix} H & H \\ H & -H \end{pmatrix}$ je tiež Hadamardova matica. □

Veta 2.19. *Normalizovaná Hadamardova matica rádu* 4μ *existuje práve vtedy, keď existuje* $(4\mu - 1, 2\mu - 1, \mu - 1)$*-diferenčná množina (typ Q).*

Konštrukcia. Konštrukcia bude prevádzať Hadamardovu maticu na cyklický blokový plán, z vety 2.9 potom vyplýva existencia diferenčnej množiny. Konštrukcia sa dá použiť aj pre opačný smer.

Začneme Hadamardovou maticou radu 4μ v normálnom tvare. Najprv z matice odstránime prvý riadok a prvý stĺpec. Následne vymeníme čísla -1 za 0. Dostaneme tak maticu incidencie $(4\mu - 1, 2\mu - 1, \mu - 1)$-BIBD.

Dôkaz. Z kolmosti riadkov Hadamardovej matice vyplýva, že každý riadok obsahuje presne polovičný počet jednotiek, čiže po odstránení prvého stĺpca ich tam bude presne $2\mu - 1$, t.j. každý prvok sa vyskytuje v práve $k = 2\mu - 1$ blokoch. To isté platí aj pre stĺpce, t.j. každý blok má práve $2\mu - 1$ prvkov.

Pre ľubovoľné dva riadky Hadamardovej matice platí, že sú kolmé, teda sa musia zhodovať na práve 2μ pozíciách, z toho presne polovica sú jednotky (viď dôkaz vety 2.17). Čiže po odstránení prvého stĺpca platí, že majú obidva riadky plus jednotky na presne $\mu - 1$ pozíciách, t.j. $\lambda = \mu - 1$.

Dôkaz platnosti konštrukcie v opačnom smere prenechávame čitateľovi ako samostatné cvičenie (úloha 32). □

Úloha 32. Dokážte platnosť konštrukcie ku vete 2.19 pre druhý smer.

Veta 2.20. *Ak platí, že $n = p^r + 1 \equiv 0 (mod\ 4)$ kde p je nepárne prvočíslo a r je kladné celé čisło tak existuje Hadamardova matica rádu n. Nasledovnú konštrukciu takejto Hadamardovej matice nazývame Paleyho konštrukcia.*

Konštrukcia. Na skonštruovanie Hadamardovej matice využíva táto konštrukcia kvadratické reziduá v konečnom poli $GF(q)$ kde $q = p^r$ a zároveň platí, že $q \equiv 3 \pmod 4$. Kvadratické reziduum je funkcia, ktorá prvku z konečného poľa F priraďuje číslo na základe toho, či je prvok druhou mocninou nejakého prvku. Formálne:

$$\chi(x) = \begin{cases} 0 & x = 0 \\ 1 & \exists y \in F, y \neq 0 : x = y \cdot y \\ -1 & \text{inak} \end{cases}$$

Zadefinujme si teraz Jacobsthalovu maticu ako maticu Q rozmerov $q \times q$. Pričom bude platiť, že $Q_{i,j} = (\chi(i-j))$. Príklad takejto matice pre pole $GF(7)$ uvádzame nižšie:

$$\mathrm{Q} = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 0 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 0 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 0 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 0 & -1 & -1 & 1 \\ 1 & -1 & 1 & 1 & 0 & -1 & -1 \\ -1 & 1 & -1 & 1 & 1 & 0 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

Nech k_q je vektor jednotiek dĺžky q. V tomto momente vieme skonštruovať Hadamardovu maticu rádu $n = q + 1$ takto:

$$H = I + \begin{bmatrix} 0 & k_q \\ k_q^T & Q \end{bmatrix}$$

Veta 2.21. *Konštrukcia Hadamardovej matice rádu 36.*

Konštrukcia. Hadamardovu maticu tohoto rádu vieme získať z latinského štvorca rádu 6. Vezmime si ľubovolný latinský štvorec L, rádu 6:

$$L = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 3 & 2 & 5 & 4 \\ 2 & 4 & 5 & 0 & 3 & 1 \\ 3 & 5 & 4 & 1 & 2 & 0 \\ 4 & 2 & 0 & 5 & 1 & 3 \\ 5 & 3 & 1 & 4 & 0 & 2 \end{bmatrix}$$

Políčka tohto latinského štvorca si teraz prečíslujeme odhora dole, zľava doprava. Konkrétne zadefinujeme funkciu f_L, ktorá usporiadanej dvojici (r, s) reprezentujúcej pozíciu políčka v r-tom riadku a s-tom stĺpci matice L, priradí jeho poradové číslo a to podľa predpisu $f_L((r, s)) = (r-1) \cdot 6 + s$. Ak si teraz zadefinujeme funkciu f_L^{-1} ako inverznú funkciu prevádzajúcu lineárny index naspäť do našej dvojrozmernej reprezentácie, vieme Hadamardovu maticu H rádu 36 skonštruovať nasledovne:

$$H = (h_{ij})$$

$$h_{i,j} = \begin{cases} 1 & \text{ak platí : } a_1 = b_1 \vee a_2 = b_2 \vee L_{a_1 a_2} = L_{b_1 b_2} \\ & \text{kde : } f_L^{-1}(i) = (a_1, a_2), f_L^{-1}(j) = (b_1, b_2) \\ -1 & \text{inak} \end{cases}$$

2.5 Konečné projektívne roviny

Jedna (algebraická) definícia konečnej projektívnej roviny (angl. *finite projective plane*, alebo skrátene FPP) už bola daná v sekcii o diferenčných množinách (definícia 2.7). V tejto sekcii uvedieme iné dve definície: axiomatickú a kombinatorickú.

Def 2.10. (Axiómy konečnej projektívnej roviny)
Pojmy bodu a priamky sú brané ako primitívne pojmy. Relácie "bod leží na priamke" (značíme $p \in l$) a "priamka prechádza bodom" považujeme za primitívne relácie.

Usporiadaná trojica $\pi = (X, \mathfrak{P}, \in)$, kde X je konečná množina bodov, $\mathfrak{P}$ je konečná množina priamok a $\in$ je relácia "patrí" medzi bodmi a priamkami, je konečnou projektívnou rovinou, ak spĺňa nasledujúce axiómy:

PP1: Každými dvomi rôznymi bodmi prechádza **práve 1** priamka.

PP2: Každé dve rôzne priamky majú **práve 1** spoločný bod.

PP3: existujú 4 body vo všeobecnej geometrickej polohe, t.j. žiadnou trojicou z týchto bodov nevedie žiadna priamka.

Veta 2.22. *PP4 (duálna ku tretej axióme)*
V konečnej projektívnej rovine (v zmysle definície 2.10) existujú 4 priamky také, že žiadna trojica z týchto priamok nemá spoločný bod.

Dôkaz. Dokáz prenechávame čitateľovi (úloha 33). □

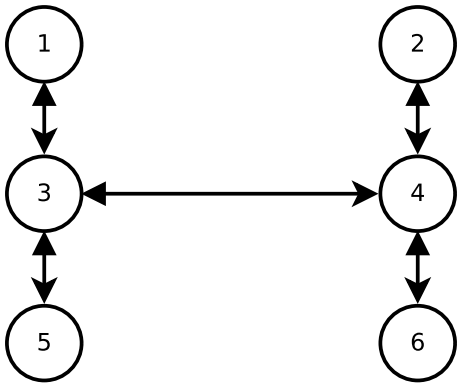
Úloha 33. Dokážte vetu 2.22 *(hint: pozorujte body vo všeobecnej polohe a ich spájajúce priamky).*

Čitateľ si môže všimnúť, že ak vymeníme v danom axiomatickom systéme pojmy "priamka" a "bod", tak dostaneme ekvivalentný systém axióm. Je ľahko nahliadnuť, že ak v ľubovolnom platnom tvrdení o konečných projektívnych rovinách vymeníme tieto pojmy, tak znovu dostaneme platné tvrdenie. Takéto tvrdenia voláme duálne (napríklad, prvá axióma je duálna ku druhej a tretia axióma je duálna ku vete 2.22).

Veta 2.23. *Nech π je konečná projektívna rovina a nech n je prirodzené číslo väčšie alebo rovné 2. Potom nasledujúce tvrdenia sú ekvivalentné:*

1. *každá priamka obsahuje práve $n+1$ bodov*
2. *každý bod leží na práve $n+1$ priamkach (duálne ku 1.)*
3. *nejaká priamka obsahuje práve $n+1$ bodov*
4. *nejaký bod leží na práve $n+1$ priamkach (duálne ku 3.)*
5. *konečná projektívna rovina π má práve n^2+n+1 bodov*
6. *konečná projektívna rovina π má práve n^2+n+1 priamok (duálne ku 5.)*

Dôkaz. Obrázok 2.1 znázorňuje schému dôkazu ekvivalencie týchto šiestich tvrdení. Treba si dávať pozor na to, že "platné" tvrdenie znamená "tvrdenie, odvodené z axiomatického systému PP1 až PP4". Preto neprehlásime duálne tvrdenia ihneď za ekvivalentné, nakoľko napríklad tvrdenie, že počet bodov je presne rovný n^2+n+1 pre nejaké fixné n, sa nedá odvodiť priamo z axiomatického systému. Na druhej strane, duálne implikácie sa dajú prehlásiť za ekvivalentné ihneď.



Obr. 2.1: Schéma dôkazu ekvivalencie tvrdení z vety 2.23

(1) $\Longrightarrow$ (3) **(a duálne** (2) $\Longrightarrow$ (4)**):** Daná implikácia je očividná z dôvodu, že tvrdenie (1) hovorí o *všetkých* priamkach, a tvrdenie (3) o existencii *aspoň jednej* takej priamky.

