

# Kombinatorické štruktúry :: sylabus

Askar Gafurov

25. júna 2017

# Obsah

<b>0</b>	<b>Úvod</b>	<b>2</b>
<b>1</b>	<b>Latinské štvorce</b>	<b>3</b>
1.1	Definícia, základné vlastnosti . . . . .	3
1.2	Ortogonálne latinské štvorce . . . . .	4
<b>2</b>	<b>Blokové plány</b>	<b>6</b>
2.1	Definícia, základné vlastnosti . . . . .	6
2.2	Cyklické blokové plány a diferenčné množiny . . . . .	7
2.3	Hadamardove matice . . . . .	8
2.4	Konečné projektívne roviny . . . . .	8
2.5	Steinerovské systémy trojíc, zovšeobecnenia . . . . .	10
<b>3</b>	<b>Matroidy</b>	<b>12</b>
3.1	Definícia, základné pojmy . . . . .	12
3.2	Dualita matroidov a triedy matroidov . . . . .	14
3.3	Matroidové algoritmy . . . . .	15

# Kapitola 0

## Úvod

Cieľom tohto textu je urobiť prehľad o kľúčových pojmoch a tvrdeniach z teórie kombinatorických štruktúr a pomôcť tak pri príprave na skúšku. Daný materiál teda obsahuje úplné znenia definícií a viet, nemá však žiadne dôkazy. Je tomu tak hlavne z dôvodu, že väčšina preberaných tvrdení je buď "pod našu uroveň" alebo "nad našu uroveň". Tvrdenia prvého typu prenechávame čitateľovi na samostatné odvodenie (časom možno pribudnú odkazy na materiály s podrobnými dôkazmi). Tvrdenia druhého typu sú v texte označené hviezdikou.

Daný text nie je náhradou pre absolvovanie prednášok<sup>1</sup>.

Pre ďalšie štúdium odporúčame knihy **TODO**.

Tento text je písaný na základe prednášok z predmetu Kombinatorické štruktúry v zimnom semestri akademického roku 2016/17.

---

<sup>1</sup>a ani náhradou pre pestrú výživu :)

# Kapitola 1

## Latinské štvorce

### 1.1 Definícia, základné vlastnosti

**Definícia 1.1.1.** Tabuľka rozmerov  $n \times n$  s prvkami z  $\{1, \dots, n\}$  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

Symbolom  $S_n$  značíme grupu permutácií veľkosti  $n$ .

**Definícia 1.1.2.** Nech  $\phi, \psi \in S_n$  sú permutácie veľkosti  $n$ . Potom vzdialenosť  $dist(\phi, \psi)$  dvoch permutácií definujeme ako počet prvkov, ktoré dané permutácie zobrazia rôzne. Formálne,

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

**Definícia 1.1.3.** Nech  $\phi \in S_n$  je permutácia veľkosti  $n$ . Potom  $Fix(\phi)$  je množina všetkých pevných bodov permutácie  $\phi$ . Formálne,

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

**Veta 1.1.1.** Nech  $\phi, \psi \in S_n$  sú permutácie veľkosti  $n$ . Potom platí:

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

**Veta 1.1.2.** Funkcia  $dist(\phi, \psi)$  je metrikou priestoru  $S_n$ , t.j. ona spĺňa nasledujúce podmienky:

1.  $dist(\phi, \psi) = 0 \Leftrightarrow \phi = \psi$
2.  $dist(\phi, \psi) = dist(\psi, \phi)$  (symetria)
3.  $dist(\phi, \psi) + dist(\psi, \lambda) \geq dist(\phi, \lambda)$  (trojuholníková nerovnosť)

**Definícia 1.1.4.** Latinský obdĺžnik rozmerov  $k \times n$  je postupnosť  $L = [\phi_1, \phi_2, \dots, \phi_k]$  permutácií z  $S_n$  takých, že všetky sú vo vzdialenosti  $n$ . Formálne,

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

**Definícia 1.1.5.** (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  $n$ .

**Veta 1.1.3.** Každý latinský obdĺžnik sa dá doplniť na latinský štvorec.

## 1.2 Ortogonálne latinské štvorce

**Definícia 1.2.1.** Nech  $l = [\phi_1, \dots, \phi_n]$  a  $l' = [\psi_1, \dots, \psi_n]$  sú latinské štvorce rádu  $n$ . Hovoríme, že  $l$  a  $l'$  sú ortogonálne (znáčime ako  $l \perp l'$ ), ak platí:

