

Kombinatorické struktury

prof. RNDr. Jan Kratochvíl, CSc.

6. července 2021

Obsah

1	Konečné/Afinní projektivní roviny	2
1.1	KPR a extrémální grafy	6
2	Latinské čtverce	6
3	Bloková schémata	12
3.1	Symetrické blokové schéma	14
3.2	Steinerovy systémy trojic	20
3.3	Hadamardovy matice	24
4	Latinské čtverce podruhe	29
5	Konečné projektivní prostory	35

1 Konečné/Afinní projektivní roviny

Definice 1.1 (Množinový systém). Necht X, I jsou množiny. Pak

$$\mathcal{M} = (M_i)_{i \in I}, \forall i \in I : M_i \subseteq X$$

nazveme množinovým systémem.

Kromě množinového zápisu a *Vennova diagramu* také můžeme incidenci značit incidenční maticí $A_{\mathcal{M}} \in \{0, 1\}^{X \times I}$, kde $A_{x,i} = 1$, právě když $x \in M_i$. Alternativou je také bipartitní graf incidence, který definujeme jako

$$B_{\mathcal{M}} = (X \cup I, \{\{x, i\} : x \in M_i\})$$

Definice 1.2 (Konečná projektivní rovina). Konečná projektivní rovina (KPR) je množinový systém $\mathcal{P} = (X, \mathcal{L})$ splňující následující axiomy:

- (A1) Pro každé dvě různé množiny $A, B \in \mathcal{L}$ platí $|A \cap B| = 1$
- (A2) Pro každé dva různé prvky $x, y \in X$ existuje $A \in \mathcal{L}$ taková, že $x, y \in A$
- (A3) V X existují čtyři prvky tak, že žádné tři z nich nepatří do stejné množiny z \mathcal{L} .

Je zvykem prvkům množiny X říkat body a množinám z \mathcal{L} přímky.

Poznámka 1.3 (Každé dva body v KPR sdílejí právě jednu přímku). Pokud $\mathcal{P} = (X, \mathcal{L})$ splňuje A1 a A2, pak každé dva různé body $x, y \in X$ náležejí právě jedné společné přímce.

Důkaz. Mějme $x, y \in X$ různé. Z A2 máme, že existuje alespoň jedna $A \in \mathcal{L}$ taková, že $x, y \in A$. Pro spor předpokládejme, že existuje i odlišná $B \in \mathcal{L}$ taková, že $x, y \in B$. Pak přímky A a B nesplňují A1, neboť $A \cap B \supset \{x, y\}$, a tedy $|A \cap B| \geq 2$, což je spor. \square

Poznámka 1.4 (O ekvivalentním axiomu ke čtveřici v KPR). Pokud systém $\mathcal{P} = (X, \mathcal{L})$ splňuje A1 a A2, pak A3 je ekvivalentní axiomu

- (A3') Body systému \mathcal{P} nemohou být pokryty jednou nebo dvěma přímkami z \mathcal{L} .

Důkaz. TODO \square

Věta 1.5 (O řádu KPR). Pro každou KPR $\mathcal{P} = (X, \mathcal{L})$ existuje přirozené číslo m takové, že

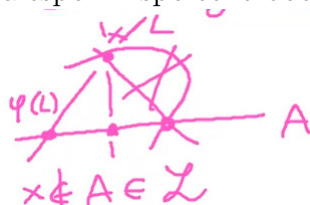
- $\forall A \in \mathcal{L} : |A| = m + 1$
- $\forall x \in X : |\{A \in \mathcal{L} : x \in A\}| = m + 1$
- $|X| = |\mathcal{L}| = m^2 + m + 1$

Toto číslo m nazýváme **řádem roviny** \mathcal{P} a můžeme psát $KPR(m)$ pro konečnou projektivní rovinu řádu m .

Důkaz. Vezmeme $x \notin A \in \mathcal{L}$. Definujme zobrazení které přiřazuje bod z přímky L bod na A :

$$\varphi : \{L : x \in L \in \mathcal{L}\} \rightarrow A$$

Neboli $\varphi(L)$ je průsečík s přímkou A (právě jeden společný bod). Různým přímkám přiřadí různé body. Necht sporem existují 2 přímky kterým φ přiřadilo stejný bod, pak mají alespoň 2 společné body. Spor s axiomem A1 Definice 1.2. Proto φ je prosté.



Na druhou stranu, každý bod A protíná ještě nějaká přímka $\Rightarrow \varphi$ je na. Neboli φ je bijekce.

Vezmeme 2 přímky A, B . Dle A3 nemůže pokrývat celou KPR.

$$\exists y : y \notin A \wedge y \notin B$$

Jelikož φ je bijekce

$$|A| = \# \text{ přímek procházejících } y = |B|$$

Dohromady

$$\exists m : \forall A \in \mathcal{L} : |A| = m + 1$$

Nechť $A \in \mathcal{L}$ libovolná přímka, má $(m + 1)$ bodů. Dal bodem $v \in A$ prochází dalších m přímek, pro nichž v je jediným společným bodem, ostatní jsou různé. Nazveme je vodorovné. Každá z nich má dalších $(m + 1) - 1 = m$ bodů, dohromady m^2 . Vezmeme další bod $s \in A$. Tím prochází dalších m přímek a musí protínat vodorovné právě v 1 bodě. Říkáme jim svislé. Z ostatních bodů A taky vychází svazek m přímek, další body již ale nejsou.

Tedy celkem $|X| = |\mathcal{L}| = m^2 + m + 1$ bodů a $|\mathcal{L}| = 1 + m(m + 1)$ přímek.

Kanonický obrázek KPR:

"Přímky" se nerovnají geometrickým přímkám, jen mnemonický název. □

Věta 1.6 (Existence KPR). Je-li $m = p^r$ mocnina prvočísla, pak existuje $KPR(m)$.

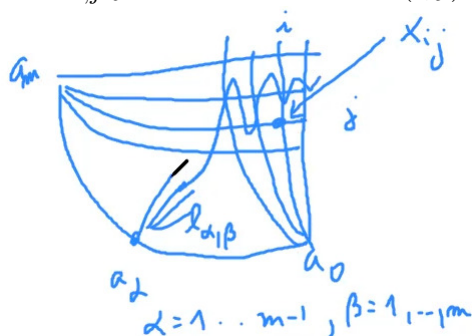
Důkaz. Konstruktivně pomocí mod aritmetiky. Z algebry $\exists GF(m)$ napíšeme jako

$$\{1, \dots, m = 0\}$$

Nechť $A = \{a_0, \dots, a_{m-1}\}$ je přímka. Označme svazek přímek vycházející z bodu a_k :

$$\forall k \in \{0, \dots, m-1\}, \forall b \in [m] : l_{k,b} = \{a_k\} \cup \{x_{i,k \cdot i + b} : i \in [m]\} \quad (1)$$

kde $x_{i,j}$ je bod se souřadnice (i, j) v šachovnici.



Šikmé přímky taky lze vyjádřit pomocí vzorečku (1):

$$\forall b \in [m] : l_{m,b} = \{a_m\} \cup \{x_{i,m \cdot i + b} : i \in [m]\}$$

Ověříme axiomy Definice 1.2:

(A1) Rozborem případů:

1. přímky ze stejného svazku dle jednoznačnosti aritmetiky modulo v tělese mají společný prvek pouze a_k .
2. Stejně pro šikmé přímky, protože je lze stejně vyjádřit.
3. Jednobodový průnik přímek ze svazku a vodorovných zaručuje jednoznačný bod $x_{i,j}$.
4. Potřebujeme ukázat

$$\forall k_1 \neq k_2, \forall b_1, b_2 : |l_{k_1, b_1}, l_{k_2, b_2}| = 1$$

Dle definice přímek ze svazku bod v průniku má souřadnice:

$$x_{i,j} = x_{i,k_1 \cdot i + b_1} = x_{i,k_2 \cdot i + b_2} \Rightarrow k_1 \cdot i + b_1 = k_2 \cdot i + b_2 \iff i = (b_1 - b_2) \cdot (k_2 - k_1)^{-1}$$

Z vlastnosti konečného tělesa, takové i je jednoznačné.

(A2) Není potřeba ukazovat rozborem případu. Stačí sečíst dvěma způsoby

$$C = |\{(x, y), A) : x, y \in A, x \neq y, A \in \mathcal{L}\}|$$

máme $(m+1)$ přímek a $\binom{m+1}{2}$ způsobů zvolit body. Taký ale z A1 2 body spojuje nejvýše 1 přímka, proto $\binom{m^2+m+1}{2} \geq C$ Dohromady

$$\binom{m^2+m+1}{2} = (m^2+m+1)m(m+1) \geq C = (m+1) \cdot \binom{m+1}{2} = (m^2+m+1)m(m+1)$$

Z rovnosti usoudíme, že každé dvojice odpovídá právě jedna přímka.

(A3) TODO z konstrukce?

□

Conjecture 1.7. $KPR(m)$ existuje, právě když m je mocnina prvočísla

Věta 1.8 (KPR(6), Dk později). $KPR(6)$ neexistuje.

Poznámka 1.9. $KPR(10)$ neexistuje, ale jediný známý důkaz je počítačovým rozborem případů.

Neznáme žádnou KPR s řádem rozdílným od mocniny prvočísla. Zároveň však známe nekonečně mnoho m takových, že $KPR(m)$ neexistuje. Nejmenší otevřený případ je $m = 12$.

Definice 1.10 (Konečná afinní rovina). Konečná afinní rovina (KAR) je množinový systém $\mathcal{P} = (X, \mathcal{L})$ splňující následující axiomy:

(AF1) Pro každé dva různé prvky $x, y \in X$ existuje právě jedna množina $A \in \mathcal{L}$ taková, že $x, y \in A$

(AF2) Pro každou množinu $A \in \mathcal{L}$ a každý prvek $x \in X$ nenáležící do A existuje právě jedna množina $B \in \mathcal{L}$ taková, že $x \in B$ a $A \cap B = \emptyset$

(AF3) V X existují tři prvky, které nepatří do stejné množiny z \mathcal{L}

Prvkům množiny X říkáme body, množinám z \mathcal{L} říkáme přímky, dvě množiny s prázdným průnikem jsou rovnoběžky a dvě množiny s neprázdným průnikem jsou různoběžky.

Poznámka 1.11 (O relaci rovnoběžnosti a směrech). Rovnoběžnost přímek v KAR je tranzitivní a symetrická relace na \mathcal{L} . Její reflexivní zúplnění je tedy ekvivalence a \mathcal{L} se tedy rozpadá na několik tříd ekvivalence. Těmito třídám říkáme směry. Přímky různých směrů jsou různoběžné.

Q: co když přímky husté?

Q: co když slepíme směry dle ekvivalence?

A: Jak slepit? Neporuší to axiomy?

Q: souvisí KAR s hyperbolickou geometrií Lobačevského?

A: ano, ale nevíme co dříve.

Věta 1.12 (O řádu KAR). Pro každou KAR $\mathcal{P} = (X, \mathcal{L})$ existuje $m \in \mathbb{N}$ (nazývané řád roviny \mathcal{P}) takové, že:

- $\forall a \in \mathcal{L} : |A| = m$
- $\forall x \in X : |\{A \in \mathcal{L} : x \in A\}| = m + 1$
- $|X| = m^2$
- $|\mathcal{L}| = m^2 + m$
- počet směrů přímek je $m + 1$, přičemž každý směr obsahuje m rovnoběžných přímek

Důkaz. Vezmeme $x \notin A \in \mathcal{L}$. Definujme zobrazení které přiřazuje bod z přímky L bod na A :

$$\varphi(L) = L \cap A, \varphi : \{L : x \in L \in \mathcal{L}, L \not\parallel A\} \rightarrow A$$

Z AF1 φ je prosté a je definované pro všechny body A proto φ je na \Rightarrow bijekce.

Jelikož φ je bijekce a z AF2 existuje právě 1 rovnoběžka k A procházející bodem x :

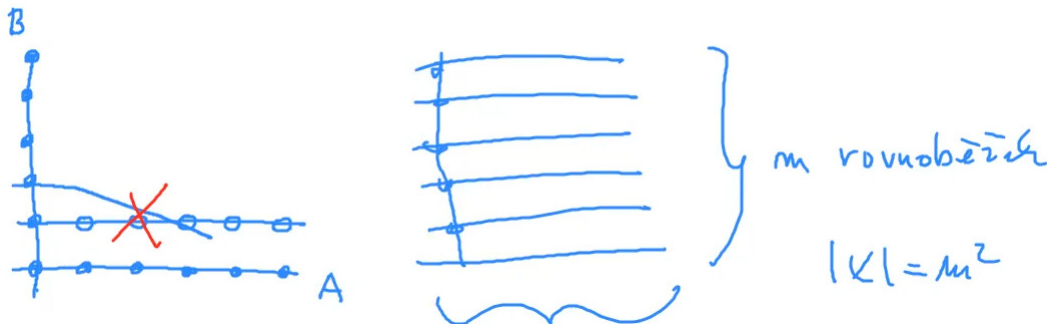
$$|A| + 1 = \# \text{ přímek obsahujících } x \quad (2)$$

Vezmeme 2 přímky $A, B : A \not\parallel B$. Dle AF1, AF2, AF3 \Rightarrow nejde pokryt 2ma různoběžnými přímkami. Pak $\exists t \notin A \cup B$, zobrazení φ určuje přímku pro každý bod A, B . Neboli $|A| = |B|$.

Vezmeme 2 rovnoběžky A, B a různoběžku C z předchozího případu usoudíme $|A| = |C| = |B|$.

Dohromady $\exists m, \forall A \in \mathcal{L} : |A| = m$. Taky z (2):

$$|\{L : x \in L \in \mathcal{L}\}| = m + 1$$

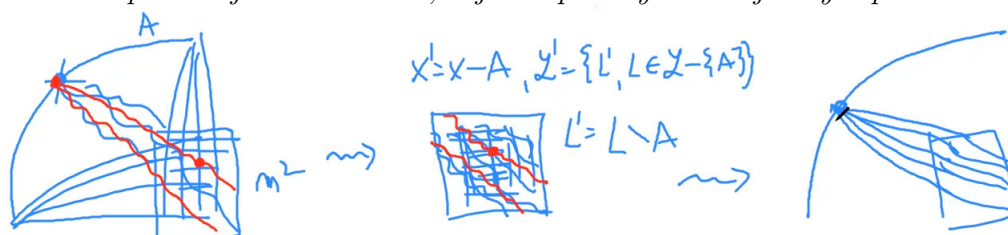


Vezmeme libovolnou přímku A , má m bodů. Přes libovolný bod $a \in A$ prochází další přímka B . Dle AF2 najdeme ke každému bodu $b_i \in B$ rovnoběžku k A která má dalších $(m-1)$ bodů. Konstrukce dává m rovnoběžek a m^2 bodů. Dohromady $|X| = m^2$. Na jedné straně, počet bodů je m^2 . Každým bodem prochází $(m+1)$ přímek. Na druhé straně se to rovná počtu přímek krát počet bodů na přímce m .

$$m^2 \cdot (m+1) = |\mathcal{L}| \cdot |A| = |\mathcal{L}| \cdot m \Rightarrow |\mathcal{L}| = m \cdot (m+1)$$

□

Důsledek 1.13 (O vztahu KAR a KPR). Každá afinní rovina řádu m vznikne z projektivní roviny řádu m vynecháním jedné přímky a jejích bodů. Naopak každá projektivní rovina řádu m vznikne z nějaké afinní roviny řádu m přidáním $m+1$ bodů, každý z nich do všech přímek jednoho směru, a jedné přímky obsahující tyto přidané body.