(3) $\Longrightarrow$ (4) **(a duálne** (4) $\Longrightarrow$ (3)**):** Nech existuje priamka L s presne $n+1$ bodmi $Q_1, \dots Q_{n+1}$. Z PP3 vyplýva, že musí existovať bod mimo priamky L, označme si ho P. Z PP1 potom musia existovať $n+1$ priamok spájajúcich body $Q_1, \dots Q_{n+1}$ s bodom P. Čiže bodom P prechádza aspoň $n+1$ priamok. Ostáva už len dokázať, že cez daný bod neprechádza žiadna ďalšia priamka.

Sporom, nech existuje priamka K, prechádzajúca bodom P. Z PP2 musí mať práve jeden spoločný bod s priamkou L. Sú tu dve možnosti: buď spoločným bodom priamok L a K je jeden z bodov $Q_1, \dots Q_{n+1}$ alebo je to nejaký iný bod na priamke L. V prvom prípade by došlo ku porušeniu PP2, keďže cez dva rôzne body P a Q_i by museli prechádzať dve rôzne priamky. V druhom prípade by došlo ku porušeniu pôvodného predpokladu, že priamka L má práve $n+1$ bodov.

V skutočnosti sme práve dokázali silnejšie tvrdenie: *bodom, ležiacim mimo priamky, ktorá má m bodov, prechádza práve m priamok* (a aj duálne ku nemu tvrdenie: *priamka, neobsahujúca bod, ktorým prechádza m priamok, obsahuje práve m bodov*).

(3) $\Longrightarrow$ (1) **(a duálne** (4) $\Longrightarrow$ (2)**):** Nech existuje priamka L s presne $n+1$ bodmi $Q_1, \dots Q_{n+1}$. Z PP3 existujú štyri body A, B, C a D vo všeobecnej polohe, čiže aspoň dva z nich neležia na priamke L. BUNV sú to A a B. Nakoľko dané body neležia na priamke L, prechádza cez ne práve $n+1$ priamok (viď tvrdenie dokázané vyššie). Z toho vyplýva, že každá priamka, neobsahujúca A alebo B, prechádza práve $n+1$ bodmi. Ostáva už len dokázať, že aj priamka, spájajúca body A a B, má tiež presne $n+1$ bodov.

Priamka AC neobsahuje v sebe bod B (lebo body A, B, C a D sú vo všeobecnej polohe), čiže tiež má presne $n+1$ bodov. Bod D neleží na priamke AC, čiže im prechádza práve $n+1$ priamok. Taktiež, bod D neleží na priamke AB, čiže priamka AB má presne $n+1$ bodov.

(3) $\Longrightarrow$ (5) **(a duálne** (4) $\Longrightarrow$ (6)**):** Nech existuje priamka L s $n+1$ bodmi $Q_1, \dots Q_{n+1}$ a bod P mimo tejto priamky (analogicky s predchádzajúcimi úvahami). Tvrdíme, že všetky body roviny sú obsiahnuté na priamkach $L, Q_1P, \dots Q_{n+1}P$. Sporom, nech existuje bod R mimo týchto priamok. Potom musí existovať priamka RP, ktorá by porušila počet priamok, ktoré prechádzajú cez bod P.

Máme už dokázanú implikáciu (3) $\Longrightarrow$ (1), takže platí, že všetky priamky majú práve $n+1$ bodov. Priamky $Q_1P, \dots Q_{n+1}P$ majú spoločný bod P, čiže z PP2 zvyšné body musia mať rôzne. Z toho už ľahko dopočítame celkový počet bodov: $(n+1)(n)+1 = n^2+n+1$.

(5) $\Longrightarrow$ (3) **(a duálne** (6) $\Longrightarrow$ (4)**):** Nech projektívna rovina má presne n^2+n+1 bodov. Vezmime si niektorú priamku a označme počet jej bodov ako $m+1$. Potom, z už dokázanej implikácie (3) $\Longrightarrow$ (5) vyplýva, že projektívna rovina má práve m^2+m+1 bodov. Z toho plynie, že $m = n$, čím je dôkaz ukončený. □

Def 2.11. (Kombinatorická definícia FPP)
Konečná projektívna rovina rádu n je $BIBD(v, k, \lambda)$ s parametrami:

$$v = n^2+n+1, k = n+1, \lambda = 1$$

Veta 2.24. *Kombinatorická a axiomatická definície konečnej projektívnej roviny sú ekvivalentné.*

Úloha 34. Dokážte vetu 2.24.

Def 2.12. Matica $C = (c_{ij})$ typu $n \times m$, kde $n \geq 4, m \geq 4$ a $c_{ij} \in \{1, \dots, n\}$, má latinskú vlastnosť, ak ľubovoľná podmatica z dvoch stĺpcov matice C nemá rovnaké riadky. Formálne,

$$\forall (i,j) \neq (k,l) : (c_{ij}, c_{il}) \neq (c_{jk}, c_{jl})$$

Navyše, ak podmatica matice C, tvorená prvými dvomi stĺpcami, obsahuje postupne všetky dvojice čísel $\{1, \dots, n\}$ v lexikografickom poradí, tak ju voláme matica s latinskou vlastnosťou v normálnom tvare.

Lema 2.25. *Nech $n \geq 3, t \geq 2$. Potom množina t navzájom ortogonálnych latinských štvorcov rádu n existuje práve vtedy, keď existuje matica typu $n^2 \times (t+2)$ s latinskou vlastnosťou v normálnom tvare.*

Konštrukcia. Nech máme maticu typu $n^2 \times (t+2)$ s latinskou vlastnosťou v normálnom tvare. Potom stĺpec $i+2$ udáva po riadkoch hodnoty políčok i-tého latinského štvorca. Prevod z množiny ortogonálnych latinských štvorcov ku matici s latinskou vlastnosťou je z toho očividný.

Dôkaz. Nech máme maticu M typu $n^2 \times (t+2)$ s latinskou vlastnosťou v normálnom tvare. Treba overiť, že konštrukciou zostrojené matice sú latinskými štvorcami a potom či sú aj ortogonálne. Prvé dva stĺpce matice M obsahujú všetky usporiadané dvojice z $\{1, \dots, n\}^2$. V normálnom tvare zodpovedajú súradniciam v latinských štvorcoch, na ktoré sa umiestnia hodnoty z príslušného riadku.

Porovnaním prvého a $(i+2)$-ého stĺpca matice M z latinskej vlastnosti plynie, že v i-tom skonštruovanom štvorci na každom riadku sú zastúpené všetky hodnoty z množiny $\{1, \dots, n\}$. Podobne, porovnaním druhého a $(i+2)$-ého stĺpca matice M plynie to isté aj pre stĺpce i-tého skonštruovaného štvorca. Čiže nami vykonštruované matice spĺňajú definíciu latinských štvorcov.

Ortogonalita i-tého a j-tého latinských štvorcov plynie priamo z porovnania príslušných stĺpcov $i+2$ a $j+2$ matice M (viď definíciu ortogonality 1.8).

Dôkaz opačného smeru konštrukcie je z toho už zrejmý. □

Veta 2.26. *Existencia konečnej projektívnej roviny rádu n je ekvivalentná s existenciou $(n-1)$ navzájom ortogonálnych latinských štvorcov rádu n.*

Konštrukcia. Nech existuje konečná projektívna rovina radu n. Potom z vety 2.23 má n^2+n+1 bodov a priamok. Označme si priamky $\mathbb{X}_1$ až $\mathbb{X}_{n^2+n+1}$. Označme si body na priamke $\mathbb{X}_1$ ako x_1 až x_{n+1} a body mimo priamky ako y_1 až y_{n^2}. Označme si priamky, odlišné od $\mathbb{X}_1$, na ktorých leží bod x_i ako $L_{i,1}$ až $L_{i,n}$.

Definujme si maticu C typu $n^2 \times (n+1)$ tak, že $C_{i,j} = k \iff y_i \in L_{j,k}$. Potom matica C má latinskú vlastnosť a z nej vieme podľa konštrukcie z lemy 2.25 zostrojiť množinu $(n-1)$ ortogonálnych latinských štvorcov radu n.

Konštrukcia pre opačný smer je z toho už zrejmá.

Dôkaz. Treba ukázať že nami definícia matice C je korektná v zmysle, že pre každé i a j existuje práve jedno vhodné k (z PP1), a že takto skonštruovaná matica má latinskú vlastnosť. Technické detaily dôkazu ponechávame čitateľovi ako samostatné cvičenie 35. □

Úloha 35. Dokážte správnosť konštrukcie z vety 2.26.

Dôsledok 2.26.1. *Ak n je mocninou prvočísla, tak existuje konečná projektívna rovina rádu n.*

Dôkaz. Nech n je mocninou prvočísla. Potom z vety 1.8 vyplýva existencia $n-1$ navzájom ortogonálnych latinských štvorcov radu n, z čoho podľa vety 2.26 vyplýva existencia konečnej projektívnej roviny radu n. □

Hypotéza 2.2. *Ak existuje konečná projektívna rovina rádu n, tak n je mocninou prvočísla.*

Veta* 2.27. *(Desarguesova[9] veta)*
Ak dva trojuholníky sú umiestnené na (euklidovskej) rovine tak, že priamky, spájajúce príslušné dvojice vrcholov, prechádzajú spoločným bodom, tak tri body, v ktorých sa pretínajú predĺženia (t.j. priamky) troch dvojíc príslušných strán trojuholníkov, sú kolineárne (viď obrázok 2.2).