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

**Veta 1.2.1.** Nech  $l = [\phi_1, \dots, \phi_n]$  a  $l' = [\psi_1, \dots, \psi_n]$  sú latinské štvorce rádu  $n$ . Zavedieme nasledovné značenia:

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

Potom platí:

1.  $l \perp l' \Leftrightarrow [\psi_1\phi_1^{-1}, \dots, \psi_n\phi_n^{-1}]$  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  $l' = l'' \circ l$

**Definícia 1.2.2.** Množina latinských štvorcov rádu  $n$   $\{l_1, \dots, l_r\}$  je maximálna, ak  $\forall i \neq j : l_i \perp l_j$  a nedá sa doplniť ďalším latinským štvorcom bez porušenia prvej podmienky.

**Veta 1.2.2.** Maximálna množina latinských štvorcov rádu  $n$  má najviac  $n - 1$  prvkov.

**Definícia 1.2.3.** Latinský štvorec je v normálnom tvare, ak prvý riadok tabuľky je rovný  $(1, \dots, n)$  a prvý stĺpec je rovný  $(1, \dots, n)^T$ .

**Definícia 1.2.4.** Latinské štvorce  $l$  a  $l'$  sú izotopické, ak sa dajú permutáciou riadkov a stĺpcov previesť na rovnaký latinský štvorec v normálnom tvare.

*Poznámka 1.2.1.* Latinský štvorec v normálnom tvare zodpovedá tabuľke binárnej operácie kvazigrupy (kvazigrupa je množina s invertovateľnou binárnou operáciou a neutrálnym prvkom<sup>1</sup>).

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

**Definícia 1.2.5.** Latinský štvorec si vieme predstaviť ako maximálnu (na inklúziu) množinu  $A$  trojíc  $(r, c, s) \in \{1, \dots, n\}^3$ , 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*.

<sup>1</sup>dá sa to neformálne predstaviť ako grupu bez zaručenej asociativity

**Veta 1.2.3.** (Stevens, 1935) Ak  $n = p^\alpha$ , kde  $p$  je prvočíslo, tak maximálna množina latinských štvorcov má  $n - 1$  prvkov.

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

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

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

**Definícia 1.2.6.**  $MOLS(n)$  je mohutnosť maximálnej množiny latinských štvorcov rádu  $n$ .

*Poznámka 1.2.2.*  $MOLS(6) = 1$

**Veta\* 1.2.4.** (Bose, Parker, Schrickhande, 1960)

$$\forall n \geq 3 \wedge n \neq 6 : MOLS(n) \geq 2$$

**Veta 1.2.5.**  $MOLS(n_1) \geq m \wedge MOLS(n_2) \geq m \Rightarrow MOLS(n_1 n_2) \geq m$

**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  $l_1, \dots, l_m$  sú ortogonálne latinské štvorce rádu  $n_1$  a  $l'_1, \dots, l'_m$  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  $n_1 n_2$ .

**Dôsledok 1.2.5.1.**

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

**Veta 1.2.6.**

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

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

$$A := (a_{ij}), a_{ij} := m(i + j) \pmod{n}$$

$$B := (b_{ij}), b_{ij} := (i - j) \pmod{n}$$

# Kapitola 2

## Blokové plány

### 2.1 Definícia, základné vlastnosti

**Definícia 2.1.1.** 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 bod je obsiahnutý v práve  $r$  blokoch.
5. každá dvojica bodov sa vyskytuje v práve  $\lambda$  blokoch.

**Veta 2.1.1.**  $\exists BIBD(v, b, r, k, \lambda) \iff \lambda$ -násobný kompletný multigraf rádu  $v$   $\lambda K_v$  sa dá rozložiť na  $b$  hranovo disjunktných klík rádu  $k$  ( $K_k$ ).

**Veta 2.1.2.** Nech existuje  $BIBD(v, b, r, k, \lambda)$ . Potom:

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

**Dôsledok 2.1.2.1.** Preto namiesto značenia  $BIBD(v, b, r, k, \lambda)$  budeme často používať značenie  $BIBD(v, k, \lambda)$ , nakoľko zvyšné parametre vieme dorátať:

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

**Veta 2.1.3.** Nech existuje  $BIBD(v, b, r, k, \lambda)$ , kde  $X = \{x_1, x_2, \dots, x_v\}$  a  $\mathcal{B} = \{B_1, \dots, B_b\}$ . 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  $v \times v$ .