Definice 1.14 (Desargova vlastnost). Desargova vlastnost je následující: Pro každých šest různých bodů $A_1, A_2, B_1, B_2, C_1, C_2$ takových, že se přímky A_1A_2, B_1B_2, C_1C_2 protínají v jednom bodě platí, že průsečíky dvojic přímek A_1B_1, A_2B_2 a B_1C_1, B_2C_2 a A_1C_1, A_2C_2 leží na jedné přímce.

Definice 1.15 (Desargovská projektivní rovina). Projektivní rovina je Desargovská, pokud má Desargovu vlastnost. Jinak je ne-Desargovská.

Cvičení 1.16. KPR sestrojené výše jsou Desargovské.

1.1 KPR a extrémální grafy

Příklad 1.17 (Extremální Moorovy grafy).

Příklad 1.18 (Copnumber grafu).

2 Latinské čtverce

Definice 2.1 (Latinský obdélník). Latinský obdélník je matice $L \in X^{k \times n}$. Taková, že prvky se neopakují ani ve sloupcích ani v řádcích. Kde X je n -prvková množina. Typický $\{1, \dots, n\} := [n]$.

Na řádky lze nahlížet jako na permutace.

Věta 2.2 (Latinské čtverce). Každý Latinský obdélník řádu $k \times n$ lze doplnit na Latinský čtverec řádu $n \times n$.

Důkaz. Dokážeme přidání nových řádků v závislosti na již existujících řádcích. V k -tem kroku se podíváme na j -tý sloupec. Nechť M_j bude množina kandidátů které můžeme dat na j -tou pozici v novém řádku.

$$M_j = [n] \setminus \{L_{ij} : i = 1, 2, \dots, k\}$$

Ted musíme z množin M_j vzít po 2 různé prvky. Jinými slovy, hledáme Systém různých reprezentantů - SRR pro $\{M_j\}_1^n$.

Sestavíme graf, kde vrcholy jsou množiny M_j a prvky z $[n]$.

$$(l, M_j) \in E \iff l \in M_j$$

Pak tento bipartitní graf je $(n - k)$ -regulární. Protože $\forall x$ je v $(n - k)$ množinách M_j .

Dle Hallové věty, v takovém grafu existuje perfektní párování, které určuje SRR. \square

Důsledek 2.3. *Latinských čtverců řádu n je $\mathcal{O}(n!)$.*

Důkaz. BUNO: v prvním řádku je $\{1, 2, \dots, n\}$. Jinak můžeme vhodně přejmenovat prvky. V druhém řádku musí být permutace $[n]$ bez pevných bodů. Z *problému šatnářky* takových permutací je

$$\frac{n!}{e}$$

Pak dle věty každý obdélník lze doplnit na čtverec. \square

Definice 2.4 (Kolmost LČ). Latinský čtverce jsou kolmé $L \perp L'$ právě když

$$\forall x, y \in [n]^2 \exists! (i, j) \in [n]^2 : L_{i,j} = x \wedge L'_{i,j} = y$$

Taky lze definovat ortogonalitu nad různými množiny.

Značení 2.5 (NOLČ(n)). $NOLČ(n)$ značíme největší počet navzájem ortogonálních Latinských čtverců řádu n .

Věta 2.6 (Horní odhad NOLČ).

$$\forall n \in \mathbb{N}, n > 1 : NOLČ(n) \leq n - 1$$

Důkaz. Necht

$$L^1, \dots, L^t \in \{1, \dots, n\}^{n \times n}, \forall i \neq j : L^i \perp L^j$$

BUNO: přejmenujeme prvky v každém LČ tak, aby v prvním řádku bylo $\{1, 2, \dots, n\}$. Takto vyrobíme LČ L^1, \dots, L^t .

Tvrdíme ale, že ortogonalita je zachovaná. Obecně pro libovolná permutace π aplikovaná na jeden z dvojice ortogonálních LČ zachovává ortogonalitu.

Pak na pozici $(2, 1)$ nemůže být 1. Pokud tam ale bude nějaké písmeno a , tak čtverce nebudou ortogonální, protože všechny dvojice (i, i) máme v prvním řádku. Z toho na pozici $(2, 1)$ můžou být prvky $\{2, \dots, n\}$ po 2 různé. Takže $NOLČ(n) \leq n - 1$. \square

Kdy máme extrémální řešení?

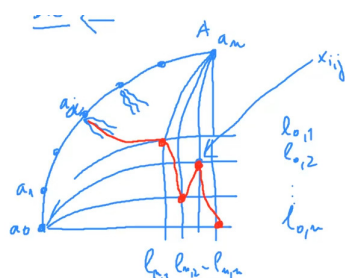
Věta 2.7 (Extremální NOLČ a KPR).

$$NOLČ(n) = n - 1 \iff \exists KPR(n)$$

Z předchozí přednášky platí pro mocniny prvočísla.

Důkaz. $KRP \Rightarrow LČ$. Sestavíme nevlastní přímku A, svislé a vodorovné přímky. Dal přímky spojující A a průniky svislých a vodorovných přímek budou určovat LČ.

$$L_{i,j}^\alpha = \beta \iff x_{i,j} \in k_{\alpha,\beta}$$



Pak písmena v LČ odpovídající červené přímce budou:



Z axiomu KPR svislé, vodorovné a přímky procházející body a_α se protínají právě v 1 bodě. Takže písmena se neopakují v řádcích a sloupcích. Jsou \perp protože

$$\forall \beta, \beta' \exists!(i, j) : L_{i,j}^\alpha = \beta \wedge L_{i,j}^\gamma = \beta'$$

Protože přímky se nemůžou protínat na nevlastní přímce A, takže se protínají uvnitř šachovnice.

$$\exists! x_{i,j} \in l_{\alpha,\beta} \cap l_{\gamma,\beta'}$$

$LČ \Rightarrow KPR$. Necht máme LČ

$$L^\alpha, \alpha \in \{1, 2, \dots, n-1\}$$

Sestavíme nevlastní, svislé a vodorovné přímky.

Šikmé přímky vytvoříme dle:

$$L_{i,j}^\alpha = \beta \iff x_{i,j} \in k_{\alpha,\beta}$$

Ověříme axiomy:

- A_1 . Přímky ze stejného svazku šikmých přímek se protínají v nevlastním bodě. Vodorovné a svislé se protínají v šachovnici.
Šikmé vs svislé a Vodorovné vs svislé se protínají protože průniky jsou určeny LČ. 2 Šikmé přímky se protínají právě v 1 bodě protože čtverce jsou \perp .
- A_3 . Plyne z toho, že $n \geq 2$.
- A_2 . Spočítáme 2ma způsoby \neq 3jic.

$$T = |\{(x, y), l) : x \neq y \in X, l \in L, x, y \in l\}|$$

Máme $(n^2 + n + 1)$ přímek, na každé z nich je $(n + 1)$ bodů. Pak

$$T = (n^2 + n + 1) \binom{n+1}{2}$$

Na druhou stranu, máme $(n^2 + n + 1)$ bodů. Každou 2ci prochází nejvýše 1 přímka.

$$T \leq 1 \cdot \binom{n^2 + n + 1}{2}$$

Dohromady

$$(n^2 + n + 1) \binom{n + 1}{2} \leq \binom{n^2 + n + 1}{2}$$

Po roznásobení dostaneme stejná čísla na obou stranách, což může nastat pouze v případě že každou 2ci bodů prochází *právě* 1 přímka.

□

Definice 2.8 (Ortogonalní tabulka). Ortogonalní tabulka řádu n , hloubky d je matice

$$M \in \{1, \dots, n\}^{d \times n^2}$$

d řádků, n sloupců. Každé 2 řádky jsou ortogonální. Formálně:

$$\forall i \neq j, \forall x, y \in [n], \exists! k \in \{1, \dots, n^2\} : M_{i,k} = x \wedge M_{j,k} = y$$

Poznámka 2.9. Jelikož počet 2jic je právě n^2 , což se rovná počtu sloupců stačí i slabší podmínka.

$$\forall i \neq j, \forall x, y \in [n], \exists k \in \{1, \dots, n^2\} : M_{i,k} = x \wedge M_{j,k} = y$$

Věta 2.10 (Ortogonalní tabulka a NOLČ).

$$\forall n, d \in \mathbb{N} \exists OA(n, d) \iff NOLČ(n) \geq d - 2$$

Důkaz. BUNO první řádek má bloky i, i, \dots, i velikosti n . Druhý řádek bloky $1, 2, \dots, n$ taky velikosti n . Jinak zvolíme vhodnou permutaci.

Pak vezmeme libovolný další řádek. Přemístíme blok velikosti n na řádek LČ.

$$L_{i,j}^3 = M_{3,n(i-1)+j}$$

Tvrdíme, že je to LČ.

- v řádku nemůže být dvakrát stejné písmeno, třeba pokud by tam bylo a . Měli bychom v původní tabulce dvakrát (i, a) v různých řádcích.
- Pokud bychom měli v sloupci 2 stejná písmena, např ve sloupci j . Tak bychom měli (j, b) na stejné pozici j . Jelikož 2. řádek má stejné bloky, tak by řádek ze kterého jsme udělali LČ nebyl \perp s 2. řádkem.

Když budeme mít 2 LČ z ortogonalní tabulky, tak jsou ortogonální. Řádky tabulky jsou kolmé \Rightarrow řádky LČ jsou kolmé.

První 2 řádky jsou zafixované, z dalších můžeme vyrobit \perp LČ. Takže dohromady $(d - 2)$. Obráceně, pokud máme $(d - 2)$ LČ, tak je poskládáme do OA. □

Věta 2.11 (Tenz produkt Ortogonalních tabulek).

$$\forall n_1, n_2, d \in \mathbb{N} \exists OA(n_1, d) \wedge OA(n_2, d) \Rightarrow \exists OA(n_1 \cdot n_2, d)$$

Důkaz. Mějme řádek z $OA(n_1) : a_1, a_2, \dots, a_n$ a řádek z $OA(n_2) : b_1, b_2, \dots, b_n$.
Uděláme výsledný řádek pomocí tenzorového součinu:

$$(a_1, b_1)(a_1, b_2), \dots (a_1, b_{n_2})(a_2, b_1) \dots$$

Vezmeme 2 řádky $OA(n_1 \cdot n_2, d)$. Necht $x = (c, d), y = (c', d')$.

Z vlastnosti OA, $\exists! k : c$ je ve stejném sloupci s c' v $OA(n_1)$. Analogický $\exists! l : d$ je ve stejném sloupci s d' v $OA(n_2)$.

Pak z definice tenzorového součinu v $OA(n_1 \cdot n_2, d) \exists! (a_k, a_l)$. Z toho $\forall c, d, c', d', \exists!$ sloupec ve kterém v tabulce jsou $(c, d) \wedge (c', d')$. \square

Věta 2.12 (Dolní odhad NOLČ). *Necht $n = \prod_1^k p_i^{r_i}$ je faktorizace n . Pak*

$$NOLČ(n) \geq \min_{i=1}^k \{p_i^{r_i} - 1\}$$

Důkaz. Necht

$$s = \min_{i=1}^k \{p_i^{r_i} - 1\}$$

Z věty 2.6

$$NOLČ(p_i^{r_i}) \geq p_i^{r_i} - 1$$

Pak protože $s = \min \Rightarrow p_i^{r_i} - 1 \geq s$.

Což spolu s větou 2.10 dává:

$$\exists OA(p_i^{r_i}, s+2)$$

Aplikujeme 2.11 induktivně, pak

$$\exists OA\left(\prod_1^k p_i^{r_i}, s+2\right) = OA(n, s+2) \Rightarrow NOLČ(n) \geq s$$

\square

Důsledek 2.13.

$$\forall n \in \mathbb{N}, n > 2 \wedge n \not\equiv 2 \pmod{4} : NOLČ(n) \geq 2$$

Důkaz. Rozložíme n na mocniny prvočísel. Pak pokud v rozkladu je 2, tak má exponent aspoň 2. Protože jinak je $n \not\equiv 2 \pmod{4}$, což jsme vyloučili předpokladem. Pro ostatní prvočísla $p_i^{r_i} - 1 \geq 2$. Dohromady $s \geq 2$. \square

Lemma 2.14 (OA $3m + 1$).

$$\exists OA(m, 4) \Rightarrow \exists OA(3m+1, 4)$$

Důkaz. Necht $X = \{x_1, x_2, \dots, x_m\}$. Dal vezmeme okruh \mathbb{Z}_{2m+1} a máme dle předpokladu $OA(m, 4)$

$$D = \begin{pmatrix} D_1 \\ D_2 \\ D_3 \\ D_4 \end{pmatrix}$$

Vezmeme

$$\begin{aligned}
a_i &= (i, i, \dots, i) \in \mathbb{Z}_{2m+1}^m \\
b_i &= (i+1, i+2, \dots, i+m) \in \mathbb{Z}_{2m+1}^m \\
c_i &= (i-1, i-2, \dots, i-m) \in \mathbb{Z}_{2m+1}^m \\
A &= (a_0, a_1, \dots, a_{2m}) \in \mathbb{Z}_{2m+1}^{m(2m+1)} \\
B &= (b_0, b_1, \dots, b_{2m}) \in \mathbb{Z}_{2m+1}^{m(2m+1)} \\
C &= (c_0, c_1, \dots, c_{2m}) \in \mathbb{Z}_{2m+1}^{m(2m+1)} \\
X &= (x_1, x_2, \dots, x_m, x_1, x_2, \dots, x_m \dots) \in X^{m(2m+1)}
\end{aligned}$$

Pak sestavíme $OA(3m+1, 4)$ nad prvky $X \cup \mathbb{Z}_{2m+1}$ takto:

$$F = \begin{pmatrix} 0 & 1 & \dots & 2m & A & B & C & X & D_1 \\ 0 & 1 & \dots & 2m & B & A & X & C & D_2 \\ 0 & 1 & \dots & 2m & C & X & A & B & D_3 \\ 0 & 1 & \dots & 2m & X & C & B & A & D_4 \end{pmatrix}$$

Počet sloupců je

$$(2m+1) + 4m(2m+1) + m^2 = 9m^2 + 6m + 1 = (3m+1)^2$$

Tedž zkontrolujeme, že $\forall x, y \in X, \forall i, j \in \mathbb{Z}_{2m+1}$ najdeme následující dvojice v sloupcích aspoň jednou.

$$z_{i,i} = \binom{i}{i}, z_{i,j} = \binom{i}{j}, z_{i,x} = \binom{i}{x}, z_{x,i} = \binom{x}{i}, z_{x,y} = \binom{x}{y}$$

Pak kvůli velikosti tabulky dvojice bude v OA právě jednou.

- $z_{i,i}$ je na začátku v $0, 1, \dots, m$.
- $z_{i,j}$ je v $\binom{A}{B} \cup \binom{B}{A}$ nebo $\binom{A}{C} \cup \binom{C}{A}$ nebo $\binom{B}{C} \cup \binom{C}{B}$
- $z_{i,x}$ je v $\binom{A}{X} \vee \binom{B}{X} \vee \binom{C}{X}$
- $z_{x,i}$ je v $\binom{A}{X} \vee \binom{B}{X} \vee \binom{C}{X}$
- $z_{x,y}$ je v D .