2.6 Steinerovské systémy trojíc, zovšeobecnenia

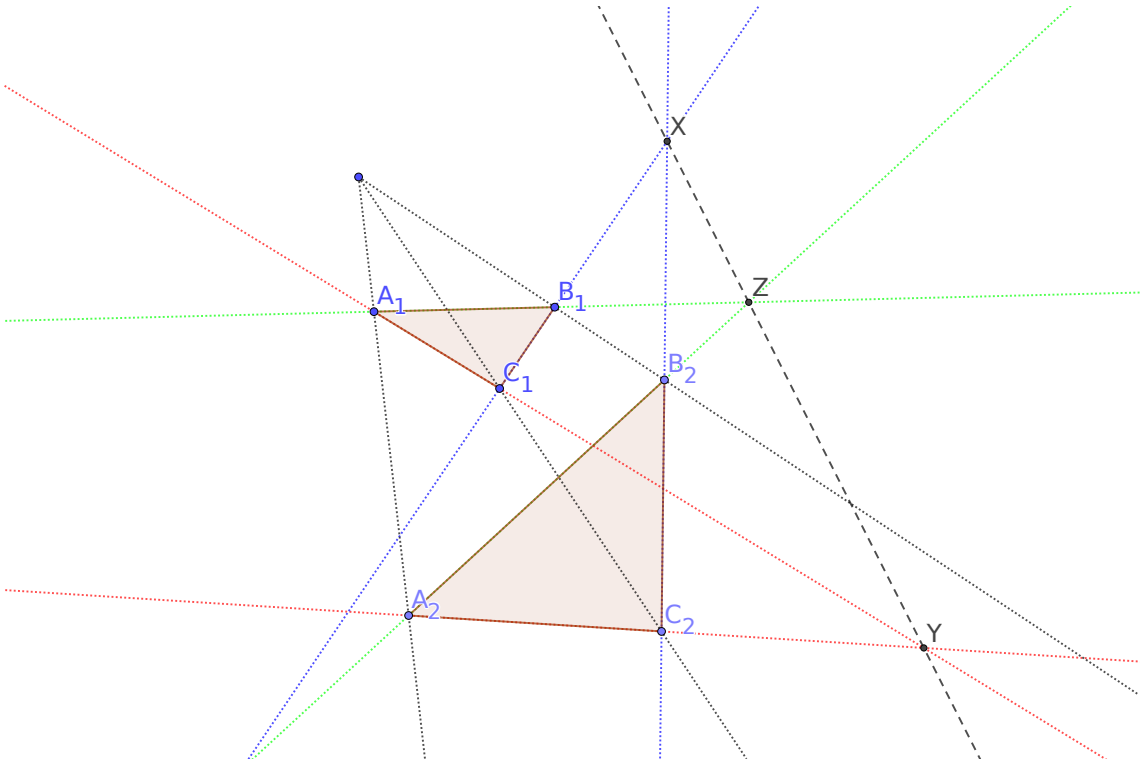
Def 2.13. Blokové plány typu $BIBD(v,3,1)$ sa volajú Steinerovské systémy trojíc (angl. *Steiner triplet system*, skrátene STS).

Poznámka 2.5. Existencia STS je ekvivalentná s existenciou rozkladu kompletného grafu K_v na trojuholníky.

Veta 2.28. *Ak v je počet objektov STS, tak $v \equiv 1 \mod 6$ alebo $v \equiv 3 \mod 6$.*

Dôkaz. Nech je dané STS s v objektmi. Potom existuje rozklad kompletného grafu K_v na trojuholníky. Počet hrán v grafe K_v je rovný $\frac{v(v-1)}{2}$. Nakoľko existuje rozklad na trojuholníky, počet hrán je deliteľný tromi, t.j. $6 | v(v-1)$. Každý vrchol má párny stupeň (lebo každý vrchol grafu sa nachádza v nejakom počte dizjunktných trojuholníkov), čiže $2 \nmid v$. Z toho už vyplýva, že $v \equiv 1,3 \mod 6$. □

[9] meno *Desargues* sa číta ako [dezarg]



Obr. 2.2: Ukážka Desarguesovej vety (2.27). Priesečníky príslušných priamok (body X, Y a Z) sú kolineárne.

Veta* 2.29. *(Kirkman)*
Ak v spĺňa podmienky z vety 2.28, tak existuje STS s práve v objektmi.

Veta 2.30. *(Projektívne STS)*
Nech $X := (\mathbb{Z}_2)^{n+1} - \left\{\vec{0}\right\}$ *je množina vektorov vektorového priestoru dimenzie* $n+1$ *nad poľom* $\mathbb{Z}_2$ *bez nulového vektora a* $\mathcal{B} := \left\{\{\vec{x},\vec{y},\vec{z}\} \mid \vec{x}+\vec{y}+\vec{z}=\vec{0}\right\}$. *Potom dvojica* $(X,\mathcal{B})$ *je STS. Alternatívne, množina priamok projektívnej roviny* $PG(2,n)$ *tvorí STS.*

Úloha 36. Dokážte vetu 2.30.

Veta 2.31. *(Afinné STS)*
Nech $X := (\mathbb{Z}_3)^n$ *je množina vektorov vektorového priestoru dimenzie* n *nad poľom* $\mathbb{Z}_3$. *Nech* $\mathcal{B} := \left\{\{\vec{x},\vec{y},\vec{z}\} \mid \vec{x}+\vec{y}+\vec{z}=\vec{0}\right\}$. *Potom dvojica* $(X,\mathcal{B})$ *je STS.*

Úloha 37. Dokážte vetu 2.31.

Veta 2.32. *(Karteziansky súčin STS)*
Nech dvojice $(X,\mathcal{B})$ *a* $(Y,\mathcal{C})$ *sú STS. Potom dvojica* $(X\times Y,\mathcal{D})$, *kde:*

1. $y \in Y, \{b_1,b_2,b_3\} \in \mathcal{B} \Longrightarrow \{(b_1,y),(b_2,y),(b_3,y)\} \in \mathcal{D}$
2. $x \in X, \{c_1,c_2,c_3\} \in \mathcal{C} \Longrightarrow \{(x,c_1),(x,c_2),(x,c_3)\} \in \mathcal{D}$
3. $\{b_1,b_2,b_3\} \in \mathcal{B}, \{c_1,c_2,c_3\} \in \mathcal{C}, \phi \in S_3 \Longrightarrow \left\{(b_1,c_{\phi(1)}),(b_2,c_{\phi(2)}),(b_3,c_{\phi(3)})\right\} \in \mathcal{D}$ *(kde* ϕ *je permutácia veľkosti* 3*)*

Potom $(X\times Y,\mathcal{D})$ *je STS.*

Úloha 38. Dokážte vetu 2.32.

Veta 2.33. *(Vzťah STS a grupoidov)*
Nech $(X, \mathcal{B})$ je STS. Potom množina X s binárnou operáciou $*$, definovanou nasledovne:

$$\begin{aligned} \forall \{x, y, z\} \in \mathcal{B} : \\ x * y = y * x = z \\ x * z = z * x = y \\ y * z = z * y = x \\ x * x = x \end{aligned}$$

je idempotentný komutatívny grupoid.

Dôkaz. Treba ukázať, že binárna operácia je definovaná na každej dvojici prvkov (platí to z definície STS), a že je definovaná jednoznačne (tiež platí z STS). □

Veta 2.34. *($(2v+1)$-konštrukcia STS)*
Nech $(X, \mathcal{B})$ je STS a $(X', \mathcal{B}')$ je jeho disjunktná izomorfná kópia (t.j. $X \cap X' = \varnothing$). Obraz prvku x v tomto izomorfizme budeme značiť x'. Nech prvok $\infty \notin X \cup X'$. Potom dvojica $(Y, \mathcal{C})$, kde $Y := X \cup X' \cup \{\infty\}$ a $\mathcal{C} := \mathcal{B} \cup \{\{x, y', z'\} \mid \{x, y, z\} \in \mathcal{B}\} \cup \{\{x, x', \infty\} \mid x \in X\}$, je STS.

Úloha 39. Dokážte vetu 2.34.

Veta 2.35. *(Wilson-Schreiberova konštrúkcia)*
Nech $n \equiv \pm 1 \pmod 6$ je také celé číslo, že číslo -2 má v grupe $(\mathbb{Z}_n^*, \cdot)$ párny rád. Potom existuje STS rádu $n+2$.

Dôkaz. Uvažujme všetky neusporiadané trojice $\langle a, b, c\rangle$ takých prvkov $\mathbb{Z}_n$, že $a+b+c = 0$. Tieto trojice sú troch typov:

1. $\langle a, b, c\rangle$, a, b, c sú navzájom rôzne,
2. $\langle a, b, c\rangle = \langle a, a, -2a\rangle$,
3. $\langle a, b, c\rangle = \langle 0, 0, 0\rangle$.

Nech multiplikatívny rád čísla -2 modulo n je $2r$. Zoberme dva nové prvky $\beta,\ \gamma \notin Z_n$. Pre fixné $a \in \mathbb{Z}_n - \{0\}$ si zoberme neusporiadané trojice druhého typu

$$\begin{gathered} \langle a, a, -2a\rangle, \\ \langle -2a, -2a, (-2)^2 a\rangle, \\ \langle (-2)^2 a, (-2)^2 a, (-2)^3 a\rangle, \\ \langle (-2)^3 a, (-2)^3 a, (-2)^4 a\rangle, \\ \vdots \\ \langle (-2)^{2r-2} a, (-2)^{2r-2} a, (-2)^{2r-1} a\rangle, \\ \langle (-2)^{2r-1} a, (-2)^{2r-1} a, a\rangle = \langle (-2)^{2r-1} a, (-2)^{2r-1} a, (-2)^{2r} a\rangle. \end{gathered}$$

Pre $i \in \{0, 1, \ldots, r-1\}$, trojicu $\langle (-2)^{2i}a, (-2)^{2i}a, (-2)^{2i+1}a\rangle$ nahradíme trojicou $\langle (-2)^{2i}a, \alpha, (-2)^{2i+1}a\rangle$ a trojicu $\langle (-2)^{2i+1}a, (-2)^{2i+1}a, (-2)^{2i+2}a\rangle$ nahradíme trojicou $\langle (-2)^{2i}a, \alpha, (-2)^{2i+1}a\rangle$. Dostaneme teda trojice typu

$$\begin{aligned}
\langle a, a, -2a\rangle &\to \langle a, \alpha, -2a\rangle,\\
\langle -2a, -2a, (-2)^2a\rangle &\to \langle -2a, \beta, (-2)^2a\rangle,\\
\langle (-2)^2a, (-2)^2a, (-2)^3a\rangle &\to \langle (-2)^2a, \alpha, (-2)^3a\rangle,\\
\langle (-2)^2a, (-2)^2a, (-2)^3a\rangle &\to \langle (-2)^2a, \beta, (-2)^3a\rangle,\\
&\vdots\\
\langle (-2)^{2r-2}a, (-2)^{2r-2}a, (-2)^{2r-1}a\rangle &\to \langle (-2)^{2r-2}a, \alpha, (-2)^{2r-1}a\rangle,\\
\langle (-2)^{2r-1}a, (-2)^{2r-1}a, a\rangle &\to \langle (-2)^{2r-1}a, \beta, a\rangle.
\end{aligned}$$

Pokiaľ nám ostala ešte nejaká trojica $\langle b, b, -2b\rangle$ typu 2, tento postup s ňou zopakujeme, pokým všetky trojice typu dva takto nenahradíme. Nakoniec trojicu $\langle 0, 0, 0\rangle$ nahradíme trojicou $\langle 0, \alpha, \beta\rangle$. Všetky trojice typu 1 ponecháme. Všetky nové trojice obsahujú tri rôzne prvky, už len ukážeme, že tvoria STS $(X, \mathcal{B})$ s nosnou množinou $X = \mathbb{Z}_n \cup \{\alpha, \beta\}$.