**Lema 2.1.4.** Nech  $A$  je matica incidencie blokového plánu  $BIBD(v, b, r, k, \lambda)$ . Potom  $\det(AA^T) = (r - \lambda)^{v-1}(v\lambda - \lambda + r)$ .

**Dôsledok 2.1.4.1.** Ak  $BIBD(v, b, r, k, \lambda)$  je blokový plán a  $b = v$ , tak matica incidencie  $A$  je regulárna a matice  $A^T$  tiež zodpovedá nejaký blokový plán.

*Poznámka 2.1.1.* Blokové plány také, že  $b = v$ , voláme symetrické.

**Veta 2.1.5.** (Fisherova nerovnosť) Nech existuje blokový plán  $BIBD(v, b, r, k, \lambda)$ . Potom  $b \geq v$ .

**Dôsledok 2.1.5.1.** Nech existuje blokový plán  $BIBD(v, b, r, k, \lambda)$ . Potom  $r \geq k$ .

## 2.2 Cyklické blokové plány a diferenčné množiny

**Definícia 2.2.1.** Množina  $D = \{d_1, \dots, d_k\} \subset \mathbb{Z}_v$  mohutnosti  $k$  sa volá  $(v, k, \lambda)$ -diferenčnou množinou, ak pre každý nenulový prvok  $a \in \mathbb{Z}_v$  existuje práve  $\lambda$  usporiadaných dvojíc  $(d_i, d_j) \in D^2$  takých, že  $d_i - d_j \equiv a \pmod v$ .

*Poznámka 2.2.1.* Množina  $\{0, 1, 3\}$  je  $(7, 3, 1)$ -diferenčnou množinou.

*Poznámka 2.2.2.* Podobným spôsobom je možné definovať diferenčné množiny nad konečnými grupami rádu  $v$ .

**Definícia 2.2.2.**  $(v, k, \lambda)$ -BIBD je cyklický, ak existuje permutácia s cyklom dĺžky  $v$  taká, že zachováva bloky<sup>1</sup>. Formálne, blokový plán je cyklický, ak existuje permutácia  $\phi \in S_v$  s cyklom dĺžky  $v$  taká, že

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

**Veta 2.2.1.** Množina  $D = \{d_1, \dots, d_k\}$  je  $(v, k, \lambda)$ -diferenčná množina práve vtedy, keď  $(X, \mathcal{B})$ , kde  $X = \mathbb{Z}_v$  a  $\mathcal{B} = \{D + i \mid \forall i \in \mathbb{Z}_v\}$  ( $D + i := \{d_1 + i, \dots, d_k + i\}$ ) je cyklický  $(v, k, \lambda)$ -BIBD.

**Definícia 2.2.3.** 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  $V^* := V - \{\vec{0}\}$ :

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

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  $PG(n, q) := \mathbb{P}^n(\mathbb{Z}_p^r)$

**Veta\* 2.2.2.** (Typ  $S$  dif. množín — Singerove dif. množiny)<sup>2</sup>

Nech množina  $D$  obsahuje všetky nadroviny konečnej projektívnej roviny  $PG(n, q)$  (nadrovina je faktorový obraz vektorového podpriestoru dimenzie  $n$ ). Potom  $D$  je  $(v, k, \lambda)$ -diferenčná množina s parametrami:

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

**Veta\* 2.2.3.** (Typ  $Q$  dif. množín — kvadratické reziduá, angl. Paley-type)

Nech  $F := GF(p^l)$  je konečné pole mohutnosti  $p^l$ , kde  $p^l \equiv 3 \pmod 4$ . Nech  $r \in F$  je generátor grupy  $F^* := (F - \{0\}, *)$ . Potom množina kvadratických reziduá grupy  $F^*$   $QR(F^*) := \{r^a \pmod{p^l} \mid a \in \{0, \dots, p^l - 1\} \wedge a \text{ je párne}\}$  je  $(v, k, \lambda)$ -diferenčnou množinou s parametrami:

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

*Poznámka 2.2.3.* Existujú aj ďalšie triedy diferenčných množín, napríklad bikvadratické reziduá alebo tzv. *twin prime power difference set*.