□

Věta 2.15 (Dolní odhad NOLČ - 2).

$$\forall k > 0 : NOLČ(12k+10) \geq 2$$

Důkaz. Pokud vezmeme $m = 4k+3$ pak dle 2.13

$$\exists OA(4k+3, 4) \stackrel{lemmga}{\Rightarrow} 2.14 \exists OA(3(4k+3)+1, 4) = OA(12k+10, 4) \iff NOLČ(12k+10) \geq 2$$

□

Poznámka 2.16. Ortogonální tabulky se používají např pro rozvrhování turnaje kde každý hraje s každým jednou. Z toho turnaje mají určitý počet hráčů, aby existovala příslušná OA.

V bridge to je složitější, protože nejlepší hraje s nejhorším. Po nějakém počtu roundů už nejde pokračovat dal.

3 Bloková schémata

Definice 3.1 (Blokové schéma (BIBD)). Blokové schéma s parametry $v, k, \lambda > 0$ $((v, k, \lambda)$ -BIBD) je množinový systém (V, \mathcal{B}) takový, že:

1. $|V| = v$
2. $\forall B \in \mathcal{B} : |B| = k$
3. $\forall x, y \in V, x \neq y : |\{B \in \mathcal{B} : x, y \in B\}| = \lambda$
4. $v > k$, netrivialita: bloky neobsahují všechny prvky.

Množiny $B \in \mathcal{B}$ jsou *bloky* schématu (V, \mathcal{B}) .

Vlastnosti 3.2 (BIBD).

BIBD reprezentujeme pomocí matice incidence, pro niž platí:

- Z 2 axiomu, sloupcový součet je právě k .
- Z 3 axiomu, libovolné 2 sloupce mají jedničky na λ společných pozicích. Neboli skalární součet je λ .

Věta 3.3 (Struktura BIBDu). *Nechť (V, \mathcal{B}) je (v, k, λ) -BIBD, pak*

1. $\forall x \in V$ patří to $r = \frac{\lambda(v-1)}{k-1}$ bloků.
2. $|\mathcal{B}| = \frac{\lambda v(v-1)}{k(k-1)}$

Důkaz. 1) ekvivalentně znamená, že řádkové součty matice se rovnají r . Zafixujeme libovolný prvek $x \in V$. Pak

$$r_x = |\{B : x \in B \in \mathcal{B}\}|$$

Spočítáme 2ma způsoby # dvojic:

$$C = |\{(y, B) : x \neq y, x, y \in B \in \mathcal{B}\}|$$

Na jedné straně je r_x způsobů zvolit B obsahující x a $(k-1)$ možností zvolit další prvek $y \in B$.

Na druhou stranu, nejprve zvolíme y , což jde udělat $(v-1)$ způsoby. Z axiomu 3 takové x, y jsou ve λ společných množinách.

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

Konečně, x byl libovolný prvek, rovnost platí $\forall x \in V$.

2) Jaký je součet všech prvků matice? Spočítáme po řádcích a po sloupcích

$$|\mathcal{B}| \cdot k = RS = SlS = v \cdot r = v \cdot \frac{\lambda(v-1)}{k-1} \Rightarrow |\mathcal{B}| = \frac{\lambda v(v-1)}{k(k-1)}$$

□

Vlastnosti 3.4 (Struktura BIBDu).

Pokud pro parametry $\exists(v, k, \lambda)$ -BIBD, tak:

D1 $\lambda(v-1)$ je dělitelné $(k-1)$.

D2 $\lambda \cdot v(v-1)$ je dělitelné $k \cdot (k-1)$.

- $r > \lambda$.

Důkaz. Plyne hned z 3.3, jelikož $r, |\mathcal{B}|$ jsou celá čísla.

3 podmínka platí z předpokladu netriviality

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

□

Příklad 3.5. Každá KPR(m) je $(m^2 + m + 1, m + 1, 1)$ -BIBD.

Každá KAR(m) je $(m^2, m, 1)$ -BIBD.

Věta 3.6 (Wilson (1975) BD).

$$\forall k, \lambda \exists v_0 : \forall v \geq v_0 \wedge [D1] + [D2] \Rightarrow \exists(v, k, \lambda) - BIBD$$

Věta 3.7 (Fisherová nerovnost). Pokud (V, \mathcal{B}) je (v, k, λ) -BIBD tak $|\mathcal{B}| \geq v$.

Důkaz. Trik jako v mnoha důkazech přednášky LAK, mocnění matice incidence. Necht A je matice incidence BIBDu, pak

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

Spočítáme determinant pomocí vzorečku multilineární formy

$$\det AA^T = (r - \lambda)^v + v \cdot \lambda \cdot (r - \lambda)^{v-1} = (r - \lambda)^{v-1}(r - \lambda + v\lambda) = (r - \lambda)^{v-1}(v(\lambda - 1) + r)$$

Dle Vlastnosti 3.4 $r > \lambda \Rightarrow (r - \lambda)^{v-1} > 0$. Dle axiomu BIBDu $\lambda - 1 \geq 0$ a $r > 0$. Takže i determinant je nenulový. Pak z LA

$$\text{rank} AA^T = v \leq \text{rank} A \leq |\mathcal{B}| \Rightarrow |\mathcal{B}| \geq v$$

□

Důsledek 3.8. Pro každý BIBD $k \leq r$.

Důkaz.

$$|\mathcal{B}| \cdot k = v \cdot r \wedge |\mathcal{B}| \geq v \Rightarrow k \leq r$$

□

3.1 Symetrické blokové schéma

Definice 3.9 (Symetrické blokové schéma). Blokové schéma se nazývá symetrické, pokud je počet jeho bloků roven počtu jeho prvků.

$$|\mathcal{B}| = v$$

Neboli extrémální případ Fisherové nerovnosti.

Věta 3.10 (Ekvivalence BIBD). *Nechť (V, \mathcal{B}) je množinový systém takový, že*

- $|V| = v$
- $|\mathcal{B}| = b$
- $A \in \{0, 1\}^{v \times b}$ je matice incidence
- $k, \lambda, r = \frac{\lambda(v-1)}{k-1} \in \mathbb{Z}^+$

Pak (V, \mathcal{B}) je (v, k, λ) -BIBD \iff :

1. $AA^T = \lambda J + (r - \lambda)E$
2. $JA = kJ \iff$ sloupcový součet v matice A je k .
3. $\text{rank} A = v$

Důkaz. " \Rightarrow ". Plyne z Fisherové nerovnosti 3.7. Z vlastnosti BIBDu Vlastnosti 3.4 sloupcový součet v matice A je $k \Rightarrow JA = kJ$.

" \Leftarrow ". Ověříme axiomy:

1. TODO není axiom ale označení proměnné?
2. $JA = kJ \Rightarrow$ sloupcový součet v matice A je $k \Rightarrow \forall B \in \mathcal{B} : |B| = k$
3. z 1 podmínky plyne, že mimo diagonálu v AA^T jsou λ . Což je skalární součin dvou libovolný řádku matice A .
4. Nechť sporem $v = k$, tak $A = J$ a pro $v \geq 2$ by již neměla plnou hodnotu. Spor s 3 podmínkou.

□

Věta 3.11 (SBIBD ekvivalence). *Nechť (V, \mathcal{B}) je množinový systém takový, že $|V| = |\mathcal{B}| > 1$ a A je matice incidence. Pak*

1. *Pokud je (v, k, λ) -SBIBD, tak*

- (a) $AA^T = \lambda J + (k - \lambda)E \iff \forall x \in V$ patří do k bloků, $\forall x \neq y \in V$ patří do λ bloků.
- (b) $A^T A = \lambda J + (k - \lambda)E$. Maticové násobení je skalárním součinem sloupců matice A , neboli se díváme na bloky. Rovnost ekvivalentně znamená, že na diagonále jsou velikosti bloku k a mimo diagonálu průniky bloků λ .

$$\forall B \in \mathcal{B} : |B| = k, \forall B_1 \neq B_2 \in \mathcal{B} : |B_1 \cap B_2| = \lambda$$

- (c) $JA = kJ \iff \forall$ prvek patří do k bloků.

(d) $AJ = kJ$ násobíme charakteristický vektor s $\bar{1}$. Neboli $\forall B \in \mathcal{B} : |B| = k$.

(e) A je regulární $\iff \text{rank} A = v$

2. Nechť A je regulární matice neboli platí e), potom pokud platí a) nebo b) $\Rightarrow (V, \mathcal{B})$ je (v, k, λ) -SBIBD.

Důkaz. Je vidět a) \Rightarrow c) a b) \Rightarrow d).

Dle 3.10 (v, k, λ) -SBIBD \iff a), d), e). Potřebujeme zkontrolovat že b) je splněno. Ukážeme ale 1 a 2 dohromady pomocí implikace

$$a), e) \Rightarrow b), d) \quad (3)$$

2 je splněná taky, protože a), e) $\stackrel{(3)}{\Rightarrow}$ b), d), c) znovu z 3.10 (V, \mathcal{B}) je (v, k, λ) -SBIBD. Obráceně pokud platí b), e) pro $A \Rightarrow$ platí a), e) pro $A^T \Rightarrow$ a)-e) pro $A^T \Rightarrow$ a)-e) pro A . Začneme d).

A regulární $\Rightarrow \exists A^{-1}$. Pak

$$A^{-1}AJ \stackrel{c)}{=} A^{-1}kJ = kA^{-1}J \stackrel{k \neq 0}{\neq} A^{-1}J = k^{-1}J$$

Dal

$$JA^T = J^T A^T = (AJ)^T = (kJ)^T = kJ$$

Taky

$$A^T = A^{-1}AA^T \stackrel{a)}{=} A^{-1}((k - \lambda)E + \lambda J) = (k - \lambda)A^{-1} + \lambda A^{-1}J = (k - \lambda)A^{-1} + \lambda k^{-1}J$$

Z rovnosti usoudíme, že $k \neq \lambda$ protože jinak A^T regulární $= c \cdot J$ která regulární není. Taky

$$JA^T = kJ = J((k - \lambda)A^{-1} + \lambda k^{-1}J) = (k - \lambda)JA^{-1} + \lambda k^{-1}J^2$$

Jelikož $J \in \{0, 1\}^{v \times v} \Rightarrow J^2 = vJ$ tak

$$JA^T = kJ = (k - \lambda)JA^{-1} + \lambda k^{-1}vJ \Rightarrow (k - \lambda)JA^{-1} = (k - \lambda k^{-1}v)J$$

Neboli

$$JA^{-1} = \frac{k - \lambda k^{-1}v}{k - \lambda} \Rightarrow J = JA^{-1}A = \frac{k - \lambda k^{-1}v}{k - \lambda}JA$$

Označme $m = \frac{k - \lambda k^{-1}v}{k - \lambda}$, dal

$$J^2 = vJ = (mJA)J = (mJ)AJ = mJkJ = mkJ^2 \Rightarrow mk = 1$$

Konečně máme d)

$$JA^{-1} = mJ = k^{-1}J \Rightarrow J = k^{-1}JA \Rightarrow JA = kJ$$

b)

$$A^T A = ((k - \lambda)A^{-1} + \lambda k^{-1}J)A = (k - \lambda)E + \lambda k^{-1}kJ = (k - \lambda)E + \lambda J$$

□

Důsledek 3.12 (Duální SBIBD). Pokud A je matice symetrického BIBDu $\Rightarrow A^T$ je matice duálního SBIBDu. Neboli

$$(V, \mathcal{B})^* = (\mathcal{B}, V^*), V^* = \{v^* : v \in V\}, v^* = \{B : v \in B \in \mathcal{B}\}$$

Definice 3.13 (Konstrukce blokových schémat ze symetrických). Pokud (V, \mathcal{B}) je (v, k, λ) -BIBD, nechť B_0 je zafixovaný blok, definujme:

1. $(B_0, \{B \cap B_0 : B \in \mathcal{B} \setminus \{B_0\}\})$ je $(k, \lambda, \lambda - 1)$ -BIBD (odvozové schéma neboli v aj derived design).
2. $(V \setminus B_0, \{B \setminus B_0 : B \in \mathcal{B} \setminus \{B_0\}\})$ je $(v - k, k - \lambda, \lambda)$ -BIBD (zbytkové schéma neboli v aj residual design).

Příklad 3.14 (KPR vs KAR). Každá konečná projektivní rovina je symetrický BIBD. Každá konečná afinní rovina je zbytkové schéma pro nějakou konečnou projektivní rovinu stejného řádu.

Lemma 3.15 (Lineární formy). Nechť $A \in \{0, 1\}^{v \times b}$ je matice incidence a $r = \frac{\lambda(v-1)}{k-1}$, pak uvažme lineární formy

$$\forall j \in [b] : L_j(x_1, \dots, x_v) = \sum_{i=1}^v a_{ij} x_i$$

Potom

$$\sum_{j=1}^b L_j^2(x_1, \dots, x_v) = (r - \lambda) \sum_{i=1}^v x_i^2 + \lambda \left(\sum_{i=1}^v x_i \right)^2$$

Důkaz. Budiž $x = (x_1, \dots, x_v)$ řádkový vektor proměnných. Označme $L_j = L_j(x_1, \dots, x_v)$, pak

$$xA = (L_1, \dots, L_b)$$

Dal

$$(xA)^T = A^T x^T = \begin{pmatrix} L_1 \\ L_2 \\ \dots \\ L_b \end{pmatrix}$$

Rovnici $AA^T = (r - \lambda)E + \lambda J$ vynásobíme x zleva a x^T zprava:

$$xAA^T x^T = x((r - \lambda)E + \lambda J)x^T$$

Kde levá strana je $(L_1, \dots, L_b) \cdot (L_1, \dots, L_b)^T = \sum L_j^2$. Pravá strana

$$x((r - \lambda)E + \lambda J)x^T = x(r - \lambda)x^T + \lambda xJx^T$$

Roznásobíme

$$(r - \lambda)xx^T + \lambda xJx^T = (r - \lambda) \sum x_i^2 + \lambda \left(\sum x_i \right) (x_1 + \dots + x_v) = (r - \lambda) \sum x_i^2 + \lambda \left(\sum x_i \right)^2$$

□

Věta 3.16 (Bruck-Ryser-Chowla). Nechť (v, k, λ) -SBIBD, položme $n = k - \lambda$, pak platí:

1. v je sudé a $n = m^2 \in \mathbb{N}$.
2. v je liché a Diofantická rovnice

$$z^2 = nx^2 + (-1)^{\frac{v-1}{2}} \lambda y^2$$

má netriviální řešení v celých číslech.

Důkaz. 1.

Dle 3.10:

$$AA^T = \lambda J + (r - \lambda)E$$

Spočítáme determinant dle vzorečku multilineární formy:

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

Dosadíme $k(k - 1) = \lambda(v - 1)$:

$$= (k - \lambda)^{v-1}(k + k^2 - k) = (k - \lambda)^{v-1}k^2$$

\forall prvočíslo $p|n = (k - \lambda)$ je v \det^2, k^2 sudá mocnina p . Takže v n^{v-1} taky sudá mocnina, jelikož v sudé $\Rightarrow v - 1$ je sudá mocnina. Neboli n je mocnina přirozeného čísla.

2.