Zoberme si ľubovoľnú dvojicu prvkov $a,\ b \in X$. Ak $\{a, b\} = \{\alpha, \beta\}$, tak sa $\{a, b\}$ nachádza v práve jednej trojici $\{0, \alpha, \beta\}$. Pokiaľ $a = \alpha$ a $b \in \mathbb{Z}_n$, tak α sa vyskytuje len v trojiciach typu 2. V nich sa b vyskytuje iba v trojiciach $\langle b, b, -2b\rangle$ a $\langle (-2)^{-1}b, (-2)^{-1}b, b\rangle$. Práve jednu z nich sme prerobili na trojicu obsahujúcu α, b. Prípad $a = \beta$, $b \in \mathbb{Z}_n$ je podobný.

Pokiaľ $a \neq b \in \mathbb{Z}_n$, tak nech $c = -a - b$. Pokiaľ $a \neq c \neq b$, tak $\{a, b, c\}$ je jediná trojica obsahujúca $\{a, b\}$. Inak BUNV $c = a$. Potom $b = -2a$ a prvky a a $-2a$ sa nachádzajú spolu v práce jednej trojici spolu s buď α, alebo β. □

Veta* 2.36. *Wilson-Schreiberova konštrúkcia (všeobecnejšia)*
Nech $n \equiv \pm 1 \pmod 6$ *a nech* A *je Abelovská grupa rádu* n*, v ktorej* -2 *má párny multiplikatívny rád. Potom existuje STS rádu* $n + 2$*.*

Táto veta využíva, že každá Abelovská grupa sa dá zapísať (vzhľadom na izomorfizus) ako súčin cyklických grúp. Pomocou nich možno definovať -2 ako $(-2, -2, \ldots, -2)$, násobenie a multiplikatívny rád.

Veta* 2.37. *(Boseova konštrúkcia STS)*
Nech je daná idempotentná komutatívna kvazigrupa $(Q, \cdot)$ *radu* $2n + 1$*. Nech* $X := Q \times \mathbb{Z}_3$*. Nech*

$$B_1 := \bigcup_{x \in Q} \{(x, 0), (x, 1), (x, 2)\}$$

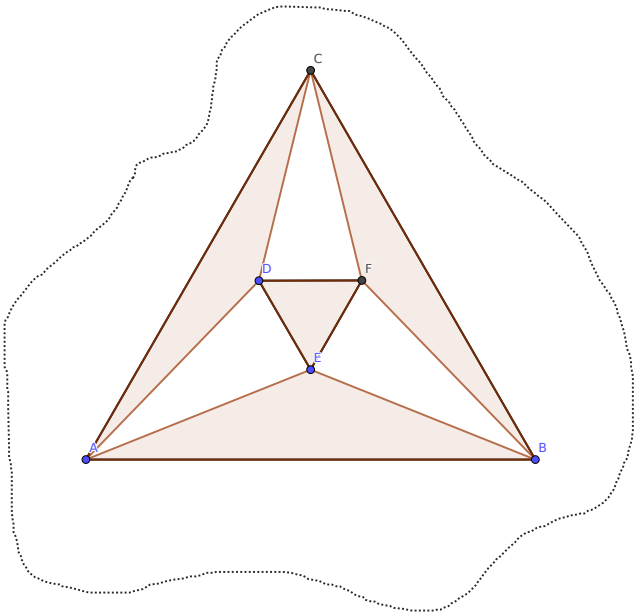
a

$$B_2 := \bigcup_{\substack{x,y \in Q,\\ x \neq y}} \bigcup_{i \in \mathbb{Z}_3} \{(x, i), (y, i), (x \cdot y, (i + 1) \pmod 3)\}.$$

Potom $(X, B_1 \cup B_2)$ *je STS.*

Veta* 2.38. *(Paschovo prepnutie)*
Ak v STS máme 6 bodov a 4 bloky "jednej farby" (podľa obrázku 2.3), tak vieme tieto bloky nahradiť zvyšnými a zachovať STS.

TODO Skolemova konštrukcia
TODO Cyklické STS



Obr. 2.3: Ukážka Paschovho prepnutia (veta 2.38). Ak v nejakej STS 4 farebné bloky vymeníme za 4 biele, tak nová štruktúra bude zase STS.

Def 2.14. Dvojica $(X, \mathcal{B})$, kde $\mathcal{B} \in \mathcal{P}(X)$, je $t-(v,k,\lambda)$-blokový plán (angl. *t-design*), ak:

- $|X| = v$
- $\forall B \in \mathcal{B} : |B| = k$
- každá t-tica objektov z X sa vyskytuje v práve λ blokoch z $\mathcal{B}$

Navyše, blokové plány typu $t-(v,k,1)$ budeme označovať ako $S(t,k,v)$.

Poznámka 2.6. Existencia $t-(v,k,\lambda)$-blokového plánu je ekvivalentná s existenciou rozkladu t-uniformného λ-násobného hypergrafu na hyperklíky veľkosti k.

Poznámka 2.7. STS s v prvkami môžeme značiť ako $S(2,3,v)$.

Def 2.15. Blokové plány $S(3,4,v)$ voláme Steinerovské systémy štvoríc (angl. *SQS*)

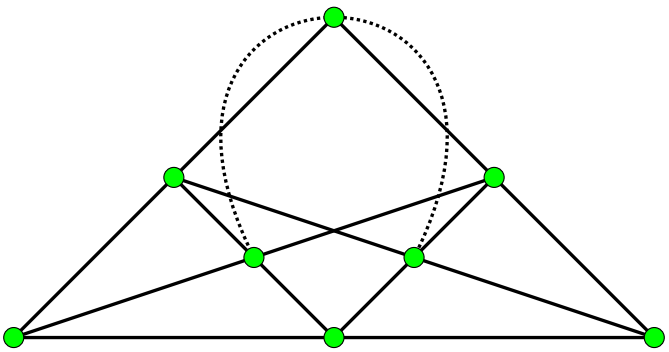
Veta* 2.39. $\exists S(3,4,v) \iff v \equiv 3,4 \mod 6$

Def 2.16. Blokové plány $S(4,5,v)$ voláme Steinerovské systémy pätíc

Veta* 2.40. $\exists S(4,5,v) \implies v \equiv 4,5 \mod 6 \wedge v \not\equiv 4 \mod 5$

2.7 Symetrické konfigurácie

Def 2.17. Konfigurácia je množina bodov a priamok, píšeme (v_γ, l_π), kde v je počet bodov, l je počet priamok, γ je počet priamok prechádzajúcich každým bodom a π je počet bodov na každej priamke.



Obr. 2.4: Konfigurácia Mobius-Kantor (zdroj obrázku: Wikipedia)

Def 2.18. Konfigurácia je symetrická, ak platí $\gamma = \pi$ (a teda nutne aj $v = l$). Vtedy konfiguráciu píšeme skratene ako (v_γ).

Def 2.19. Čiastočný Steinerovský systém $S_p(v, k, t)$ je množina k-prvkových podmnožín (blokov) v-prvkovej množiny bodov taká, že každá t-prvková podmonožina bodov sa nachádza v najviac jednom bloku.

Konfigurácie (v_3) voláme symetrické v_3-konfigurácie.

Lema 2.41. *Symetrická v_3-konfigurácia je $S_p(v, 3, 2)$.*

Dôkaz. Priamo z definície čiastočného Steinerovského systému. Bloky interpretujeme ako priamky. Dva body jednoznačne určujú priamku, preto $t = 2$. □

Úloha 40. Presvedčte sa, že Fanova rovina (viď obr. 3.1) je symetrická 7_3-konfigurácia.

Úloha 41. Konfigurácia Möbius-Kantor
Presvedčte sa, že afínna geometria AG(2,3) bez jedného bodu a priamok ktoré prechádzajú tým bodom (viď obr. 2.4) je symetrická 8_3-konfigurácia.

Úloha 42. Pappusova konfigurácia
Presvedčte sa, že konfigurácia použitá v Pappusovej vete (viď obr. 2.5) je symetrická 9_3-konfigurácia.

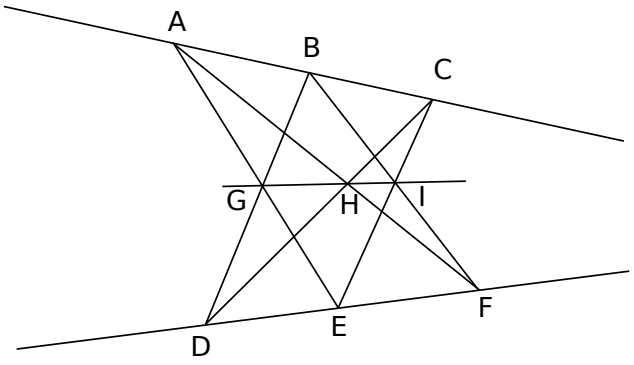
Úloha 43. Desarguesová konfigurácia
Presvedčte sa, že Desaurgová konfigurácia (viď obr. 2.2) je symetrická 10_3-konfigurácia.