**TODO** rozpísať bikvadratické reziduá, resp. twin prime power.

<sup>1</sup>bijektívne zobrazenia množiny na ňu samu, ktoré zachovávajú vzťahy medzi objektami, sa všeobecne nazývajú *automorfizmy*

<sup>2</sup>**TODO** je to bez dokazu ci s dokazom?



## 2.3 Hadamardove matice

**Definícia 2.3.1.** 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 2.3.1.** Nech matica  $H$  je Hadamardova matica rádu  $n$ . Potom platí:

1. vymenou riadkov (stĺpcov) matice  $H$  dostaneme Hadamardovu maticu
2. matica  $H$  je normálna, t.j.  $HH^T = H^T H$

**Definícia 2.3.2.** Hadamardova matica je v normálnom tvare, ak prvý riadok aj prvý stĺpec obsahujú iba hodnoty  $+1$ .

**Veta\* 2.3.2.** Nech  $H$  je Hadamardova matica rádu  $n$ . Potom  $\det H = \sqrt{n^n}$ .

**Veta\* 2.3.3.** (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 2.3.4.** Ak  $H$  je Hadamardova matica rádu  $n$ , tak  $n$  je buď 1, 2 alebo násobok 4.

**Hypotéza 2.3.1.** (Hadamard)

$\forall n \in \{1, 2\} \cup \{4k \mid k \in \mathbb{N}\} \implies \text{existuje Hadamardova matica rádu } n$ .

**Veta 2.3.5.** (Hadamard, Sylvester)

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

**Veta 2.3.6.** Normalizovaná Hadamardova matica rádu  $4\mu$  existuje práve vtedy, keď existuje  $(4\mu - 1, 2\mu - 1, \mu - 1)$ -diferenčná množina (typ  $Q$ ).

## 2.4 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 2.2.3). V tejto sekcii uvedieme iné dve definície: axiomatickú a kombinatorickú.

**Definícia 2.4.1.** (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.

Usporiadana trojiica  $\pi = (X, \mathfrak{P}, \in)$ , 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:

1. Každými dvomi rôznymi bodmi prechádza **práve 1** priamka.
2. Každé dve rôzne priamky majú **práve 1** spoločný bod.
3. existujú 4 body vo všeobecnej geometrickej polohe, t.j. žiadnou trojicou z týchto bodov nevedie žiadna priamka.

**Veta\* 2.4.1.** (Desarguesova veta)

**TODO** obrázok

**Veta 2.4.2.** V konečnej projektívnej rovine (v zmysle definície 2.4.1) existujú 4 priamky také, že žiadna trojica z týchto priamok nemá spoločný bod.

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 ľubovoľnom 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 2.4.2).

**Veta 2.4.3.** *Nech  $\pi$  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  $\pi$  má práve  $n^2 + n + 1$  priamok
6. konečná projektívna rovina  $\pi$  má práve  $n^2 + n + 1$  bodov (duálne ku 5.)

**Definícia 2.4.2.** (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 2.4.4.** *Kombinatorická a axiomatická definície konečnej projektívnej roviny sú ekvivalentné.*

**Veta\* 2.4.5.** *Ak  $n$  je mocninou prvočísla, tak existuje konečná projektívna rovina rádu  $n$ .*

**Hypotéza 2.4.1.** *Ak existuje konečná projektívna rovina rádu  $n$ , tak  $n$  je mocninou prvočísla.*

**Definícia 2.4.3.** 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.

**Veta 2.4.6.** *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.*

**Veta 2.4.7.** *Existencia konečnej projektívnej roviny rádu  $n$  je ekvivalentná s existenciou  $(n - 1)$  navzájom ortogonálnych latinských štvorcov rádu  $n$ .*

**Konstruktia. TODO**

## 2.5 Steinerovské systémy trojíc, zovšeobecnenia

**Definícia 2.5.1.** Blokové plány typu  $BIBD(v, 3, 1)$  sa volajú Steinerovské systémy trojíc (angl. *Steiner triplet system*, skratene STS).

*Poznámka 2.5.1.* Existencia STS je ekvivalentná s existenciou rozkladu kompletného grafu  $K_v$  na trojuholníky.

**Veta 2.5.1.** Ak  $v$  je počet objektov STS, tak  $v \equiv 1 \pmod{6}$  alebo  $v \equiv 3 \pmod{6}$ .

**Veta\* 2.5.2.** (Kirkman)

Ak  $v$  spĺňa podmienky z vety 2.5.1, tak existuje STS s práve  $v$  objektmi.