Nejprve použijeme Lagrangeovu větu o 4 \square :

$$n = b_1^2 + b_2^2 + b_3^2 + b_4^2, b_i \in \mathbb{Z}$$

Vezmeme matici

$$B = \begin{pmatrix} b_1 & -b_2 & -b_3 & -b_4 \\ b_2 & b_1 & -b_4 & b_3 \\ b_3 & b_4 & b_1 & -b_2 \\ b_4 & -b_3 & b_2 & b_1 \end{pmatrix}$$

Využijeme kvaterniony a konkrétně normu

$$N(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2, N(ab) = N(a) \cdot N(b)$$

která je multilineární formou. Pak zobrazení $y = Bx$ je $\mathbb{Q}^4 \rightarrow \mathbb{Q}^4$ tak že po aplikaci normy platí:

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = (b_1^2 + b_2^2 + b_3^2 + b_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = n(x_1^2 + x_2^2 + x_3^2 + x_4^2)$$

Nahlédneme B je regulární. Jinak sporem je singulární, pak $Bx = 0$ má netriviální řešení, z toho

$$N(x) = n \cdot \sum x_i = 0 \Rightarrow \sum x_i = 0 \iff \forall i : x_i = 0$$

Což je spor.

Rozebereme 2 případy: 2a) $v \equiv 1 \pmod{4}$

Nechť máme proměnné $x_1, \dots, x_v \in \mathbb{Q}$. Aplikujeme zobrazení určené matici B po 4cích, pak

$$\sum y^2 = n(\sum x^2)$$

Rovnice z lemma 3.15 po transformaci je

$$\sum L_j^2 = \sum_{i=1}^{v-1} y_i + nx_v^2 + \lambda(\sum x_i)^2$$

Označme $w = \sum x_i$, taky nahlížeje na L_j jako na lineární formy v proměnných y_1, \dots, y_v . Dosadíme do L_j výrazy získané pomocí $x = \bar{B}y$. Taky ale $y_v = x_v$.

$$\sum L_j^2 = \sum_{i=1}^{v-1} y_i + ny_v^2 + \lambda w^2$$

Zvolme lineární formy tak, aby $L_j^2 = y_j^2$ (proces specializace):

$$L_1 = \sum c_j y_j = y_1 \Rightarrow \sum_{j=1}^{v-1} c_j y_j = (1 - c_1)y_1$$

Pak zvolme

$$y_1 = \begin{cases} \frac{\sum_{j=1}^{v-1} c_j y_j}{1-c_1} & \text{pro } c_1 \neq 1 \\ \frac{\sum_{j=1}^{v-1} c_j y_j}{-2} & \text{pro } c_1 = 1, L_1 = -y_1 \end{cases}$$

Pokračujeme induktivně, zbývá:

$$L_v^2 = ny_v^2 + \lambda w^2$$

Kde L_v, y_v, w jsou lineární formy v y_v . Proto

$$L_v = \frac{p}{q} y_v, w = \frac{r}{s} y_v \Rightarrow \frac{p^2}{q^2} y_v^2 = ny_v^2 + \lambda \frac{r^2}{s^2} y_v^2$$

Dosadíme $y_v = 1$:

$$p^2 s^2 = nq^2 s^2 + \lambda r^2 q^2$$

Položme $z = ps, x = qs \neq 0, y = rs$. Rovnice obecnějšího tvaru dostaneme protože $v \equiv 1 \pmod{4} \Rightarrow v-1$ je dělitelné 2.

2b) $v \equiv 3 \pmod{4}$. Uvažme rovnici z lemma 3.15, doplníme poslední 4ce proměnnou x_{v+1} :

$$\sum_{j=1}^{v+1} L_j^2 = \sum_{i=1}^{v+1} y_i - nx_{v+1}^2 + \lambda w^2$$

Znovu překloupíme na lineární formy v y_i a po specializaci:

$$0 = y_{v+1}^2 - nx_{v+1}^2 + \lambda w^2, x_{v+1}^2 = \frac{p}{q} y_{v+1}^2, w = \frac{r}{s} y_{v+1}^2$$

Dostaneme

$$y_{v+1}^2 = n - \frac{p^2}{q^2} - \lambda \frac{r^2}{s^2} y_{v+1}^2$$

Dosadíme $y_{v+1} = 1$:

$$(qs)^2 = n(ps)^2 - \lambda(rq)^2$$

Znovu dostáváme rovnici

$$z^2 = nx^2 - \lambda y^2$$

□

Důsledek 3.17 (\nexists KPR(6)).

Důkaz. Kdyby existovala KPR(6), tak by existoval i (43, 7, 1)-SBIBD. Pak ale dle 3.16 rovnice má netriviální řešení

$$z^2 = 6x^2 + (-1)^{21} y^2 \Rightarrow z^2 + y^2 = 6x^2$$

Pokud existovalo netriviální řešení, tak po zrušení společných dělitelů dostaneme řešení $(x, y, z) = 1$ nesoudělná. Vezmeme nemenší takové a upravíme $\pmod{3}$. Kvadratické residua jsou 0, 1. Na pravé straně zbytek je vždy 0, aby i na levé byl 0 tak y, z jsou zároveň dělitelné 3mi.

$$9z^2 + 9y^2 = 6x^2 \Rightarrow 3z^2 + 3y^2 = 2x^2 \Rightarrow 3|x$$

Spor s $(x, y, z) = 1$.

□

Věta 3.18 (Teorie čísel (BD)). $\forall n : n = a^2 + b^2 \iff$ prvočíslo $p = 4k + 3$ vystupuje v rozvoji s sudou mocninou.

Důkaz. " \Rightarrow " již bylo ukazáno na příkladě rovnice $z^2 + y^2 = nx^2$ pro $x = 1$. " \Leftarrow ".

Pozorování 1 Pokud $n = n_1 + n_2 \wedge n_1 = x_1^2 + y_1^2 \wedge n_2 = x_2^2 + y_2^2$ tak:

$$n = (x_1^2 + y_1^2)(x_2^2 + y_2^2) = x_1^2 x_2^2 + x_1^2 y_2^2 + y_1^2 x_2^2 + y_1^2 y_2^2 = (x_1 x_2 + y_1 y_2)^2 + (x_1 y_2 - y_1 x_2)^2$$

Pozorování 2 Z $n = \prod p_i^a$ vytkneme prvočísla $p \equiv 3 \pmod{4}$ do n_2 :

$$n = \prod p_i^a = n_1^2 \cdot (2) \cdot n_2$$

Pak $n_1^2 = n_1^2 + 0^2$ a $2 = 1^2 + 1^2$. Neboli úloha je redukována na $\forall p$ prvočíslo $p = 4k + 1 = a^2 + b^2$.

Pozorování 3 Pro $p = 4k + 1$ v tělese \mathbb{Z}_p je $(-1) \equiv l^2, l \in \mathbb{Z}_p$. Dal aplikujeme Diofantickou aproximaci

$$\forall e \in R, \forall n \exists \frac{h}{k} \in \mathbb{Q}, 0 < k \leq n : |e - \frac{h}{k}| \leq \frac{1}{k(n+1)}$$

pro $e = \frac{l}{p}, n = \lceil \sqrt{p} \rceil$. Pak

$$n+1 > \sqrt{p} \Rightarrow \frac{1}{n+1} < \frac{1}{\sqrt{p}}$$

Dle aproximaci

$$\exists \frac{h}{k}, k \leq \sqrt{p} : \left| \frac{l}{p} - \frac{h}{k} \right| \leq \frac{1}{k(n+1)} < \frac{1}{k\sqrt{p}}$$

Zvolme $c = lk - ph$. Pak

$$|lk - ph| < \sqrt{p} \Rightarrow c^2 < p \& c \equiv lk \pmod{p}$$

Dal

$$0 < k^2 + c^2 \equiv k^2 + l^2 k^2 = k^2(1 + l^2) \equiv 0 \pmod{p} \Rightarrow k^2 + c^2 < 2p \Rightarrow k^2 + c^2 = p$$

□

Věta 3.19 (\exists KPR □). $\exists KRP(n) \wedge n \equiv 1 \vee 2 \pmod{4} \Rightarrow \exists a, b \in \mathbb{Z} : n = a^2 + b^2$.

Důkaz. Z Příklad 3.14 KPR(m) existuje právě tehdy když existuje $(m^2 + m + 1, m + 1, 1)$ -SBIBD. Z 3.16 rovnice má netriviální řešení:

$$z^2 = nx^2 + (-1)^{\frac{v-1}{2}} \lambda y^2$$

Z druhého předpokladu dostaneme

$$z^2 + y^2 = nx^2$$

Podíváme se na prvočísla $p \equiv 3 \pmod{4} : p|n \iff n = p^c \cdot n_1, (p, l) = 1$. Z teorie čísel $p \equiv 3 \pmod{4} \Rightarrow -1$ je kvadratický nezbytek \pmod{p} . Jelikož kvadratické □-zbytek $\cdot (-1) = \square$ -nezbytek, tak

$$p|z, p|y \Rightarrow z = pz_1, y = py_1 \Rightarrow p^2 z_1^2 + p^2 y_1^2 = n_1 x^2$$

Po upravě

$$z_1^2 + y_1^2 = \frac{n}{p^2} x^2$$

Postupným dělením prvočíslem p dostaneme

$$p^{\lceil \frac{c}{2} \rceil} |z, p^{\lceil \frac{c}{2} \rceil} |y \Rightarrow p^{\lceil \frac{c}{2} \rceil} |n \Rightarrow c = 0 \pmod{2}$$

použijeme 3.18 $\Rightarrow n = a^2 + b^2$.

□

3.2 Steinerovy systémy trojic

Definice 3.20 (Steinerův systém trojic). Steinerův systém trojic je $(v, k = 3, \lambda = 1)$ -BIBD, značíme $\text{STS}(v)$.

Věta 3.21 (Existence STS a počet prvků). *Existuje-li $\text{STS}(v)$, pak $v \equiv 1$ nebo $v \equiv 3$ modulo 6.*

Důkaz. Z věty o parametrech BIBDu 3.3:

$$r = \frac{\lambda(v-1)}{k-1} = \frac{v-1}{2} \in \mathbb{Z} \Rightarrow v \equiv 1 \pmod{2}$$

Taky

$$|\mathcal{B}| = \frac{\lambda v(v-1)}{k(k-1)} = \frac{v(v-1)}{6} \in \mathbb{Z} \Rightarrow v \not\equiv 5 \pmod{6} \Rightarrow v \equiv 3 \pmod{6}$$

□

Definice 3.22 (Komutativní idempotentní kvazigrupa (KIK)). Je téměř grupa ale operace nemusí být asociativní, nemusí existovat e . Splňuje:

- komutativní: $xy = yx$
- idempotentní: $xx = x$
- kvazigrupa: $xy = xz \Rightarrow y = z$

Věta 3.23 (STS a speciální kvazigrupa). *$\text{STS}(v)$ existuje, právě když existuje komutativní idempotentní kvazigrupa na v prvcích splňující Definice 3.22 a $x(xy) = y$.*

Důkaz. " \Rightarrow ". Necht (V, \mathcal{F}) je STS. Definujme binární operaci:

$$xy = \begin{cases} x & \text{pro } x = y, \text{idempotence} \\ z & \text{pro } x \neq y \text{ a } \{x, y, z\} \in \mathcal{F} \end{cases}$$

Vezmeme jednoznačný prvek ve stejné 3ci jako x, y .

Zkontrolujeme vlastnosti operace:

- komutativní: vždy bereme prvek z 3ci, je jedno jestli se ptáme na xy nebo yx .
- idempotentní: z definice
- podmínka $x(xy) = y$:
 $x = y \Rightarrow x(xx) = xx = x$.
 $x \neq y \Rightarrow x(xy) = xz = y$.
- kvazigrupa: Necht $xy = xz$
 $x = y \Rightarrow x = z \Rightarrow x = y \Rightarrow y = z$
 $x \neq y$, necht sporem $y \neq z$ pak bychom měli 2 3ce které sdílí 2 prvky. Spor s STS.

" \Leftarrow ". Máme kvazigrupa (V, \cdot) , definujme 3ce:

$$\mathcal{F} = \{\{x, y, x \cdot y\} | x \neq y \in V\}$$

Ověříme axiomy:

1. $\mathcal{F} \subset \binom{V}{3}$. Necht sporem $x \cdot y = y \Rightarrow yx = y$. Pak ale $y(yx) = yy \stackrel{\text{idempotence}}{=} y = x$ spor.

2. Vezmeme libovolnou 3ci dle definice \mathcal{F} . Necht sporem máme další prvek $xy = z$ který tvoří další 3ci:

$$\{x, z, xz\} = \{x, z, x(xy) = y\}$$

□

Věta 3.24 (Kombinace STS). $\forall v_1, v_2 : \exists STS(v_1), STS(v_2) \Rightarrow \exists STS(v_1 \cdot v_2)$.

Důkaz. Necht máme (V_1, \circ_1) a (V_2, \circ_2) splňující Definice 3.22 a $x(xy) = y$. Pak kartezský součin s operaci definovanou po složkách je algebra stejného typu

$$(V_1, \circ_1) \times (V_2, \circ_2) = (V_1 \times V_2, \circ), (a, b) \circ (x, y) = (a \circ_1 x, b \circ_2 y)$$

□

Důsledek 3.25 (STS(9)). $\exists STS(9) = STS(3) \times STS(3)$.

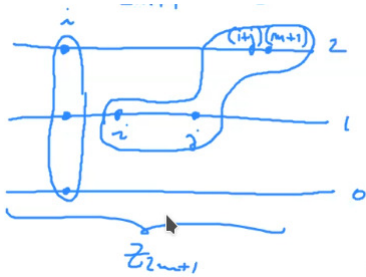
Sice STS(3) na 3-prvkové množině by nesplňoval $v \neq k$ ale z historických důvodů ho považujeme za validní. Stejně tak STS(1) (jeden prvek).

Cvičení 3.26 ($\exists STS(15)$?).

Věta 3.27 (Nutná podmínka je i postačující pro STS). $\forall v \equiv 1, v \equiv 3 \pmod{6}, \exists STS(v)$.

Důkaz pro 3, Boseho konstrukce. $V = \mathbb{Z}_{2m+1} \times \mathbb{Z}_3$, pak 3ce budou

$$\mathcal{F} = \{ \{(i, 0), (i, 1), (i, 2)\} | i \in \mathbb{Z}_{2m+1} \} \cup \{ \{(i, k), (j, k), ((m+1)(i+j), k+1)\} | i \neq j \in \mathbb{Z}_{2m+1}, k \in \mathbb{Z}_3 \}$$



1. # prvků $|V| = (2m+1)3 = 6m+3 \equiv 3 \pmod{6}$.

2. # 3c

$$\begin{aligned} |\mathcal{F}| &= 2m+1 + 3 \binom{2m+1}{3} = 2m+1 + 3 \cdot \frac{(2m+1)2m}{2} = 6m^2 + 5m + 1 = \\ &= (3m+1)(2m+1) = \frac{1}{6}(6m+3)(6m+2) = \frac{1}{6}|V|(|V|-1) \end{aligned}$$

Zbývá zkontrolovat, že pro libovolnou 3ci prvků máme množinu. Zkontrolujeme 3ce rozbořením případu

- (a) prvky jsou v různých řádcích ale nad sebou. Pak existuje množina z první podmínky.
(b) prvky jsou ve stejném řádku. Pak existuje množina z druhé podmínky.
(c) prvky jsou v různých řádcích ale ne nad sebou, na pozicích $(j, k), (h, k+1)$. Pak hledáme $i : h = (m+1)(i+j) \iff 2h = (2m+2)(i+j) = i+j \iff i = 2h-j$. Z vlastnosti kvazigrupy takové i je jednoznačné. Musíme zkontrolovat $i \neq j$.
Necht sporem $i = j \Rightarrow 2j = 2h \Rightarrow j = h$. Spor s volbou prvku z různých řádků.