Úloha 44. Konfigurácia Cremona-Richmond
Presvedčte sa, že konfigurácia Cremona-Richmond (viď obr. 2.6) je symetrická 15_3-konfigurácia.

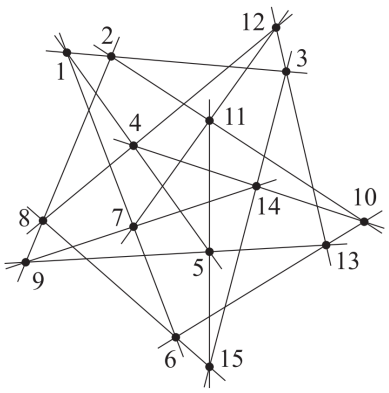
Hypotéza 2.3. *Fulkerson*
Každý bezmostový kubický graf má 6 1-faktorov takých, že každá hrana grafu leží v práve 2 z nich.

Ľahko sa dá nahliadnúť, že konfigurácia Cremona-Richmond v ktorej sú body dvojprvkové podmnožiny množiny $\{1, 2, \ldots, 6\}$ a priamky sú trojice takýchto bodov sa dá použiť na sformulovanie Fulkersonovej vety. Hranám v grafe pridelíme bod z konfigurácii a vrcholom v grafe priradíme priamky (bloky) z konfigurácii.

[10]Boben, M., Grunbaum, B., Pisanski, T., & Zitnik, A. (2006). Small triangle-free configurations of points and lines. Discrete & Computational Geometry, 35(3), 405-427.



Obr. 2.5: Pappusova konfigurácia



Obr. 2.6: Konfigurácia Cremona-Richmond[10]

2.8 Konečné jednoduché grupy

Def 2.20. Grupa G sa nazýva jednoduchá, ak $|G| > 1$ a pre každú jej normálnu podgrupu H platí $|H| = 1$ alebo $H = G$.

Def 2.21. Grupa G je konečná, ak má konečný počet prvkov, teda $|G| = n$, $n \in \mathbb{N}$.

.

2.8.1 Klasifikácia konečných jednoduchých grúp

Dôležitou otázkou v teórii grúp bolo ako popísať všetky konečné jednoduché grupy. Nasledovná teoréma bola úplne dokázaná v roku 2004. Dôkaz bol publikovaný na desiatky tisíc strán po častiach od roku 1955[11].

Veta* 2.42. *Každá konečná jednoduchá grupa je izomorfná s jednou z nasledovných grúp:*

- *cyklická grupa $\mathbb{Z}_p$, kde p je prvočíslo*
- *alternujúca grupa A_n, kde $n \geq 5$*
- *projektívna špeciálna lineárna grupa $PSL(2, q)$, kde q je mocnina prvočísla*
- *niektorá z grúp Lie typu*
- *niektorá z 26 sporadických grúp*[12]
- *Titsova grupa ${}^2F_4(2)'$*

Naznačíme ako sú sporadické Mathieu[13] grupy prepojené so Steinerovskými systémami. Existuje 5 grúp tohoto typu:

- Grupe M_{11} zodpovedá grupa automorfizmov $S(4, 5, 11)$, píšeme $Aut(S(4, 5, 11))$
- Grupe M_{12} zodpovedá $Aut(S(5, 6, 12))$
- Grupe M_{22} zodpovedá podgrupa indexu 2 grupy $Aut(S(3, 6, 22))$, teda $M_{22} \triangleleft_2 Aut(S(3, 6, 22))$
- Grupe M_{23} zodpovedá $Aut(S(4, 7, 23))$
- Grupe M_{24} zodpovedá $Aut(S(5, 8, 24))$

[11] Tento dôkaz vynecháme zo skrípt :)

[12] 20 z 26 týchto grúp spolu tvoria *šťastnú rodinku* v ktorej sú okrem iných grúp aj grupa monštrum M a grupa bábätko monštrum B :)

[13] francúzsky matematik Émile Léonard Mathieu

Kapitola 3

Matroidy

3.1 Definícia, základné pojmy

Def 3.1. Dvojica $(X, \mathcal{N})$, kde $\mathcal{N} \subseteq \mathcal{P}(X)$ a $\mathcal{N}$ je konečná, je matroid, ak sú splnené nasledujúce podmienky:

1. $\varnothing \in \mathcal{N}$
2. $N \in \mathcal{N} \wedge N' \subseteq N \Longrightarrow N' \in \mathcal{N}$
3. $N, N' \in \mathcal{N} \wedge |N| < |N'| \Longrightarrow \exists x \in N' - N : N \cup \{x\} \in \mathcal{N}$

Množiny z $\mathcal{N}$ voláme nezávislé množiny. Množiny mimo $\mathcal{N}$ voláme závislé.

Veta 3.1. *(Matroid z vektorového priestoru)*
Nech $V_n(F) \cong F^n$ je vektorový priestor dimenzie $n < \infty$ nad (nie nutné konečným) poľom F. Nech $(\vec{x}_1, \ldots, \vec{x}_r)$ je postupnosť (nie nutné rôznych) vektorov z $V_n(F)$. Nech $X := \{1, \ldots, r\}$, $\mathcal{N} := \{Q \mid Q \subseteq X \wedge \{\vec{x}_i \mid i \in Q\}$ je nezávislá v $V_n(F)\}$. Potom dvojica $(X, \mathcal{N})$ je matroid.

Dôkaz. Treba postupne overiť všetky tri podmienky z definície matroidu.

$\varnothing \in \mathcal{N}$**:** Prázdna množina vektorov je (lineárne) nezávislá, takže patrí do množiny $\mathcal{N}$.

$N \in \mathcal{N} \wedge N' \subseteq N \Longrightarrow N' \in \mathcal{N}$**:** Podmnožina (lineárne) nezávislej množiny vektorov je tiež (lineárne) nezávislá.

$N, N' \in \mathcal{N} \wedge |N| < |N'| \Longrightarrow \exists x \in N' - N : N \cup \{x\} \in \mathcal{N}$**:** Sporom, nech $\forall x \in N' - N : N \cup \{x\} \notin \mathcal{N}$, čiže množina vektorov $N \cup \{x\}$ je vždy (lineárne) závislá. Potom platí, že vektor x sa dá vyjadriť ako lineárna kombinácia zvyšných vektorov v tejto množine. To znamená, že každý vektor z $N' - N$ sa dá vyjadriť ako lineárna kombinácia vektorov z N.

Z toho vyplýva, že dimenzia lineárneho obalu množiny N' nie je väčšia ako dimenzia lineárneho obalu množiny N. Nakoľko obidve množiny N a N' sú (lineárne) nezávislé, tak ich mohutnosti sú rovné dimenziám príslušných lineárnych obalov. Potom $|N| \geq |N'|$, čo je spor. □

Veta 3.2. *(Matroid z grafu)*
Nech $G = (V, E)$ je jednoduchý graf. Nech $X := E$. Nech množina hrán $A \subseteq E$ patrí do množiny $\mathcal{N}$ práve vtedy, keď indukovaný graf neobsahuje kružnice. Potom dvojica $M(G) = (X, \mathcal{N})$ je matroid.

Dôkaz. Schéma dôkazu je totožná s predošlou vetou, ponechávame preto tento dôkaz ako samostatné cvičenie (úloha 45). □

Úloha 45. Dokážte vetu 3.2.

Def 3.2. Nech $M = (X, \mathcal{N})$ je matroid a nech $A \subseteq X$. Množinu $B \subseteq A$ voláme bázou množiny A v matroide M, ak je to maximálna (na inklúziu) nezávislá množina v A. Formálne, B je bázou A v matroide $M = (X, \mathcal{N})$, ak:

$$B \subseteq A \wedge B \in \mathcal{N} \wedge (\forall B' \supset B : B' \subseteq A \Longrightarrow B' \notin \mathcal{N})$$

Špeciálne, bázy množiny X voláme bázy matroidu. Množinu báz matroidu M značíme ako $\mathcal{B}$.

Veta 3.3. *Nech $(X, \mathcal{N})$ je matroid a $A \subseteq X$. Nech N, N' sú bázy množiny A. Potom $|N| = |N'|$.*

Dôkaz. Sporom, nech mohutnosti báz N a N' sú rôzne. BUNV, $|N| < |N'|$. Potom z tretej vlastnosti matroidov (definícia 3.1) vyplýva, že existuje prvok $x \in N' - N \subseteq A$ taký, že $N \cup \{x\} \in \mathcal{N}$. To je však spor s tvrdením, že množina N je bázou, t.j. maximálnou na inklúziu nezávislou podmnožinou A. □

Def 3.3. Nech $(X, \mathcal{N})$ je matroid. Hodnosťou množiny $A \subseteq X$ voláme veľkosť nejakej bázy B množiny A a značíme ako $r(A) := |B|$.

Veta 3.4. *Nech $(X, \mathcal{N})$ je matroid a $r : \mathcal{P}(X) \to \mathbb{N}_0$ je jeho hodnostná funkcia. Potom platí:*

1. $r(\varnothing) = 0$
2. $r(\{x\}) \leq 1$
3. $A \subseteq B \Longrightarrow r(A) \leq r(B)$
4. $r(A \cup B) \leq r(A) + r(B) - r(A \cap B)$ *(semimodularita)*

Navyše, ak nejaká funkcia $r' : \mathcal{P}(X) \to \mathbb{N}_0$ spĺňa vyššie uvedené podmienky, tak existuje jediný matroid, ktorého hodnostnou funkciou je práve r'.