**Veta 2.5.3.** (Projektívne STS)<sup>3</sup>

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

**Veta 2.5.4.** (Afinné STS)<sup>4</sup>

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

**Veta 2.5.5.** (Karteziánsky súčin STS)

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

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

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

**Veta 2.5.6.** (Vzťah STS a grupoidov)

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

$$\forall \{x, y, z\} \in \mathcal{B} :$$

$$x * y = y * x = z$$

$$x * z = z * x = y$$

$$y * z = z * y = x$$

$$x * x = x$$

je idempotentný komutatívny grupoid.

**Veta 2.5.7.**  $((2v+1)$ -konštrukcia STS)

Nech  $(X, \mathcal{B})$  je STS a  $(X', \mathcal{B}')$  je jeho disjunktná izomorfná kópia (t.j.  $X \cap X' = \emptyset$ ). 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.

**TODO** Paschovo prepnutie

**TODO** Wilson-Schreiberova konštrukcia

**TODO** Boséova konštrukcia

**TODO** Skolemova konštrukcia

**TODO** Cyklické STS

**TODO** Symetrické  $v_3$ -konfigurácie (čiasť STS)

---

<sup>3</sup>**TODO** treba dôkaz?

<sup>4</sup>**TODO** treba dôkaz?

**Hypotéza 2.5.1.** Každý bezmostový kubický graf má 6 1-faktorů takých, že každá hrana grafu leží v právě 2 z nich.

**Definícia 2.5.2.** 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 objektů z  $X$  sa vyskytuje v práve  $\lambda$  blokoch z  $\mathcal{B}$

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

*Poznámka 2.5.2.* Existencia  $t - (v, k, \lambda)$ -blokového plánu je ekvivalentná s existenciou rozkladu  $t$ -uniformného  $\lambda$ -násobného hypergrafu na hyperklíky veľkosti  $k$ .

*Poznámka 2.5.3.* STS s  $v$  prvkami môžeme značiť ako  $S(2, 3, v)$ .

**Definícia 2.5.3.** Blokové plány  $S(3, 4, v)$  voláme Steinerovské systémy štvoríc (angl. *SQS*)

**Veta\* 2.5.8.**  $\exists S(3, 4, v) \iff v \equiv 3, 4 \pmod{6}$

**Definícia 2.5.4.** Blokové plány  $S(4, 5, v)$  voláme Steinerovské systémy päťíc

**Veta\* 2.5.9.**  $\exists S(4, 5, v) \implies v \equiv 4, 5 \pmod{6} \wedge v \not\equiv 4 \pmod{5}$

**TODO** konečné jednoduché grupy.

# Kapitola 3

## Matroidy

### 3.1 Definícia, základné pojmy

**Definícia 3.1.1.** Dvojica  $(X, \mathcal{N})$ , kde  $\mathcal{N} \in \mathcal{P}(X)$  a  $\mathcal{N}$  je konečná, je matroid, ak sú splnené nasledujúce podmienky:

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

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

**Veta 3.1.1.** (Matroid z vektorového priestoru)

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

**Veta 3.1.2.** (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.

**TODO** konstrukcia matroidu cez signovane grafy?

**Definícia 3.1.2.** 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:

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

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

**Veta 3.1.3.** Nech  $(X, \mathcal{N})$  je matroid a  $A \subseteq X$ . Nech  $N, N'$  sú bázy množiny  $A$ . Potom  $|N| = |N'|$ .

**Definícia 3.1.3.** Nech  $(X, \mathcal{N})$  je matroid. Hodnotou množiny  $A \subseteq X$  voláme veľkosť nejakej bázy  $B$  množiny  $A$  a známe ako  $r(A) := |B|$ .

**Veta 3.1.4.** Nech  $(X, \mathcal{N})$  je matroid a  $r : \mathcal{P}(X) \rightarrow \mathbb{N}_0$  je jeho hodnotná funkcia. Potom platí:

1.  $r(\emptyset) = 0$

$$2. r(\{x\}) \leq 1$$

$$3. A \subseteq B \implies r(A) \leq r(B)$$

$$4. r(A \cup B) \leq r(A) + r(B) - r(A \cap B) \text{ (semimodularita)}$$

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

**Veta 3.1.5.** 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

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

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

**Definícia 3.1.4.** Nech  $M = (X, \mathcal{N})$  je matroid a  $A \subseteq X$ . Prvok  $x \in X$  voláme závislý od množiny  $A$  v matroide  $M$ , ak  $r(A) = r(A \cup \{x\})$ .