□

Důkaz pro 1, Skolemova konstrukce. $v = 6m + 1$. Nechť

$$V = \mathbb{Z}_{2m} \times \mathbb{Z}_3 \cup \{w\}$$

Představujeme $\mathbb{Z}_{2m} = \{1, \dots, 2m = 0\}$.

$$\begin{aligned} \mathcal{F} = & \{ \{ (i, 0), (i, 1), (i, 2) \} \mid i \in [m] \} \cup \\ & \{ \{ (i, k), (i + m, k - 1), w \} \mid i \in [m], k \in [3] \} \cup \\ & \{ \{ (i, k), (j, k), (L_{i,j}, k + 1) \} \mid i \neq j \in \mathbb{Z}_{2m}, k \in [3] \} \end{aligned}$$



Kde $L \in Z_{2m}^{2m \times 2m}$ je *symetrický* Latinský čtverec takový, že na diagonále má dvakrát posloupnost $1, \dots, m$:

$$L_{i,i} = L_{m+i,m+i} = i, i \in [m]$$

Potřebujeme symetrický LČ protože 3 podmínka množiny musí být stejná nezávislé na tom, jestli se ptáme na i, j nebo j, i .

1. # prvků $|V| = 6m + 1 \equiv 1 \pmod{6}$.
2. # 3c, sčítance odpovídají typům množin v definici

$$\begin{aligned} |\mathcal{F}| &= m + 3m + 3 \binom{2m}{2} = 4m + 3 \cdot \frac{(2m-1)2m}{2} = 6m^2 + m = \\ &= \frac{1}{6}(6m+1)6m = \frac{1}{6}|V|(|V|-1) \end{aligned}$$

Zbývá zkontrolovat, že pro libovolnou 3ci prvků máme množinu. Zkontrolujeme 3ce rozbo-rem případu

- (a) jeden z prvků je w a druhý prvek je v první půlce $\in [m]$. Pak třetí prvek v druhé půlce o řád dole.
- (b) jeden z prvků je w a druhý prvek je v druhé půlce $\in \{m, \dots, 2m\}$. Pak třetí prvek v druhé půlce o řád nahoře v první půlce.
- (c) prvky jsou ve stejném řádku. Pak existuje množina z třetí podmínky.
- (d) prvky jsou v různých řádcích ale nad sebou v první polovině. Pak existuje množina z první podmínky.



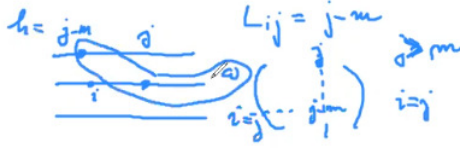
- (e) prvky jsou v různých řádcích ale nad sebou v druhé polovině. Chceme $\exists i : L_{i,j} = j \& i \neq j$. Z vlastnosti LČ i je jednoznačné a nemůže se rovnat j protože v druhé polovině na j -té pozici je prvek $j - m \neq j$.

- (f) prvky jsou v různých řádcích ale ne nad sebou, na pozicích $(j, k), (h, k+1)$. Chceme $\exists i : h = L_{i,j}$. Z vlastnosti LČ i je jednoznačné, chceme znovu $i \neq j$. Necht' sporem $i = j$, pak jsme na diagonále.

Pokud $j > m \Rightarrow h = j - m \neq j$. Opačně, $j \leq m \Rightarrow i = j = m$, což je již vyřešený případ v d).



- (g) prvky na pozicích $(h = j - m, k+1)$ a (j, k) . Pak ale $j = i$ a případ pokrývá 3ce s w .



□

Obecný „tabulkový“ důkaz.

Lemma 3.28 (Tabulkový důkaz 1). $\exists STS(v_1) = S_1, STS(v_2) = S_2, STS(v_3) = S_3 : S_3 \subseteq S_2 \Rightarrow \exists S = STS(v_3 + v_1(v_2 - v_1))$ Navíc obsahuje původní jako podsystemy: $\simeq S_i \subseteq S, i \in [3]$.

Důkaz. Označme $t = v_2 - v_3$. TODO

□

Lemma 3.29 (Tabulkový důkaz 2). $\exists STS(v) \subseteq KPR(2)$ (Fanová rovina) $\Rightarrow \exists STS(f(v))$ který taky obsahuje Fanovu rovinu, kde f je specifikovaná dle pravidel:

- a) $v_1 = v, v_2 = 3, v_3 = 1 \Rightarrow 1 + v(3 - 1) = 2v + 1$
- b) $v_1 = 3, v_2 = v, v_3 = 1 \Rightarrow 1 + 3(v - 1) = 3v - 2$
- c) $v_1 = 3, v_2 = v, v_3 = 3 \Rightarrow 3 + 3(v - 3) = 3v - 6$
- d) $v_1 = v, v_2 = 9, v_3 = 3 \Rightarrow 3 + v(9 - 3) = 6v + 3$
- e) $v_1 = 3, v_2 = v, v_3 = 7 \Rightarrow 7 + 3(v - 7) = 3v - 14$
- f) $v_1 = v, v_2 = 7, v_3 = 1 \Rightarrow 1 + v(7 - 1) = 6v + 1$

Předpoklad o Fanové rovině potřebujeme pouze pro e).

Důkaz. Ověříme, že $\forall v \equiv 1 \vee 3 \pmod{6}$ pokud $v \leq 1944 \exists STS(v)$, pak pokud $v \geq 325 \exists STS(v) \supseteq KPR(2)$.

Indukci dokážeme $\forall v \equiv 1 \vee 3 \pmod{6}$ pokud $v \leq 1944 \exists STS(v) \supseteq KPR(2)$. Rozbor případů dle $v \pmod{36}$, napíšeme $v = 36t + z$. Taky $1944 = 36 \cdot 54 \Rightarrow t \geq 54 \Rightarrow 6t \geq 324$.

□

□

3.3 Hadamardovy matice

Definice 3.30 (Hadamardova matice (HM)). Hadamardova matice řádu m je $H \in \{-1, 1\}^{m \times m}$ taková, že $HH^T = mI_m$. m na diagonále znamená, že všechny souřadnice jsou nenulové. Nuly mimo diagonále - řádky jsou ortogonální.

Lemma 3.31 (Transpozice Hadamardovy matice). H je Hadamardova matice, právě když H^T je Hadamardova matice.

Důkaz. Kvůli symetrii pojmů, stačí jedna implikace směrem. Podělíme matici \sqrt{m} :

$$\left(\frac{1}{\sqrt{m}}H\right)\left(\frac{1}{\sqrt{m}}H^T\right) = E$$

Neboli

$$\left(\frac{1}{\sqrt{m}}H\right) = \left(\frac{1}{\sqrt{m}}H\right)^{-1} = \sqrt{m}H^{-1}$$

Tedy

$$H^TH = mH^{-1}H = mE$$

□

Definice 3.32 (Normální forma HM). Hadamardova matice je v *normální formě*, pokud všechny prvky v prvním řádku a prvním sloupci jsou $+1$.

Pozorování 3.33 (Uzavřenost HM). Přehození řádků či sloupců, stejně tak jako vynásobení řádku či sloupce -1 , zachovává vlastnost "býti Hadamardovou maticí". Každou HM lze tedy vynásobením vhodných řádků a sloupců číslem -1 převést na HM stejného řádu, která je v normálním tvaru.

Věta 3.34 (Hadamardova matice a řád dělitelný čtyřmi). Je-li $m > 2$ řád HM, pak $m \equiv 0 \pmod{4}$.

Důkaz. Triviální případy: $m = 1$ matice je skalár. Pro $m = 2$ máme jedinou možnost

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Nechť H je HM v normální formě, $m > 2$. Řádkovými a sloupcovými úpravy převedeme matici na následující tvar

$$H = \begin{pmatrix} \begin{smallmatrix} ||| \\ ||| \\ ||| \end{smallmatrix} & \begin{smallmatrix} ||| \\ ||| \\ --- \end{smallmatrix} & \begin{smallmatrix} ||| \\ --- \\ ||| \end{smallmatrix} & \begin{smallmatrix} ||| \\ --- \\ --- \end{smallmatrix} \\ \vdots & \vdots & \ddots & \vdots \end{pmatrix}$$

Uvažme prvky v prvních třech řádcích. V prvním řádku jsou všechny prvky $+1$. Budiž a počet sloupců, ve kterých má jak druhý, tak třetí řádek $+1$, b počet sloupců, ve kterých má druhý řádek $+1$ a třetí řádek -1 , c počet sloupců, ve kterých má druhý řádek -1 a třetí řádek $+1$, a konečně d počet sloupců, ve kterých má jak druhý, tak třetí řádek -1 . Z ortogonality řádků vyplývá, že

$$\begin{aligned} a + b + c + d &= m \\ a + b - c - d &= 0 \\ a - b + c - d &= 0 \\ a - b - c + d &= 0 \end{aligned}$$

Sečtením 2 a 3 rovnice dostaneme $a = d$. Sečtením 1 a 4 rovnice $a = d = \frac{m}{4}$. Pak 1 a 2 dostaneme $b = \frac{m}{4}$. Neboli soustava má jediné řešení $a = b = c = d = \frac{m}{4} \Rightarrow m \equiv 0 \pmod{4}$. □

Věta 3.35 (Hadamardova matice a symetrické BIBDy). *HM řádu $m = 4t$ existuje \iff existuje symetrický $(4t - 1, 2t - 1, t - 1)$ -BIBD.*

Důkaz. Necht H je HM v normální formě. Vyškrtneme první řádek a sloupec, čímž dostaneme matici velikosti $(4t - 1)$. Tak nahradíme $-1 \rightarrow 0$. Necht matice po úpravách je A . Z vlastnosti HM, matice A má v každém sloupci $(2t - 1)$ jedniček. Ekvivalentně:

$$JA = (2t - 1)J$$

Neboli A jako matice incidence množinového systému implikuje, že každá množina má $(2t - 1)$ prvků. Zkontrolujeme ještě, že 2 prvky leží ve stejném počtu bloků \rightarrow skalární součin 2 řádků. Pro 2 libovolné řádky (kromě prvního) platí, že mají na čtvrtině míst $(t - 1)$ 1 proti -1 , viz důkaz 3.34.

Transformace matice lze provést i opačným směrem, což dává ekvivalenci. \square

Definice 3.36 (Tensorový součin). Jsou-li $A \in T^{m \times m}, B \in T^{n \times n}$, indexujeme prvky A jako a_{ij} , pak jejich tenzorový součin je matice (bloková):

$$A \times B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1m}B \\ a_{21}B & a_{22}B & \dots & a_{2m}B \\ \vdots & \vdots & \ddots & \vdots \end{pmatrix}$$

Věta 3.37 (Kombinace Hadamardových matic). *Existují-li HM řádů m_1, m_2 , pak existuje HM řádu $m_1 \cdot m_2$.*

Důkaz. Necht výsledná matice je H . Dostaneme ji pomocí tenzorového součinu Definice 3.36 daných matic. Z konstrukce, každý blok nové matice dostaneme násobením HM H_2 prvkem $a_{ij} \in \{-1, 1\}$. Dle 3.33 $H \in \{0, 1\}^{m_1 \cdot m_2 \times m_1 \cdot m_2}$.

Vezmeme 2 libovolné řádky H ze stejného bloku, jejich skalární součin je

$$\sum_{j=1}^{n_1} a_{ij}^2 \langle H_2, H_2 \rangle = \sum_{j=1}^{n_1} a_{ij}^2 \cdot 0$$

Pro 2 řádky z různých bloků (pro $u \neq w$ dopadne stejné jako předchozí):

$$u = w : \sum_{j=1}^{n_1} a_{ij} \cdot a_{kj} \langle H_2, H_2 \rangle = \sum_{j=1}^{n_1} a_{ij}^2 \cdot m_2$$

Vytkneme m_2 ze sumy a dostaneme skalární součin i -ho a j -ho řádku matice H_1 , což je taky nula. \square

Důsledek 3.38 (Sylvester). *HM řádu 2^k existují pro $\forall k \in \mathbb{N}$.*

Conjecture 3.39 (Hadamard). *HM řádu m existuje pro každé $m = 4t$.*

Důsledek 3.40 (Exponenciální Hadamardovy matice). *Pro každé k existuje HM řádu 2^k .*

Věta 3.41 (Payleyho konstrukce). *a) Je-li $q = p^r$ mocnina prvočísla p a $q \equiv 3 \pmod{4}$, pak existuje HM řádu $q + 1$.*

*b) Je-li $q = p^r$ mocnina prvočísla p a $q \equiv 1 \pmod{4}$, pak existuje HM řádu $2q + 2$.
Případ pro $q = 2$ je pokrytý kvůli 3.38.*

Důkaz. Vezměme konečné těleso $GF(q)$. Definujme *kvadratický charakter* $\chi : GF(q) \rightarrow \{-1, 0, 1\}$:

$$\chi(x) = \begin{cases} 0 & \text{pro } x = 0 \\ 1 & \text{pro } \exists y \in GF(q) : x = y^2 \\ -1 & \text{pro } \textit{jinak} \end{cases}$$

Znovu \square -zbytky a nezbytky. Jelikož multiplikativní grupa je cyklická s generátorem g , pak \square -zbytek je g^{2k} a nezbytky naopak liché mocniny. Proto

$$\chi(xy) = \chi(x) \cdot \chi(y)$$

Taky máme polovinu \square -zbytků a polovinu nezbytků, tak

$$\sum_{b \in GF(q)} \chi(b) = 0 \quad (4)$$

Z čehož odvodíme:

Lemma 3.42 (Posunutí χ).

$$\forall c \neq 0 : S = \sum_{b \in GF(q)} \chi(b) \chi(b+c) = -1$$

Důkaz. Vyjádříme $(b+c)$ jako $b \cdot y$.

$$y = \frac{b+c}{b}$$

pro $b=0$ charakter je nula, takové sčítanci neovlivňují součet, proto

$$S = \sum_{b \neq 0 \in GF(q)} \chi(b) \chi(b+c)$$

Taky nahlédneme, že y je jednoznačné a zobrazení $b \rightarrow y$ je prosté a na \Rightarrow bijekce. Navíc $b = \frac{c}{y-1}$ platí vždy protože pro $y=1$ bychom dostali $c=0$.

$$S = \sum_{b \neq 0} \chi(b) \chi(by) = \sum_{y \neq 1} \chi(b)^2 \chi(y) \stackrel{\chi^2(b)=1}{=} \sum_{y \neq 1} \chi(y) = \sum \chi(y) - \chi(1) = -1$$

□

Definice 3.43 (Charakterová matice Q). Označme $GF(q) = \{a_1, \dots, a_q\}$, definujme matici $Q \in \{-1, 0, 1\}^{q \times q}$ předpisem

$$Q_{ij} = \chi(a_i - a_j)$$

Nechť $\bar{1}$ je vektor délky q , $\forall i : \bar{1}_i = +1$

a) pokud $q \equiv 3 \pmod{4}$, pak

$$H_{q+1} = \begin{pmatrix} 0 & \bar{1} \\ -\bar{1}^T & Q \end{pmatrix} + I_{q+1}$$

je HM řadu $(q+1)$. Dostaneme matici

$$H = \begin{pmatrix} | & | & | & | & | & \dots \\ - & | & q & q & q & \dots \\ - & q & | & q & q & \dots \\ - & q & q & | & q & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \end{pmatrix}$$