Dôkaz. Prvé tri vlastnosti hodnostnej funkcie sú triviálne na dokazovanie, sústrediť sa budeme na štvrtú vlastnosť.

Nech I je bázou množiny $A \cap B$. Nech $I' \supseteq I$ je bázou množiny $A \cup B$, obsahujúca množinu I (pomocou tretej vlastnosti[1] z definície matroidov). Keďže každá podmnožina nezávislej množiny musí byť tiež nezávislá (druhá vlastnosť z definície matroidov), tak $|I' \cap (A \cap B)| \leq |I|$ (keďže I je maximálna nezávislá množina v $A \cap B$). Keďže I' (z definície) obsahuje I, tak platí $I' \cap (A \cap B) = I$.

Ďalej platí, že $|I' \cap A| \leq r(A)$ a $|I' \cap B| \leq r(B)$, nakoľko $I' \cap A$ a $I' \cap B$ sú nezávislé (z druhej vlastnosti matroidov), ale nie nutné maximálne v príslušných podmnožinách.

Použitím pravidla zapojenia a vypojenia na množiny $A \cap I'$ a $B \cap I'$ dostaneme:

$$|(A \cup B) \cap I'| = |A \cap I'| + |B \cap I'| - |A \cap B \cap I'|.$$

[1] túto techniku budeme používať aj neskôr

Využitím vyššie odvodených faktov po dosadení dostaneme:

$$r(A \cup B) \leq r(A) + r(B) - r(A \cap B).$$

Konštrukcia matroidu pomocou hodnostnej funkcie: množina $N \subseteq X$ je nezávislá práve vtedy, keď jej mohutnosť je zhodná s jej hodnosťou, formálne $\mathcal{N} := \{N \in X \mid r(N) = |N|\}$. Overenie správnosti tejto konštrukcie prenechávame ako samostatné cvičenie (úloha 46).

spravit dokaz

□

Úloha 46. Dokážte správnosť konštrukcie z vety 3.4.

Veta 3.5. *Nech $(X, \mathcal{N})$ je matroid a $\mathcal{B}$ je množina jeho báz. Potom platí:*

B1: žiadne 2 prvky množiny $\mathcal{B}$ nie sú v inklúzii

B2: $B, B' \in \mathcal{B} \Longrightarrow \forall x \in B - B'\ \exists y \in B' - B : (B - \{x\}) \cup \{y\} \in \mathcal{B}$

Navyše, ak množina $\mathcal{B}'$ spĺňa vyššie uvedené podmienky B1 a B2, tak existuje jediný matroid, ktorého množinou báz je práve $\mathcal{B}'$.

Dôkaz. Prvá vlastnosť triviálne plynie z definície bázy. Druhú vlastnosť budeme dokazovať priamo. Nech množiny B a B' sú bázy a nech $x \in B - B'$. Množina $(B - \{x\}) \cup B'$ má maximálnu hodnosť, nakoľko je nadmnožinou bázy B': $r((B - \{x\}) \cup B') \geq r(B') = r(X)$. Nech C je bázou množiny $(B - \{x\}) \cup B'$. Množina $(B - \{x\})$ je nezávislá, lebo je podmnožinou bázy B. Z tretej vlastnosti matroidov potom plynie, že existuje prvok $y \in ((B - \{x\}) \cup B') - (B - \{x\}) = B' - B$ taký, že $(B - \{x\}) \cup \{y\} \in \mathcal{N}$. Keďže hodnosť $(B - \{x\}) \cup \{y\}$ je rovná hodnosti bázy B a množina je nezávislá, tak je tiež bázou.

Konštrukcia matroidu z množiny báz: za nezávislé množiny prehlásime všetky podmnožiny báz. Overenie správnosti tejto konštrukcie prenechávame ako samostatné cvičenie (úloha 47). □

Úloha 47. Dokážte správnosť konštrukcie z vety 3.5.

Def 3.4. Nech $M = (X, \mathcal{N})$ je matroid a $A \subseteq X$. Prvok $x \in X$ voláme závislý od množiny A v matroide M, ak $r(A) = r(A \cup \{x\})$.

Def 3.5. Nech $M = (X, \mathcal{N})$ je matroid a $A \subseteq X$. Uzáverom množiny A v matroide M voláme množinu $\bar{A}$ všetkých závislých prvkov od A. Formálne,

$$\bar{A} := \{x \in X \mid r(A) = r(A \cup \{x\})\}$$

Veta 3.6. *Nech $M = (X, \mathcal{N})$ je matroid a $A \subseteq X$. Potom platí:*

1. $A \subseteq \bar{A}$
2. $\forall x \in X : r(A \cup \{x\}) = r(A) \Longrightarrow \bar{A} = \overline{A \cup \{x\}}$
3. $\bar{A} = \bar{\bar{A}}$
4. $r(A) = r(\bar{A})$
5. $\bar{A} = \bigcup_{B \in \mathcal{P}(X)} \{B \mid B \supseteq A \wedge r(B) = r(A)\}$

Dôkaz. Prvá vlasnosť je očividná z definície.

2. $\forall x \in X : r(A \cup \{x\}) = r(A) \Longrightarrow \bar{A} = \overline{A \cup \{x\}}$**:** Musíme dokázať rovnosť dvoch množín. Dokážeme postupne $\bar{A} \subseteq \overline{A \cup \{x\}}$ a $\bar{A} \supseteq \overline{A \cup \{x\}}$.

$\bar{A} \subseteq \overline{A \cup \{x\}}$**:** Nech $y \in \bar{A}$, čiže $r(A \cup \{y\}) = r(A)$. Sporom, nech $y \notin \overline{A \cup \{x\}}$, t.j. $r(A \cup \{x\} \cup \{y\}) > r(A \cup \{x\}) = r(A)$. Označme si bázu množiny A ako N, a bázu množiny $A \cup \{x\} \cup \{y\}$ ako N'. Potom platí $|N| < |N'|$. Z tretej vlastnosti matroidov vyplýva, že musí existovať prvok $z \in N' - N$ taký, že $N \cup \{z\} \in \mathcal{N}$. Prvok z nemôže byť z množiny A, lebo množina N je jej bázou. Čiže prvok z je buď rovný x alebo y. Ale z definícií príslušných prvkov platí, že $r(A \cup \{x\}) = r(A \cup \{y\}) = r(A) = |N|$, čiže spor.

$\overline{A \cup \{x\}} \subseteq \bar{A}$**:** Nech $w \in \overline{A \cup \{x\}}$, t.j. $r(A \cup \{x\} \cup \{w\}) = r(A \cup \{x\}) = r(A)$. Z vlastností hodnostnej funkcie (veta 3.4) vyplýva, že $r(A \cup \{x\} \cup \{w\}) \geq r(A \cup \{w\})$ a zároveň $r(A \cup \{w\}) \geq r(A)$. Z toho však už plynie[2], že $r(A \cup \{w\}) = r(A)$, čiže $w \in \bar{A}$.

3. $\bar{A} = \bar{\bar{A}}$**:** Indukciou na počet prvkov v množine $\bar{A} - A$. Postupne si ich popridávam do množiny pomocou predošlej vlastnosti.

4. $r(A) = r(\bar{A})$**:** Indukciou na počet prvkov v množine $\bar{A} - A$. Postupne si ich popridávam do množiny A so zachovaním hodnosti (pomocou vlastnosti číslo 2).

5. $\bar{A} = \bigcup_{B \in \mathcal{P}(X)} \{B \mid B \supseteq A \wedge r(B) = r(A)\}$**:** Toto je rovnosť množín, dokazovať ju budeme pomocou dvoch inklúzií.

$\bar{A} \subseteq \bigcup_{B \in \mathcal{P}(X)} \{B \mid B \supseteq A \wedge r(B) = r(A)\}$**:** Z prvej vlastnosti plynie, že $\bar{A} \supseteq A$, zo štvrtej vlastnosti plynie, že $r(A) = r(\bar{A})$.

$\bigcup_{B \in \mathcal{P}(X)} \{B \mid B \supseteq A \wedge r(B) = r(A)\} \subseteq \bar{A}$**:** Ukážeme, že každá množina B zo zjednotenia na ľavej strane patrí do $\bar{A}$. Nech $x \in B - A$. Potom $r(B) \geq r(A \cup \{x\}) \geq r(A)$. Z toho vyplýva[3], že $r(A \cup \{x\}) = r(A)$, čiže $x \in \bar{A}$. □

Veta 3.7. *Nech $M = (X, \mathcal{N})$ je matroid a $\Phi : \mathcal{P}(X) \to \mathcal{P}(X)$ je jeho uzáverová funkcia (t.j. $\Phi(A) = \bar{A}$). Potom platí:*

U1: $\forall A \subseteq X : A \subseteq \bar{A}$

U2: $A \subseteq \bar{B} \Longrightarrow \bar{A} \subseteq \bar{B}$

U3: $x \notin \bar{A} \wedge x \in \overline{A \cup \{y\}} \Longrightarrow y \in \overline{A \cup \{x\}}$

Navyše, ak existuje funkcia $\Phi' : \mathcal{P}(A) \to \mathcal{P}(A)$, ktorá spĺňa podmienky U1 — U3, tak existuje jediný matroid, ktorého uzáverovou funkciou je práve Φ'.

Dôkaz. Prvá vlastnosť je už dokázaná vo vete 3.6.