**Definícia 3.1.5.** Nech  $M = (X, \mathcal{N})$  je matroid a  $A \subseteq X$ . Úzaverom 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 3.1.6.** Nech  $M = (X, \mathcal{N})$  je matroid a  $A \subseteq X$ . Potom platí:

$$1. A \subseteq \bar{A}$$

$$2. \bar{\bar{A}} = \bar{A}$$

$$3. \bar{A} = \bigcup_{B \in \mathcal{P}(X)} \{B \mid B \supseteq A \wedge r(B) = r(A)\}$$

$$4. r(A) = r(\bar{A})$$

**Veta 3.1.7.** Nech  $M = (X, \mathcal{N})$  je matroid a  $\Phi : \mathcal{P}(X) \rightarrow \mathcal{P}(X)$  je jeho úzaverová funkcia (t.j.  $\Phi(A) = \bar{A}$ ). Potom platí:

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

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

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

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

**Definícia 3.1.6.** 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:

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

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

**Veta 3.1.8.** 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

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

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

## 3.2 Dualita matroidov a triedy matroidov

**Veta 3.2.1.** (veta o dualite)

Nech  $M = (X, \mathcal{N})$  je matroid. Nech  $\mathcal{B}$  je množina báz matroidu  $M$  a  $r : \mathcal{P}(X) \rightarrow \mathbb{N}_0$  je hodnotná funkcia matroidu  $M$ . Ďalej nech:

- $\mathcal{B}^* := \{X - B \mid B \in \mathcal{B}\}$
- $\mathcal{N}^* := \{X - A \mid A \subseteq X \wedge r(A) = r(X)\}$
- $r^* : \mathcal{P}(X) \rightarrow \mathbb{N}_0$  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 hodnotnou funkciou nejakého matroidu
4. navyše, všetky 3 vyššie uvedené matroidy sú rovnaké

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

**Definícia 3.2.1.** Nech  $X := \{1, \dots, n\}$ ,  $\mathcal{N} := \{A \mid A \subseteq X \wedge |A| \leq k\}$ . Potom dvojica  $U_k^n = (X, \mathcal{N})$  je matroid.

**Veta 3.2.2.**  $(U_k^n)^* = U_{n-k}^n$

**Veta 3.2.3.** Nech  $M(G)$  je grafový matroidu grafu  $G$ . Potom nasledujúce podmienky sú ekvivalentné:

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

**Definícia 3.2.2.** 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  $f : X \rightarrow V$  také, že

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

**Definícia 3.2.3.** Matroid je reprezentovateľný, ak je  $F$ -reprezentovateľný nad nejakým polom  $F$ .

**Definícia 3.2.4.** Matroid je binárny, ak je  $GF(2)$ -reprezentovateľný.

**Definícia 3.2.5.** Matroid je regulárny, ak je  $F$ -reprezentovateľný nad každým polom  $F$ .

**Veta\* 3.2.4.** Každý grafový matroid je regulárny.

**TODO** Cayleho grafy?

**TODO** rezy a kružnice sú kolmé v každej reprezentácii?

**Definícia 3.2.6.** (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  $Y$ .

**Definícia 3.2.7.** (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  $Y$ .

**Veta 3.2.5.**  $(M.Y)^* = M^*/_Y$

**Definícia 3.2.8.** Matroid  $M'$  je minorom matroidu  $M$ , ak sa matroid  $M'$  dá dostať z matroidu  $M$  pomocou postupnosti zúžení a kontrakcií.

**TODO** Fannov matroid

**Veta\* 3.2.6.** (*Charakterizácia tried matroidov*)

Oznáčme Fannov matroid ako  $\mathcal{F}$ .

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

**Definícia 3.3.1.** Problém maximálnej množiny je trojica  $(X, \mathcal{M}, c)$ , kde  $X = x_1, \dots, x_n$  je množina objektov,  $\mathcal{M} \subseteq \mathcal{P}(X)$  je množina prípustných riešení a  $c : X \rightarrow \mathbb{R}^+ \cup \{0\}$  je cenová funkcia, rozširiteľná 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,

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

**Definícia 3.3.2.** (Pažravý algoritmus)

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

1.  $M_0 := \emptyset$
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 3.3.1.** (*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