Z definici Q a vlastnosti konečného tělesa Q má mimo diagonálu $-1 \vee 1$. Neboli $H \in \{0, 1\}^{q+1 \times q+1}$. Skalární součin řádku se sebou, $i > 0$:

$$S = -1 + 1 + \sum_{j=1}^q \chi(a_i - a_j)$$

Jelikož $j \in [q]$, tak suma probíhá všemi prvky $GF(q)$, dle (4) je 0. Takže $S = 0$. Skalární součin dvou libovolných řádků, $i, k > 0$:

$$S = 1 + \chi(a_k - a_i) + \chi(a_i - a_k) + \sum_{j=1}^q \chi(a_i - a_j) \chi(a_k - a_j)$$

Pak

$$\chi(a_k - a_i) + \chi(a_i - a_k) = \chi(a_k - a_i) + \chi(-1(a_k - a_i)) = \chi(a_k - a_i) + \chi(-1)\chi(a_k - a_i) \stackrel{\chi(-1)=-1}{=} 0$$

Kde $q \equiv 3 \pmod{4} \Rightarrow \chi(-1) = -1$. Použijeme lemma 3.42 na

$$\sum_{j=1}^q \chi(a_i - a_j) \chi(a_k - a_j)$$

tak, že $b = a_i - a_j$ a $c = a_k - a_i \neq 0$. Neboli součet je -1 . Dokázali jsme taky

$$QJ = 0 = JQ$$

A

$$QQ^T = \begin{pmatrix} q-1 & -1 \\ -1 & \ddots \end{pmatrix} = qI_q - J$$

b) Pokud $q \equiv 1 \pmod{4}$, sestavíme HM řádu $2q+2$ takto:

$$H_{2q+2} = \begin{pmatrix} 0 & \bar{1} & 0 & \bar{1} \\ \bar{1}^T & Q & \bar{1}^T & Q \\ 0 & \bar{1} & 0 & -\bar{1} \\ \bar{1}^T & Q & -\bar{1}^T & -Q \end{pmatrix} + \begin{pmatrix} I_{q+1} & -I_{q+1} \\ -I_{q+1} & -I_{q+1} \end{pmatrix}$$

Technickým rozбором případů ověříme, že H_{2q+2} je HM. □

Lemma 3.44 (O tenzorovém součinu (BD)). Pro A, A_1, A_2 čtvercové matice řádu m , B, B_1, B_2 čtvercové matice řádu n :

- $(A \times B)^T = A^T \times B^T$
- $\forall \alpha \in T : \alpha(A \times B) = (\alpha A) \times B = A \times (\alpha B)$
- $(A_1 + A_2) \times B = A_1 \times B + A_2 \times B$
- $A \times (B_1 + B_2) = A \times B_1 + A \times B_2$
- $(A_1 \times B_1)(A_2 \times B_2) = (A_1 A_2) \times (B_1 B_2)$

Pozorování 3.45 (Tenzorový produkt I).

$$\forall m, n : I_m \times I_n = I_{mn}$$

Věta 3.46 (Kombinace HM alternativní). Existují-li HM řádů m_1, m_2 , pak existuje HM řádu $m_1 \cdot m_2$.

Alternativní důkaz věty o kombinaci Hadamardových matic. Nechť A je HM řádu m_1 , B řádu m_2 . Pak z lemma 3.44

$$(A \times B)(A \times)^T = (A \times B)(A^T \times B^T) = (AA^T) \times (BB^T) = (mI_m) \times (nI_n) = mnI_{mn}$$

□

Poznámka 3.47 (Tensorový součin symetrických matic). Pokud jsou matice A , B symetrické, je i jejich tenzorový součin symetrická matice. Takže pokud existují symetrické HM řádů m_1 a m_2 , pak existuje symetrická HM řádu $m_1 m_2$.

Věta 3.48 (Payleyho konstrukce revisited).

Důkaz. a) Nechť Q je matice definovaná jako Definice 3.43, pak označme

$$S = S_{q+1} = \begin{pmatrix} 0 & \bar{1} \\ -\bar{1}^T & Q \end{pmatrix} \quad (5)$$

Pak platí:

$$\begin{aligned} QJ &= 0 = JQ \\ QQ^T &= qI_q - J \\ SS^T &= qI_{q+1} \end{aligned}$$

Z $q \equiv 3 \pmod{4} \Rightarrow \chi(-1) = -1$, matice S je *antisymetrická*: $S^T = -S$ proto pro $H_{q+1} = S + I_{q+1}$ platí:

$$H_{q+1}H_{q+1}^T = (S + I_{q+1})(S^T + I_{q+1}) = SS^T + S^T + S + I_{q+1} = qI_{q+1} - S + S + I_{q+1} = (q+1)I_{q+1}$$

Neboli dle definice H_{q+1} je HM.

b) je speciální případ tzv Williamsonové konstrukce kterou ukážeme níže. □

Lemma 3.49 (Williamson). *Bud' $S \in \mathbb{R}^{n \times n}$ t.ž.*

$$SS^T = (n-1)I_n \text{ a } S^T = \varepsilon S, \varepsilon \in \{-1, 1\}$$

Mějme $A, B \in \mathbb{R}^{m \times m}$ takové, že

$$AA^T = BB^T = mI_m, AB^T = -\varepsilon BA^T$$

Pak pro matici

$$K = A \times E_n + B \times S$$

platí $KK^T = mnI_{mn}$.

Důkaz.

$$\begin{aligned} KK^T &= (A \times I_n + B \times S)(A^T \times I_n + B^T \times S^T) = \\ &= AA^T \times I_n + AB^T \times S^T + BA^T \times S + BB^T \times SS^T = \\ &= mI_m \times I_n + (-\varepsilon BA^T) \times (\varepsilon S) + BA^T \times S + mI_m \times (n-1)I_n \\ &= mI_m \times (-\varepsilon^2 + 1)(BA^T \times S) + m(n-1)I_{mn} = mnI_{mn} \end{aligned}$$

□

Věta 3.50 (Williamsonova konstrukce). *Bud' $q = p^r$ mocnina prvočísla p a $q \equiv 1 \pmod{4}$ a existuje HM řádu $h > 1$. Potom existuje HM řádu $h(q+1)$.*

Důkaz. Pro matici S definovanou v (5) platí:

$$S^T = S \& S S^T = q I_{q+1}$$

protože $q \equiv 1 \pmod{4}$ je $-1 \square$ -nezbytek. Neboť S splňuje předpoklady lemma 3.49 pro $\varepsilon = 1$. Nechť A je HM řádu h . Sestrojíme pomocnou U :

$$U = I_{\frac{h}{2}} \times \begin{pmatrix} 0 & 1 \\ 01 & 1 \end{pmatrix}$$

Což je komplikovaný zápis pro matici, která má 0 na hlavní diagonále. Na dvou vedlejších diagonálách se střídá 1, -1 . Položme

$$B = UA$$

Pak

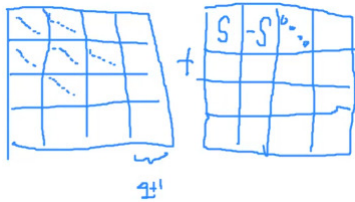
$$\begin{aligned} BB^T &= UAA^TU^T = U(hI_h)U^T = hUU^T = hI_H (= AA^T), \\ AB^T &= AA^TU^T = (hI_h)U^T = -hU \\ BA^T &= UAA^T = U(hI_h) = hU \end{aligned}$$

Neboli S, A, B splňují předpoklady Williamsonova lemmatu lemma 3.49. Proto pro

$$K = A \times I_{q+1} + B \times S$$

platí $KK^T = h(q+1)I_{h(q+1)}$ což je definice HM řádu $h(q+1)$. Musíme ale ověřit, že prvky v K jsou $\in \{-1, 1\}$.

Matice $A \times I_{q+1}$ se skládá z bloků diagonálních matic s 1 nebo -1 na diagonále. Matice B umístí do bloků buď S nebo $-S$. Jelikož matice Q má nuly na diagonále a $-1, 1$ mimo diagonálu v součtu na každé pozici dostaneme $0 \pm 1 = \pm 1$.



□

HW: pro jakou matici A dostaneme Payleyho konstrukce z Williamsonové?

4 Latinské čtverce podruhe

Definice 4.1 (Trochu méně pravidelné blokové schéma). (V, \mathcal{B}) je $(v, k_1, \dots, k_m, \lambda)$ -BIBD, jestliže

- $|V| = v$
- $\forall B \in \mathcal{B} \exists i \in [k] : |B| = k$
- $\forall x \neq y \in V : |\{B \in \mathcal{B} : \{x, y\} \in B\}| = \lambda$

Dále jako \mathcal{B}_i značíme bloky velikosti k_i , $b_i = |\mathcal{B}_i|$, $b = |\mathcal{B}|$.

Poznámka 4.2 (O b a b_i méně pravidelných schémat). • $\sum_{i=1}^m b_i = b$

• $\lambda v(v-1) = \sum_{i=1}^m b_i k_i (k_i - 1)$

Důkaz. Spočítáme 2ma způsoby

$$\binom{v}{2} \cdot \lambda = |\{(\{x, y\}, B) : x \neq y \forall x, y \in B \in \mathcal{B}\}| = \sum_i^m b_i \binom{k_i}{2}$$

TODO

□

Definice 4.3 (Průhledná množina). Buď $(V, \mathcal{B}), \mathcal{A} \subseteq \mathcal{B}$. Pak \mathcal{A} je průhledná množina bloků, pokud obsahuje navzájem disjunktní bloky.

Definice 4.4 (BIBD se středníkem).

(V, \mathcal{B}) definujeme jako $(v, k_1, \dots, k_r; k_{r+1}, k_m, \lambda)$ -BIBD, je-li $(v, k_1, \dots, k_r, k_{r+1}, k_m, \lambda)$ -BIBD a $\mathcal{B}_1 \cup \dots \cup \mathcal{B}_r$ je průhledná množina.

Věta 4.5 (Dolní odhad na NOLČ).

Existuje-li $(v, k_1, \dots, k_r; k_{r+1}, k_m, \lambda)$ -BIBD, pak

$$NOLČ(v) \geq \min\{NOLČ(k_1), \dots, NOLČ(k_r), NOLČ(k_{r+1}) - 1, \dots, NOLČ(k_m) - 1\}$$

Důkaz. Z 2.10 $NOLČ(k_i) \geq d \iff \exists OA(k_i, d+2)$. Označme

$$c = \min\{NOLČ(k_1) + 2, \dots, NOLČ(k_r) + 2, NOLČ(k_{r+1}) + 1, \dots, NOLČ(k_m) + 1\}$$

Pro $i \leq r$ z 2.10:

$$NOLČ(k_i) + 2 \geq c \Rightarrow \exists OA(k_i, c)$$

Označme OA jako A_i nad symboly $1, 2, \dots, k_i$. Pro $i > r$ z 2.10:

$$NOLČ(k_i) + 1 \geq c \Rightarrow \exists OA(k_i, c+1)$$

Sestrojíme tabulku A_i následovně. Začneme s ortogonální tabulkou D_i hloubky $c+1$ nad symboly $\{1, 2, \dots, k_i\}$, jejíž sloupce popřeházíme tak, aby první řádek začínal k_i symboly 1 a každý další řádek začínal $1, 2, \dots, k_i$. Matici A_i získáme z D_i škrtnutím prvního řádku a prvních k_i sloupců. Takže A_i má c řádků a $k_i^2 - k_i$ sloupců a její řádky jsou na sebe skoro kolmé v tom smyslu, že každé dva řádky nad sebou vidí všechny dvojice různých prvků z $\{1, 2, \dots, k_i\}$.



Zafixujme nyní $(v, k_1, k_2, \dots, k_r; k_{r+1}, \dots, k_m, 1)$ -BIBD (V, \mathcal{B}) , který podle předpokladu existuje, a necht S_1, S_2, \dots, S_b jsou bloky. Pro každý blok S_j velikosti k_i vytvoříme matici B_j z matice A_i tak, že symboly $1, 2, \dots, k_i$ nahradíme jmény prvků z bloku S_j . Potom matice

$$(B_1, \dots, B_b, E)$$

kde E je matice obsahující sloupce $(x, \dots, x)^T$ pro všechna

$$x \in V \setminus \bigcup_{S_j \in \bigcup_i^T \mathcal{B}_i} S_j$$

Pak tato matice je matice $OA(v, c) \stackrel{2.10}{\Rightarrow} NOL\check{C}(v) \geq c - 2$.

Alternativně, můžeme upozornovat, že # sloupců této matice je

$$\sum_i^r b_i \cdot k_i^2 + \sum_{i=r+1}^m b_i(k_i^2 - k_i) + \text{sloupce z } E = \sum_{i=1} b_i(k_i^2 - k_i) + \sum_i^r b_i \cdot k_i + v - \sum_i^r b_i \cdot k_i = \\ = v + \sum b_i(k_i^2 - k_i) = v + v(v - 1) = v^2$$

□

Příklad 4.6. $KPR(4) = (21, 5, 1)\text{-BIBD} \stackrel{4.5}{\Rightarrow} NOL\check{C}(21) \geq NOL\check{C}(5) - 1 = 3$.

To je protipříklad na hypotézu McNeishe $NOL\check{C}(p_i^{r_i}) = \min_i \{p_i^{r_i} - 1\}$.

Věta 4.7 ((v, k, 1)-BIBD a NOLČ). *Existuje-li (v, k, 1)-BIBD, pak*

- 1) $NOL\check{C}(v - 1) \geq \min(NOL\check{C}(k - 1), NOL\check{C}(k) - 1)$
- 2) *Pro* $2 \leq x \leq k$, *pak* $NOL\check{C}(v - x) \geq \min\{NOL\check{C}(k - x), NOL\check{C}(k) - 1, NOL\check{C}(k - 1) - 1\}$

Důkaz. 1) Z blokového schématu (v, k, 1)-BIBDu zahodíme jeden prvek. Dostaneme tak (v - 1, k - 1; k, 1)-BIBD (protože r - 1 bloků o k - 1 prvcích je po dvou disjunktních).

$$(V, \mathcal{B}) \rightarrow (V \setminus \{a\}, \mathcal{B}')$$

- 2) Z blokového schématu (v, k, 1)-BIBD zahodíme x prvků, které patří do stejného bloku. Dostaneme tak (v - x, k - x; k - 1, k, 1)-BIBD (protože jediný blok o k - x prvcích triviálně tvoří průhlednou množinu).

□

Věta 4.8 ((v, k, 1)-BIBD a NOLČ(v - 3)). *Existuje-li (v, k, 1)-BIBD, pak* $NOL\check{C}(v - 3) \geq \min\{NOL\check{C}(k - 2), NOL\check{C}(k - 1) - 1, NOL\check{C}(k) - 1\}$.

Důkaz. Z blokového schématu (v, k, 1)-BIBD zahodíme tři prvky, které neleží ve stejném bloku. Dostaneme tak (v - 3, k - 2; k, k - 1, 1)-BIBD (protože bloky o k - 2 prvcích jsou po dvou disjunktní).



□

Příklad 4.9. $KPR(4) = (21, 5, 1)\text{-BIBD} \stackrel{4.8}{\Rightarrow}$:

$$NOL\check{C}(18) \geq \min\{NOL\check{C}(3) = 2, NOL\check{C}(5) - 1 = 3, NOL\check{C}(4) - 1 = 2\} = 2$$

Přitom $18 \equiv 2 \pmod{4}$, ale 18 není tvaru $12k + 10$.

Definice 4.10 (Řešitelný systém). Systém (V, \mathcal{B}) je řešitelný, pokud $\mathcal{B} = \mathcal{B}_1 \dot{\cup} \dots \dot{\cup} \mathcal{B}_r$ takový, že

1. $\forall i : \mathcal{B}_i$ je průhledná

$$2. \cup \mathcal{B}_i = B$$

Pak \mathcal{B}_i nazveme třídy řešitelnosti.