[2] v tejto chvíli si študenti informatiky FMFI UK môžu nostalgicky spomenúť na vetu o dvoch prstoch a Kubáčkovom nose z prvého semestra matematickej analýzy

[3] tuto sa ku nostalgii môžu pridať aj študenti matematiky

2. $A \subseteq \bar{B} \Longrightarrow \bar{A} \subseteq \bar{B}$**:** Sporom, nech existuje prvok $x \in \bar{A} - A$ taký, že $x \notin \bar{B}$. Z toho vyplýva, že $r(A \cup \{x\}) = r(A)$ a $r(B \cup \{x\}) > r(B)$. Nech N_A je bázou množiny A a nech množina $N_B \supseteq N_A$ je doplnením množiny N_A na bázu množiny B. Potom z $r(B \cup \{x\}) > r(B)$ plynie, že $N'_B := N_B \cup \{x\} \in \mathcal{N}$, a z $r(A \cup \{x\}) = r(A)$ plynie, že $N'_A := A \cup \{x\} \notin \mathcal{N}$. Zároveň platí, že N'_A je podmnožinou N'_B. Dostali sme spor s druhou vlastnosťou matroidov, že podmnožina nezávislej množiny je tiež nezávislá.

3. $x \notin \bar{A} \wedge x \in \overline{A \cup \{y\}} \Longrightarrow y \in \overline{A \cup \{x\}}$**:** Sporom, nech $y \notin \overline{A \cup \{x\}}$. Zo semimodularity hodnostnej funkcie (veta 3.4, vlastnosť 4) vyplýva, že $r(A \cup \{a\}) \leq r(A)+1$ pre ľubovoľný prvok a.

Z $x \notin \bar{A}$ plynie, že $r(A \cup \{x\}) > r(A)$, spolu s predošlým výsledkom máme $r(A \cup \{x\}) = r(A)+1$. Z $x \in \overline{A \cup \{y\}}$ vyplýva, že $r(A \cup \{x\} \cup \{y\}) = r(A \cup \{y\}) \leq r(A)+1$. Z $y \notin \overline{A \cup \{x\}}$ vyplýva, že $r(A \cup \{x\} \cup \{y\}) > r(A \cup \{x\}) = r(A)+1$. Syntézou týchto dvoch nerovností dostávame $r(A)+1 < r(A \cup \{x\} \cup \{y\}) \leq r(A)+1$, čo je nemožné, čiže sme dospeli ku sporu.

Konštrukcia matroidu z uzáverovej funkcie: Množinu $A \subseteq X$ prehlásime za nezávislú práve vtedy keď každá jej podmnožina má menší uzáver. Formálne,

$$A \in \mathcal{N} \Longleftrightarrow \forall B \subsetneq A : \Phi'(B) \subsetneq \Phi'(A).$$

Overenie správnosti konštrukcie prenechávame ako samostatné cvičenie (úloha 48). □

Úloha 48. Dokážte správnosť konštrukcie z vety 3.7.

Def 3.6. Nech $(X, \mathcal{N})$ je matroid. Množina $K \subseteq X$ sa volá kružnica, ak je to najmenšia (na inklúziu) závislá množina. Formálne, množina $K \subseteq X$ je kružnica, ak:

$$K \notin \mathcal{N} \wedge (\forall K' \subsetneq K : K' \in \mathcal{N})$$

Množinu všetkých kružníc matroidu označujeme ako $\mathcal{K}$.

Veta 3.8. *Nech $(X, \mathcal{N})$ je matroid a $\mathcal{K}$ je množina všetkých jeho kružníc. Potom platí:*

K1: žiadne dva prvky množiny $\mathcal{K}$ nie sú v inklúzii

K2: $K, K' \in \mathcal{K} \wedge K \neq K' \wedge \exists x \in K \cap K' \Longrightarrow \exists L \in \mathcal{K} : L \subseteq (K \cup K') - \{x\}$

Navyše, ak existuje množina $\mathcal{K}'$, ktorá spĺňa podmienky K1 a K2, tak existuje jediný matroid, ktorého množinou kružníc je práve $\mathcal{K}'$.

Dôkaz. Prvá vlastnosť je očividná z definície kružnice.

2. $K, K' \in \mathcal{K} \wedge K \neq K' \wedge \exists x \in K \cap K' \Longrightarrow \exists L \in \mathcal{K} : L \subseteq (K \cup K') - \{x\}$**:** Na overenie platnosti tohto tvrdenia stačí ukázať, že množina $(K \cup K') - \{x\}$ je závislá. Pozrime[4] sa na hodnosť množiny $K \cup K'$:

$$r(K \cup K') \overset{semimodularita}{\leq} r(K) + r(K') - r(K \cap K') \overset{*}{=}$$
$$\overset{*}{=} (|K| - 1) + (|K'| - 1) - |K \cap K'| = |K \cup K'| - 2$$

[4]toto je klasický prípad dôkazu metódou "pozriem a vidím", obľúbenej vyučujúcimi a nenávistnej študentom. Tá istá myšlienka sa dá použiť priamo na množinu $(K \cup K') - \{x\} = (K - \{x\}) \cup (K' - \{x\})$, je to však o niečo menej prehľadné

(*) Treba si uvedomiť, že každá vlastná podmnožina kružnice je nezávislá množina, takže ich mohutnosti sú totožné s ich hodnosťami.

Z danej nerovnosti už vyplýva, že ani $K \cup K'$, ani $(K \cup K') - \{x\}$ nie sú nezávislými množinami, čím je dôkaz ukončený.

Konštrukcia matroidu z množiny kružníc: Za nezávisle množiny prehlásime všetky množiny, ktoré neobsahujú ani jednu kružnicu. Overenie správnosti konštrukcie prenechávame ako samostatné cvičenie (úloha 49). □

Úloha 49. Dokážte správnosť konštrukcie z vety 3.8.

Def 3.7. Nech $G = (V, E)$ je jednoduchý graf a $\phi : E \longrightarrow \{+, -\}$ je funkcia, ktorá každej hrane grafu G priradí buď plus alebo mínus. Potom trojica (V, E, ϕ) je signovaný graf. Hrany signovaného grafu, ktorým je priradená hodnota $+$, voláme *kladné*. Ostatné hrany voláme *záporné*.

Def 3.8. Nech G je signovaný graf. Potom kružnice s párnym počtom záporných hrán, voláme *balansované*. Ostatné kružnice voláme *nebalansované*.

Veta 3.9. *(Matroid zo signovaného grafu)*
Nech $G = (V, E, \phi)$ je signovaný graf. Nech $X := E$ a nech do množiny $\mathcal{K}$ patria také množiny hrán, ktoré indukujú balansované kružnice a také množiny hrán, ktoré indukujú graf, pozostávajúci z dvoch nebalansovaných kružníc, spojených cestou (nie nutne kladnej dĺžky). Potom existuje jediný matroid $(X, \mathcal{N})$, ktorého množinou kružníc je práve $\mathcal{K}$.

Úloha 50. Dokážte vetu 3.9 (*hint: pomocou vety 3.8*).

3.2 Dualita matroidov a triedy matroidov

Veta 3.10. *(veta o dualite)*
Nech $M = (X, \mathcal{N})$ je matroid. Nech $\mathcal{B}$ je množina báz matroidu M a $r : \mathcal{P}(X) \to \mathbb{N}_0$ je hodnostná funkcia matroidu M. Ďalej nech:

- $\mathcal{B}^* := \{X - B \mid B \in \mathcal{B}\}$
- $\mathcal{N}^* := \{X - A \mid A \subseteq X \wedge r(A) = r(X)\}$
- $r^* : \mathcal{P}(A) \to \mathbb{N}_0$ *taká, že* $r^*(A) := |A| - r(X) + r(X - A) = |A| - (r(X) - r(X - A))$

Potom platí:

1. *množina $\mathcal{B}^*$ je systémom báz nejakého matroidu*
2. *množina $\mathcal{N}^*$ je systémom nezávislých množín nejakého matroidu*
3. *funkcia r^* je hodnostnou funkciou nejakého matroidu*
4. *navyše, všetky 3 vyššie uvedené matroidy sú rovnaké*

Takýmto spôsobom zostrojený matroid sa volá duálny a značí sa ako $M^* = (X, \mathcal{N}^*)$.

Dôkaz. Je zrejmé, že ak dvojica $(X, \mathcal{N}^*)$ je matroidom, tak množina $\mathcal{B}^*$ bude množinou jeho báz a naopak, ak $\mathcal{B}^*$ je množinou báz nejakého matroidu, tak nezávislé množiny v tomto matroide budú práve $\mathcal{N}^*$. Treba teda dokázať, že dvojica $(X, \mathcal{N}^*)$ spĺňa definíciu matroidu, a že jeho hodnostnou funkciou je práve r^*. Tým ukážeme, že funkcia r^* spĺňa podmienky hodnostnej funkcie, a z predošlých viet (veta 3.4) bude teda platiť unikátnosť z nej odvodeného matroidu.

Na overenie, či je dvojica $(X, \mathcal{N}^*)$ matroidom, treba overiť tri podmienky:

1. $\varnothing \in \mathcal{N}^*$**:** Množina X má plnú hodnosť v pôvodnom matroide, preto do $\mathcal{N}^*$ z konštrukcie patrí jej komplement, teda prázdna množina. Formálne,

$$X \subseteq X \wedge r(X) = r(X) \Longrightarrow X - X = \varnothing \in \mathcal{N}^*.$$

2. $N \in \mathcal{N}^* \wedge N' \subseteq N \Longrightarrow N' \in \mathcal{N}^*$**:** To, že množina $N \in \mathcal{N}^*$ znamená, že jej komplement $X - N$ má plnú hodnosť v pôvodnom matroide. Keďže množina N' je podmnožinou N, tak jej komplement $X - N'$ je nadmnožinou $X - N$, čiže tiež má plnú hodnosť v pôvodnom matroide. Z toho podľa konštrukcie plynie, že aj množina N' je v množine $\mathcal{N}^*$.

3. $N, N' \in \mathcal{N}^* \wedge |N| < |N'| \Longrightarrow \exists x \in N' - N : N \cup \{x\} \in \mathcal{N}^*$**:** Prepíšeme najprv toto tvrdenie do jazyku pôvodného matroidu:

$$r(X - N) = r(X) \wedge r(X - N') = r(X) \wedge |X - N| > |X - N'| \stackrel{?}{\Longrightarrow}$$
$$\exists x \in (X - N) - (X - N') : r((X - N) - \{x\}) = r(X).$$

Inak povedané, ak máme v matroide nejaké dve množiny A a B plnej hodnosti, pričom $|A| > |B|$, tak či existuje taký prvok x z $A - B$, že jeho odobratím z A zachováme jej hodnosť?