Příklad 4.11 (Řešitelný systém). Každá KAR řádu m je řešitelný $(m^2, m, 1)$ -BIBD s $(m+1)$ třídami řešitelnosti, neboť každá třída ekvivalence rovnoběžnosti tvoří jednu třídu řešitelnosti.



Věta 4.12 (Řešitelnost a odhady na NOLČ). Pokud existuje řešitelný $(v, k, 1)$ -BIBD a r třídami řešitelnosti, pak

1. $NOLČ(v+1) \geq \min\{NOLČ(k) - 1, NOLČ(k+1) - 1\}$
2. pro $2 \leq x \leq r-2$: $NOLČ(v+x) \geq \min\{NOLČ(x), NOLČ(k) - 1, NOLČ(k+1) - 1\}$
3. $NOLČ(v+r-1) \geq \min\{NOLČ(r-1), NOLČ(k), NOLČ(k+1) - 1\}$
4. $NOLČ(v+r) \geq \min\{NOLČ(r), NOLČ(k+1) - 1\}$

Důkaz. Pro prvních x tříd řešitelnosti přidáme jeden prvek y_i , přidáme blok obsahující všechna y_i (pokud jich je více než 1) a zároveň prvek y_i přidáme ke každému bloku „své“ třídy řešitelnosti. Tím získáme po řadě

- 1) $(v+1, k, k+1, 1)$ -BIBD
- 2a) $(v+x, x; k, k+1, 1)$ -BIBD pro $x \neq k$
- 3a) $(v+r-1, r-1, k; k+1, 1)$ -BIBD pro $r-1 \neq k, k+1$
- 4a) $(v+r, r; k+1, 1)$ -BIBD pro $r \neq k+1$

Pro speciální případy:

- 2b) $x = k$: máme $(r+k, k, k+1, 1)$ -BIBD, tedy $NOLČ(r+k) \geq \min\{NOLČ(k)-1, NOLČ(k+1)-1\} \geq \min\{NOLČ(x), NOLČ(k)-1, NOLČ(k+1)-1\}$
- 3b) $r-1 = k$: máme $(r+k, k; k+1, 1)$ -BIBD, tedy $NOLČ(r+k) \geq \min\{NOLČ(k), NOLČ(k+1)-1\}$
- 3c) $r-1 = k+1$: máme $(r+k+1, k+1, 1)$ -BIBD, tedy $NOLČ(r+k+1) \geq NOLČ(k+1) - 1 \geq \min\{NOLČ(k+1), NOLČ(k+1) - 1\}$
- 4b) $r = k+1$, tedy máme $(r+k+1, k+1, 1)$ -BIBD, tedy $NOLČ(r+k+1) \geq NOLČ(k+1) - 1 \geq \min\{NOLČ(k+1), NOLČ(k+1) - 1\}$

□

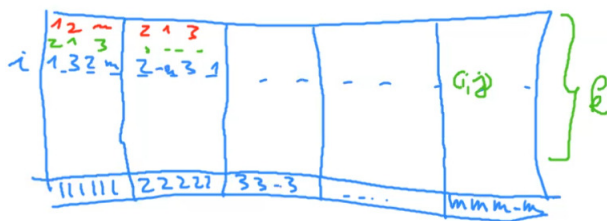
Příklad 4.13 (Řešitelný systém 2). KAR(7) je $(49, 7, 1)$ -BIBD, je řešitelný a má osm tříd řešitelnosti.

Tedy při volbě $x = 1$

$$NOLČ(50) \geq \min\{NOLČ(7) - 1, NOLČ(8) - 1\} = \min\{5, 6\} = 5$$

a při volbě $x = 5$:

$$NOLČ(54) \geq \min\{NOLČ(5), NOLČ(7) - 1, NOLČ(8) - 1\} = \min\{4, 5, 6\} = 4$$



Obrázek 1: GD NOLČ

Definice 4.14 (Skupinově rozložitelný systém). Množinový systém (V, \mathcal{B}) se nazývá skupinově rozložitelný (group divisible), pokud $\exists V_1, \dots, V_n : V_i \subseteq V, V_i \cap V_j = \emptyset$.

- a) $\forall x, y \in V_i : \exists \lambda_1$ bloků sdílejících x, y
- b) pro $i \neq j : \forall x \in V_i, \forall y \in V_j : \exists \lambda_2$ bloků sdílejících x, y .

Pokud všechny bloky mají velikost k , $|V_i| = m$, pak značíme systém jako $GD(v, k, m, \lambda_1, \lambda_2)$. Často se říká, že # skupin je $n \Rightarrow v = nm$.

Věta 4.15 (NOLČ a existence GD). Pokud pro m, k platí $NOLČ(m) \geq k - 1$, pak $\exists GD(km, k, m, 0, 1)$ s m třídami řešitelnosti.

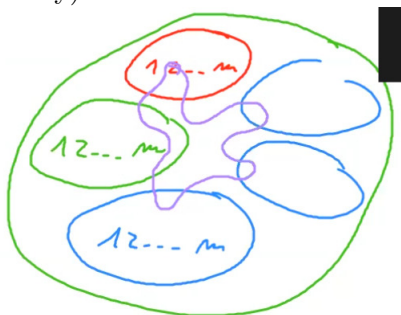
Důkaz. $NOLČ(m) \geq k - 1 \Rightarrow \exists OA(m, k + 1)$. BÚNO poslední řádek v tabulce má symbol i v i -tém bloku. Tento řádek zahodíme.

Prvek na pozici (i, j) nahradíme právě dvojicí souřadnic, takže stejná písmena v různých řádcích jsou odlišné. Postavíme množinový systém:

$$V = \{1, \dots, k\} \times \{1, \dots, n\}$$

kde $1 - k$ jsou původní symboly a $1 - n$ jsou "barvy".

Řádky OA tvoří třídy řešitelnosti velikosti m , bloky jsou sloupce OA (bereme jeden prvek každé barvy).



Z konstrukce máme parametry $GD(km, k, m, ?, ?)$, zbývá zkontrolovat λ_1, λ_2 . Necht x, y jsou libovolné 2 prvky ze stejné skupiny nějaké barvy. Jelikož do bloku vždy bereme jenom 1 prvek z barevné skupiny, nemůžou být ve stejném bloku $\Rightarrow GD(km, k, m, 0, ?)$.

Necht x, y jsou libovolné prvky z dvou skupin různých barev. Z vlastnosti OA symboly x, y jsou nad sebou právě v jediném sloupci $\Rightarrow GD(km, k, m, 0, 1)$.

Konečně zkontrolujeme řešitelnost. Každý obdélník na obrázku fig. 1 tvoří průhlednou množinu. Všechny takové pokrývají celý systém. \square

Věta 4.16 (Řešitelný GD a NOLČ). Existuje-li $GD(v, k, m, 0, 1)$ řešitelný, GD má r tříd řešitelnosti, pak

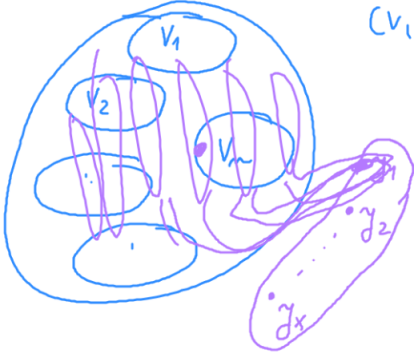
$$\forall x \in [r - 1] : NOLČ(v + x) \geq \min\{NOLČ(m), NOLČ(x), NOLČ(k) - 1, NOLČ(k + 1) - 1\}$$

Důkaz. Označme skupiny rozložitelnosti V_1, \dots, V_n , pak $v = mn$. Přidáme skupiny jako bloky

$$(V, \mathcal{B}) \rightarrow (V, \mathcal{B}'), \mathcal{B}' = \mathcal{B} \cup \{V_1, \dots, V_n\}$$

Pak (V, \mathcal{B}') je $(v, m; k, \lambda = 1)$ -BIBD. λ je uniformní, protože prvky z S_i teď patří do 1 společného bloku. Navíc bloky S_i velikosti m jsou po 2 disjunktní. Pozor, toto neplatí pro $m = k$, tedy průhlednou množinu tvoří právě bloky V_1, \dots, V_n .

Přidáme navíc prvky y_1, \dots, y_x , taky přidáme blok $\{y_1, \dots, y_x\}$. Do všech množin z i -te třídy řešitelnosti přidáme prvek y_i . Čímž vznikne množinový systém (V', \mathcal{B}'') . Kde $|V'| = v + x$ a je to $(v + x, m, k + 1, k, ?, ?)$.



Zkontrolujeme λ rozбором případu:

- 2 prvky z modrých množin pořád jsou v 1 společném bloku.
- prvek y_i a nějaký prvek z třídy řešitelnosti je právě v 1 bloku
- 2 prvky y_i, y_k jsou v 1 nově přidaném bloku.

Dohromady máme $(v + x, m, x; k + 1, k, \lambda = 1)$ -BIBD. Navíc bloky tvořící skupiny rozložitelnosti a nový blok y -ů tvoří průhlednou množinu. Dle 4.5:

$$NOLČ(v + x) \geq \min\{NOLČ(m), NOLČ(x), NOLČ(k) - 1, NOLČ(k + 1) - 1\}$$

Když $m = k$ tak $NOLČ(m)$ je v min zbytečný, protože $NOLČ(k) - 1$ je o 1 menší. Neboli v tomto případě nezáleží jestli bloky skupiny řešitelnosti tvoří průhlednou množinu.

Taky ale může být $m = k + 1, x = k, x = k + 1$. Všechny tyto případy jsou analogické $m = k$. \square

Důsledek 4.17 (O násobení NOLČ). Je-li $NOLČ(m) \geq k - 1$, pak

$$\forall x \in [r - 1] : NOLČ(km + x) \geq \min\{NOLČ(m), NOLČ(x), NOLČ(k) - 1, NOLČ(k + 1) - 1\}$$

Ale kvůli tomu, že třídy řešitelnosti jsou obdélníky na obrázku fig. 1 a jsou velikosti m můžeme vzít větší x :

$$\forall x \in [m - 1] : NOLČ(km + x) \geq \min\{NOLČ(m), NOLČ(x), NOLČ(k) - 1, NOLČ(k + 1) - 1\}$$

Lemma 4.18 (Dolní odhad pro NOLČ). Pokud $NOLČ(4t + 2) \geq 2$ pro každé $2 \leq t \leq 181$, pak $NOLČ(4t + 2) \geq 2$ pro každé $t \geq 2$.

Znění říká, že pokud existují aspoň 2 ortogonální LČ pro $10, 14, 18, \dots, 5 \cdot 181 + 2 = 726$.

Důkaz. Nechť $t \geq 730, v = 4t + 2$. Podělíme $v - 10$ číslem 144: $v - 10 = 144g + z, z \in [0, 144)$. Jelikož $v, 10 \equiv 2 \pmod{4}$ tak jejich součet je dělitelný 4. Taky $144 = 36 \Rightarrow z = 4u, u \in [0, 36)$.

Přepíšeme $v = 4 \cdot 36g + 4u + 10$. Dal

$$NOLČ(36g) = NOLČ(2^{\geq 2} \cdot 3^{\geq 2} \cdot 5 \cdot \dots) \geq \min(NOLČ(2^{\geq 2}), NOLČ(3^{\geq 2}), \dots) \stackrel{2,12}{\geq} \min(3, 8, \geq 3, \dots) = 3 \geq k - 1$$

Použijeme 4.17 s $m = 36g, k = 4, x = 4u + 10$.

$$\begin{aligned} \text{NOLČ}(m) &\geq k - 1 \stackrel{4.17}{\Rightarrow} \text{NOLČ}(mk + x) = \text{NOLČ}(v) \geq \\ &\geq \min(\text{NOLČ}(36g) \geq 3, \text{NOLČ}(4u + 10), \text{NOLČ}(4) - 1 = 2, \text{NOLČ}(5) - 1 = 3) \end{aligned}$$

Taky $10 \leq 4u + 10 \leq 4 \cdot 35 + 10 = 150 \leq 726$. Takže dle předpokladu $\text{NOLČ}(4u + 10) \geq 2$. Neboli

$$\min(\text{NOLČ}(36g) \geq 3, \text{NOLČ}(4u + 10) \geq 2, \text{NOLČ}(4) - 1 = 2, \text{NOLČ}(5) - 1 = 3) = 2$$

□

Věta 4.19 (NOLČ je aspoň 2). $\forall v > 6 : \text{NOLČ}(v) \geq 2$.

Důkaz. Pokud $v \not\equiv 2 \pmod{4}$ tak jsme dokázali v 2.13.

Jinak $v \equiv 2 \pmod{4}$ & $v \leq 726$ věříme jako fakt. Pro $v \geq 730$ existuje z lemma 4.18. □

5 Konečné projektivní prostory

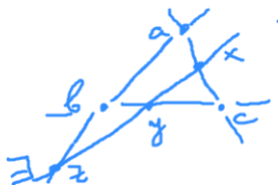
Definice 5.1 (Konečný projektivní prostor, kolinearita). (P, \mathcal{L}) takový, že P je konečná množina bodů a \mathcal{L} je množinový systém (přímek) na P , je konečný projektivní prostor, splňuje-li axiomy A1, A2, A3.

Dále body $x \neq y \neq z \neq x$ takové, že $x, y, z \in l \in \mathcal{L}$, nazveme kolineární.

(A1) $\forall x \neq y \in P \exists ! l \in \mathcal{L} : x, y \in l$ Takové přímce říkáme xy .

(A2) netrivialita: $\forall l \in \mathcal{L} : |l| \geq 3$

(A3) $\forall a, b, c : a \neq b \neq c \neq a$, & a, b, c nekolineární: $\forall x \in ac, y \in bc \exists z \in ab$ takový, že x, y, z jsou kolineární.



Pozorování 5.2.

$$\forall l_1 \neq l_2 \in \mathcal{L} : |l_1 \cap l_2| \leq 1$$

Protože jinak pro 2 body ležící v průniku je porušen A1.

Definice 5.3 (Podprostor). Je-li (P, \mathcal{L}) konečná geometrie, pak $U \subseteq P$ je podprostor, jestliže

$$\forall x \neq y \in U : xy \subseteq U$$

Zachovává přímky pro všechny body v podprostoru.

Poznámka 5.4 (Podprostor a KPP). Je-li $U \subseteq P$ podprostor, pak $(U, \mathcal{L}|_U)$ je konečný projektivní prostor.

Lemma 5.5 (Průnik podprostorů je podprostor). Pro $U, V \subseteq \mathcal{L}$ je podprostor, pak $U \cap V$ je podprostor.

Důkaz. Pro libovolné 2 různé body v průniku, dle definice podprostoru

$$x \neq y \in U \cap V \Rightarrow xy \subseteq U, xy \subseteq V \Rightarrow xy \subseteq U \cap V$$

□

Pozorování 5.6 (Triviální podprostory). $(\{x\}, \emptyset)$ je KPP protože splňuje všechna tvrzení o přímkách, jelikož žádné nemá.

Podobně (\emptyset, \emptyset) je KPP, z toho lze udělat disjunktní podprostory.