Dokážeme toto tvrdenie priamo. Nech C je bázou množiny $A \cap B$ v pôvodnom matroide, C_A je jej rozšírením na bázu množiny A a C_B je rozšírením množiny C na bázu množiny B. Veľkosti množín $C_A - C$ a $C_B - C$ sú rovnaké (lebo C_A a C_B sú bázami pôvodného matroidu). Z toho vyplýva, že $|C_A - C| = |C_B - C| \leq |B - (A \cap B)| < |A - (A \cap B)|$, čiže množina $(A - (A \cap B)) - (C_A - C)$ je neprázdna. A je už zrejmé, že odstránením ľubovoľného prvku množiny $(A - (A \cap B)) - (C_A - C)$ z množiny A sa hodnosť množiny A nezmení (lebo bude stále obsahovať množinu C_A, ktorá je bázou množiny X).

Týmto je overenie, že $(X, \mathcal{N}^*)$ je matroidom, ukončené. Ostáva už len ukázať, že jeho hodnostnou funkciou je práve r^*. Označíme dočasne hodnostnú funkciu matroidu $(X, \mathcal{N}^*)$ ako g.

Nech bázou $A \subseteq X$ v matroide M^* je množina N^*. Potom $N^* \in \mathcal{N}^*$, čiže z konštrukcie $r(X - N^*) = r(X)$. Nech B_0 je bázou množiny $X - A$ v matroide M. Nech B_1 je rozšírením množiny B_0 na bázu množiny $X - N^*$ v matroide M. Všimneme si, že $B_1 - B_0 \subseteq A - N^*$ (lebo B_0 je bázou $X - A$ v matroide M). Hodnosť množiny B_1 je rovná hodnosti množiny $X - N^*$ (lebo je jej bázou), z definície N^* platí $r(B_1) = r(X - N^*) = r(X)$. Teda množina B_1 je bázou matroidu M. Z toho plynie, že $|B_1| = r(X)$.

Nech $B^* := A - B_1$, potom $|B^*| = |A - (B_1 - B_0)| = |A| - |B_1| + |B_0| = |A| - r(X) + r(X - A)$. Všimneme si, že $X - B^* \supseteq B_1$, teda $r(X - B^*) \geq r(B_1) = r(X)$. Z toho plynie, že $B^* \in \mathcal{N}^*$. Nakoľko $B^* \in \mathcal{N}^*$ a $B^* \subseteq A$, tak $|B^*| \leq |N^*|$ (lebo N^* je bázou množiny A, t.j. najväčšou nezávislou podmnožinou A). Nakoľko však

$B_1 - B_0 \cap N^* = \varnothing$, platí, že $N^* \subseteq B^*$. Z toho vyplýva, že $B^* = N^*$, a teda $g(A) = |N^*| = |B^*| = |A| - r(X) + r(X - A)$. □

Veta* 3.11. *Nech $M(G)$ je grafový matroidu grafu G. Potom nasledujúce podmienky sú ekvivalentné:*

1. *M^* je grafový matroid*
2. *G je planárny graf*

Def 3.9. Nech $M = (X, \mathcal{N})$ je matroid a F je pole. Matroid M je F-reprezentovateľný, ak existuje vektorový priestor V konečnej dimenzie nad F a zobrazenie $f : X \to V$ také, že

$$\forall A \in X : (A \in \mathcal{N} \iff f(A) \text{ je lineárne nezávislá vo } V)$$

Def 3.10. Matroid je reprezentovateľný, ak je F-reprezentovateľný nad nejakým poľom F.

Def 3.11. Matroid je binárny, ak je $GF(2)$-reprezentovateľný.

Def 3.12. Matroid je regulárny, ak je F-reprezentovateľný nad každým poľom F.

Veta* 3.12. *Každý grafový matroid je regulárny.*

Def 3.13. (Zúženie matroidu)
Nech $M = (X, \mathcal{N})$ je matroid a $Y \subseteq X$. Nech $\mathcal{N}_Y := \{A \mid A \subseteq Y \wedge \exists B \in \mathcal{N} : A = B \cap Y\}$. Potom ${}^{M}\!/_{Y} := (Y, \mathcal{N}_Y)$ je matroid a nazýva sa zúžením matroidu M na množinu Y.

Úloha 51. Dokážte, že zúženie matroidu je tiež matroid.

Def 3.14. (Kontrakcia matroidu)
Nech $M = (X, \mathcal{N})$ je matroid a $Y \subseteq X$. Nech $A \subseteq Y$ patrí do systému $\mathcal{N}_Y$ práve vtedy, keď existuje báza B množiny $X - Y$ v matroide M taká, že $A \cup B \in \mathcal{N}$. Potom dvojica $M.Y := (Y, \mathcal{N}_Y)$ je matroid a nazýva sa kontrakciou matroidu M na množinu Y.

Úloha 52. Dokážte, že kontrakcia matroidu je tiež matroid.

Veta* 3.13. ${}^{M^*}\!/_{Y} = (M.Y)^*$

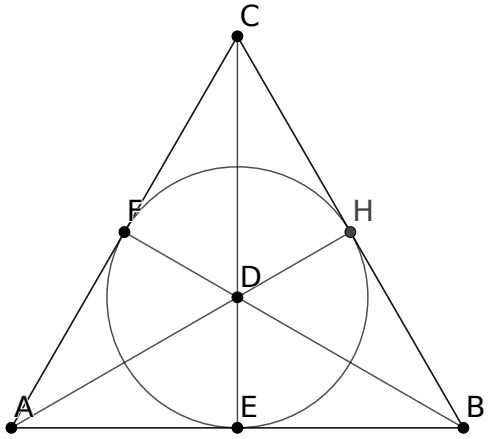
Def 3.15. Matroid M' je minorom matroidu M, ak sa matroid M' dá dostať z matroidu M pomocou postupnosti zúžení a kontrakcií.

Def 3.16. Nech $\pi_F = (X, \mathcal{B}, \in)$ je Fanova projektívna rovina (viď obrázok 3.1). Nech množina $\mathcal{N}$ obsahuje všetky podmnožiny X mohutnosti najviac dva a také trojice bodov, ktoré neležia na jednej priamke. Potom $(X, \mathcal{N})$ je Fanov matroid a označuje sa $\mathcal{F}$.

Úloha 53. Overte, či definícia 3.16 spĺňa podmienky z definície matroidu.

Def 3.17. Nech $X := \{1, \ldots, n\}$, $\mathcal{N} := \{A \mid A \subseteq X \wedge |A| \leq k\}$. Potom dvojica $U_k^n = (X, \mathcal{N})$ je matroid.

Veta 3.14. $(U_k^n)^* = U_{n-k}^n$



Obr. 3.1: Fanova projektívna rovina

Veta* 3.15. *(Charakterizácia tried matroidov)*

1. *matroid M je binárny $\iff$ U_2^4 nie je minorom matroidu M.*
2. *matroid M je regulárny $\iff$ U_2^4, $\mathcal{F}$, $\mathcal{F}^*$ nie sú minormi matroidu M.*
3. *matroid M je grafový $\iff$ U_2^4, $\mathcal{F}$, $\mathcal{F}^*$, $M^*(K_{3,3})$, $M^*(K_5)$ nie sú minormi matroidu M.*
4. *matroid M je kografový $\iff$ U_2^4, $\mathcal{F}$, $\mathcal{F}^*$, $M(K_{3,3})$, $M(K_5)$ nie sú minormi matroidu M.*
5. *matroid M je planárny $\iff$ matroid M je grafový a kografový.*

3.3 Matroidové algoritmy

Def 3.18. Problém maximálnej množiny je trojica $(X, \mathcal{M}, c)$, kde $X = x_1, \ldots, x_n$ je množina objektov, $\mathcal{M} \subseteq \mathcal{P}(X)$ je množina prípustných riešení a $c : X \to \mathbb{R}^+ \cup \{0\}$ je cenová funkcia, rozšíriteľná na $\mathcal{P}(X)$, a to takým spôsobom: $\forall A \in \mathcal{P}(X) : c(A) := \sum_{x_i \in A} c(x_i)$. Riešením problému maximálnej množiny je množina $M^* \in \mathcal{M}$ s maximálnou cenou. Formálne,

$$M^* := \arg\max_{M \in \mathcal{M}} c(M)$$

Def 3.19. (Pažravý algoritmus)
Nech $(X, \mathcal{M}, c)$ je problém maximálnej množiny. Potom nasledovný algoritmus je pažravým algoritmom pre nájdenie riešenia daného problému:

1. $M_0 := \varnothing$
2. $M_{i+1} := M_i \cup \{x\}$, ak x spĺňa nasledovné podmienky:
   (a) $x \notin M_i$
   (b) $M_i \cup \{x\} \subseteq M' \in \mathcal{M}$ (t.j. existuje také $M' \in \mathcal{M}$)

(c) x má spomedzi všetkých prvkov, ktoré spĺňajú predchádzajúce podmienky, maximálnu cenu $c(x)$

3. Opakujeme krok 2. Ak x, vyhovujúce všetkým podmienkam z druhého kroku, neexistuje, tak algoritmus končí a odpoveďou je posledná množina M_i.

Veta 3.16. *(Vzťah matroidov a pažravých algoritmov)*
Nech X je konečná množina, $\mathcal{M} \subseteq \mathcal{P}(X)$. Potom nasledujúce podmienky sú ekvivalentné:

1. *pre každé nezáporné ohodnotenie c množiny X pažravý algoritmus nájde optimálne riešenie*

2. *existuje matroid na množine X taký, že $\mathcal{M}$ je systémom báz daného matroidu*

overit presne znenie vety (mnozina maximalnych na inkluziu pripustnych rieseni je systemom baz?)