Definice 5.7 (Obal). Buď $A \subseteq P, (P, \mathcal{L})$: pak $\langle A \rangle$ je nejmenší podprostor, který obsahuje A .

$$\langle A \rangle = \bigcap_{\substack{U \text{ podpr. } P \\ A \subseteq U}} U$$

Protože platí:

$$\forall U \text{ podpr. } P, A \subseteq U : \langle A \rangle \subseteq U$$

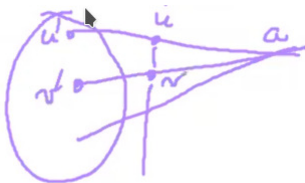
Lemma 5.8 (O přidání prvku do podprostoru). Buď $S \subseteq P$ podprostor (P, \mathcal{L}) , $a \notin S$. Potom $\langle S \cup \{a\} \rangle = \bigcup_{x \in S} ax$.

Důkaz. " $\langle S \cup \{a\} \rangle \supseteq \bigcup_{x \in S} ax$ ". Jelikož obal je podprostor, všechny přímky ax v něm musí být. Opačnou inkluzi ukážeme tak, že $AX = \bigcup_{x \in S} ax$ je podprostor. Obal je průnikem všech podprostoru, takže pokud průnik obsahuje AX tak nemůže mít nic navíc. Neboli $\langle S \cup \{a\} \rangle \subseteq \bigcup_{x \in S} ax$ ". Dle Definice 5.3 musíme ukázat:

$$\forall t \neq r : tr \subseteq AX$$

Rozbor případů:

1. $t = a \vee r = a$, tak druhý bod leží na nějaké přímce ax . Triviálně celá přímka $ax \subseteq AX$.
2. $t \in S \wedge r \in S$ je splněno dle Definice 5.3.
3. BUNO ($t \in S \iff t = x$) $\wedge r \notin S$. Pokud $r \in ax$ triviálně. Jinak $r \in ay, y \in S$. // TODO finish
4. $r, t \notin S; r, t \neq a; rt \not\subseteq a$ Chceme $w \in rt \Rightarrow w \in AX$.



Nechť $r' \in ar \wedge r' \in S$ analogicky t' . Dle A3:

$$\exists y : rt \cap r't' \in S$$

Další 3ce nekolineárních bodů je r, r', y . Proto $\exists w' \in r'y \subseteq S$. Pak i $w \in w'a \Rightarrow w \in AX$.

□

Lemma 5.9 (Sjednocení podprostorů). Buďte $S, T \subseteq P$ podprostory (P, \mathcal{L}) . Potom

$$\langle S \cup T \rangle = \bigcup_{\substack{s \in S, t \in T \\ s \neq t}} st$$

Důkaz. Označme $\bigcup_{s \in S, t \in T, s \neq t} st = SUT$. Triviálně platí: $SUT \subseteq \langle S \cup T \rangle$. Pro rovnost stačí ukázat že SUT je podprostor. Triviální případy:

1. $a \in S \wedge b \in S$ je splněno dle Definice 5.3. Analogicky pro T .
2. $a \in S \wedge b \in T$ dle konstrukce SUT .
3. $a \in S \wedge b \in rp, r \in S, p \in T$ jako v lemma 5.8.

Netriviální případ:

$$u \in s_1 t_1 : s_1 \in S, t_1 \in T \wedge v \in s_2 t_2 : s_2 \in S, t_2 \in T$$

Pokud by $s_1 = s_2 \vee t_1 = t_2$ tvrzení platí z lemma 5.8.

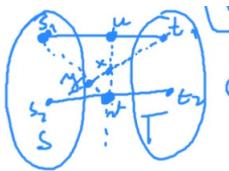
Chceme

$$\forall x \in uv \exists a, b : a \in S, b \in T : x \in ab$$

Kroky:

1. podíváme se na body s_1, u, v :

$$t_1 x \cap s_1 u = t_1 \wedge t_1 x \cap uv = x \xrightarrow{A^3} \exists y : t_1 x \cap s_1 v = y$$



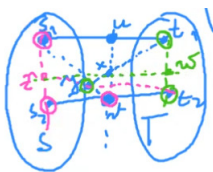
2. podíváme se na body s_1, s_2, v :

$$t_1 y \cap s_2 v = t_2 \wedge t_1 y \cap s_1 v = y \xrightarrow{A^3} \exists z \in S : t_2 y \cap s_1 s_2 = z$$



3. podíváme se na body t_1, t_2, y :

$$zx \cap y t_1 = x \wedge zx \cap t_2 y = z \xrightarrow{A^3} \exists q \in T : t_1 t_2 \cap zx = q$$



Dohromady $x \in zq$. □

Definice 5.10 (Projektivně nezávislá množina). Množina $A \subseteq P$ v (P, \mathcal{L}) je projektivně nezávislá, jestliže

$$\forall a \in A : \langle A \setminus \{a\} \rangle \neq \langle A \rangle$$

Lemma 5.11 (Přidání prvku do projektivně nezávislé množiny). Je-li A projektivně nezávislá a $b \notin \langle A \rangle$, pak $A \cup \{b\}$ je projektivně nezávislá.

Analogie z vektorových prostorů: pokud máme lineárně nezávislé vektory a přidáme vektor který nelze vyjádřit jako lineární kombinaci, tak dostaneme množinu lineárně nezávislých vektorů.

Důkaz. Necht sporem $A \cup \{b\}$ není projektivně nezávislá \Rightarrow

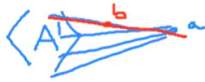
$$\exists a \in A \cup \{b\} : \langle A \cup \{b\} \setminus \{a\} \rangle = \langle A \cup \{b\} \rangle$$

Rozebereme 2 případy:

1. $a = b \Rightarrow \langle A \rangle = \langle A \cup \{b\} \rangle \Rightarrow b \in \langle A \rangle$ spor s předpokladem.
2. $a \in A$. Necht $A' = A \setminus \{a\}$. Pak

$$\langle A' \cup \{b\} \rangle = \langle A \cup \{b\} \rangle = \langle A' \cup \{b\} \cup \{a\} \rangle \Rightarrow a \in \langle A' \cup \{b\} \rangle$$

Pak ale a leží na nějaké přímce mezi A' i $\{b\}$. Neboli nastane situace na obrázku



$$b \in \langle \langle A' \rangle \cup \{a\} \rangle = \langle A \rangle$$

spor s předpokladem.

□

Pozorování 5.12 (Projektivní nezávislost a generované podprostory). $A_1, A_2 \subseteq P : \langle A_1 \rangle = \langle A_2 \rangle \Rightarrow \forall x : A_1 \cup \{x\}$ je projektivně nezávislá, právě když $A_2 \cup \{x\}$ je projektivně nezávislá.

Důkaz. Tvrzení je symetrické, stačí ukázat:

$$A_1 \cup \{x\} \text{ je pr n} \Rightarrow A_2 \cup \{x\} \text{ je pr n}$$

$$A_1 \cup \{x\} \text{ je pr n} \Rightarrow \langle A_1 \cup \{x\} \rangle \neq \langle A_1 \rangle \Rightarrow x \notin \langle A_1 \rangle \Rightarrow x \notin \langle A_2 \rangle \Rightarrow A_2 \cup \{x\} \text{ je pr n.}$$

□

Věta 5.13 (O výměně). Budte A, B projektivně nezávislé množiny v (P, \mathcal{L}) , $|A| < |B|$. Pak existuje $b \in B$ taková, že $A \cup \{b\}$ je projektivně nezávislá.

Důkaz. Indukci podle $|A|$ a zpětnou indukci (sestupně) dle $|A \cap B|$.

1) $A = \emptyset \Rightarrow B \neq \emptyset \Rightarrow \exists b \in B \Rightarrow A \cup \{b\} = \{b\}$ je triviální případ KPP.

$A \subseteq B \Rightarrow \exists b \in B \setminus A \Rightarrow A \cup \{b\}$ je pr nezávislá protože je podmnožinou pr nezávislé.

2) indukční krok $\exists a \in A \setminus B$. Uvažme $A' = A \setminus \{a\}$. Jelikož $|A'| < |A| < |B|$. Dle i.p $\exists b \in B : A' \cup \{b\}$ je pr nezávislá. Rozebereme případy:

1. $b \notin \langle A \rangle \xrightarrow{\text{lemma 5.11}} A \cup \{b\}$ je pr nezávislá.

2. $b \in \langle A \rangle$. Označme $A'' = A' \cup \{b\}$ $|A''| = |A| < |B|$. Taky $|A'' \cap B| > |A \cap B|$.

Dle i.p (velikost průniku) $\exists c \in B : A' \cup \{c\}$ je pr nezávislá. Dal $b \in \langle A \rangle \Rightarrow \langle A'' \rangle$. Dle 5.12 $A' \cup \{c\}$ je pr nezávislá.



□

Definice 5.14 (Projektivní báze). Projektivní báze je do inkluze maximální projektivně nezávislá množina.

Důsledek 5.15 (Projektivně nezávislá množina a báze). Každou projektivně nezávislou množinu lze doplnit na bázi a všechny projektivní báze mají stejnou mohutnost.

Důkaz. Nechť máme pr nezávislou A . KPP je konečný, takže i $\#$ pr nezávislých je konečný. Vezmeme největší B pr nezávislou. Pak buď $|A| = |B| \Rightarrow A$ je maximální je pr báze.

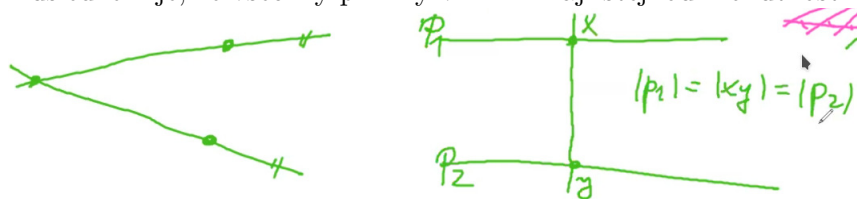
Nebo $|A| < |B| \xrightarrow{5.13} \exists b \in B : A \cup \{b\}$ je pr nezávislá. Můžeme postupovat dokud $|A| < |B|$. \square

Definice 5.16 (Dimenze). $\dim_P S = |B| - 1$, kde B je projektivní báze S .

Poznámka 5.17 (O dimenzi). • $\dim_P(\{a\}, \emptyset) = 0$

- $\dim_P(\emptyset, \emptyset) = -1$
- $\dim_P(\text{přímka}) = 2 - 1 = 1$. 2 body tvoří pr nezávislou množinu, 3 již určují stejnou přímku.
- Vezmeme 3 pr nezávislé body jejich obal je KPR. Pak $\dim_P(\text{KPR}) = 2$ Taký ale libovolný podprostor s $\dim_P = 2$ je KPR.

Důsledkem je, že všechny přímky v KPP mají stejnou mohutnost.



Příklad 5.18. Nechť $q = p^r$ taky $n \leq 3 \in \mathbb{N}$. Uvažme $GF(q)^{n+1}$, pak body jsou lineární obaly jednotlivých vektorů:

$$P = \{\langle u \rangle \mid u \in GF(q)^{n+1} \setminus \{0\}\}$$

Přímky budou všechny podprostory dimenze 2:

$$\mathcal{L} = \{\langle u, v \rangle \mid u, v \in GF(q)^{n+1}\}$$

Označme přímky určené vektory $u, v := l_{u,v}$.

Ověříme axiomy Definice 5.1:

1. $|l_{u,v}|$. Lineární kombinace dvou vektorů je tvaru $\alpha u + \beta v$. Kde $\alpha, \beta \in GF(q)$, neboli q možnosti zvolit každý. Musíme ale zahodit kombinaci která dává 0 vektor. Vždy ale $q-1$ násobku stejného vektoru je dle definice stejný bod.

$$\# = \frac{q^2 - 1}{q - 1} = q + 1$$

Toto q bude řád prostoru.

2. z konstrukce $\forall u, v \in LN \exists!$ přímka $l : \langle u \rangle, \langle v \rangle \in l$.
3. Nechť u, v, w jsou LN vektory. Vezmeme a, b ležící na přímce vu, uw :

$$a = \alpha u + \beta v, b = \gamma u + \delta w$$

Chceme $xa + yb = rv + sw$.

$$x(\alpha u + \beta v) + y(\gamma u + \delta w) = rv + sw$$

$$x\alpha + y\gamma = 0$$

$$x\beta = r$$

$$y\delta = s$$

Soustava má řešení.

Věta 5.19 (Singerova konstrukce). *Existuje-li (P, \mathcal{L}) KPP řádu q dimenze n , pak existuje cyklický $(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1})$ -BIBD.*

Důkaz. $V = P$, \mathcal{B} = nadroviny v (P, \mathcal{L}) = podprostory $\dim = n - 1$. Které vzniknou tak, že ve vektorovém prostoru vezmeme podprostor $\dim = n$.

$$|V| = |P| = \frac{q^{n+1}}{q-1} = q^n + q^{n-1} + \dots + 1$$

Velikost nadroviny $H \subseteq P : |H| = \frac{q^n-1}{q-1} = q^{n-1} + q^{n-2} + \dots + 1$. TODO □

Věta 5.20 (O dimenzi průniku a spojení). *Budte U, V podprostory (P, \mathcal{L}) . Pak $\dim_P(U \cap V) + \dim_P(U \vee V) = \dim P(U) + \dim_P(V)$.*

Důkaz. TODO □

Věta 5.21 (Modularita). *Nechť A, B, C jsou podprostory v (P, \mathcal{L}) taková, že $B \subseteq A$. Pak $A \cap (B \vee C) = B \vee (A \cap C)$.*

Důkaz. TODO □

Důsledek 5.22 (Průnikem dvou rovin v prostoru je přímka). *Bud' $P, \pi, \sigma : \dim_P P = 3, \dim_P \pi = \dim_P \sigma = 2, \pi \neq \sigma \Rightarrow \pi \cap \sigma$ je přímka - $\dim_P(\pi \cap \sigma) = 1$.*

Důkaz. TODO □

Věta 5.23 (Roviny si jsou podobné). *Bud' (P, \mathcal{L}) , s π, σ rovinami v P . Pak $\pi \cong \sigma$.*

Důkaz. TODO □

Věta 5.24 (Nadroviny KPP tvoří BIBD). *Bud' (P, \mathcal{L}) konečný projektivní prostor řádu q a dimenze n . Pak jeho nadroviny tvoří symetrický $(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1})$ -BIBD.*

Důkaz. TODO □

Věta 5.25 (KPP dimenze alespoň 3 mají Desargovskou vlastnost). *Konečné projektivní prostory dimenze alespoň 3 mají Desargovskou vlastnost.*

Důkaz. TODO □

Definice 5.26 (Automorfismus). *Bijekce $\alpha : (V, \mathcal{B}) \rightarrow (V, \mathcal{B})$ taková, že $\forall B \in \mathcal{B} \alpha[B] \in \mathcal{B}$ je automorfismus.*

Poznámka 5.27 (Inverz automorfismu je automorfismus). *Pro konečné prostory platí, že pro α automorfismus je α^{-1} automorfismus.*

Důkaz. TODO □

Definice 5.28 (Kolineace). *Kolineace je zobrazení $\alpha : V \cup \mathcal{B} \rightarrow V \cup \mathcal{B}$ takové, že $\alpha \upharpoonright V$ je bijekce na V , $\alpha \upharpoonright \mathcal{B}$ je bijekce na \mathcal{B} a $\forall x \in V, \forall B \in \mathcal{B} : x \in B \Leftrightarrow \alpha(x) \in \alpha(B)$.*

Věta 5.29 (Automorfismy a kolineace). *Nechť pro (V, \mathcal{B}) každé dva různé prvky patří do jednoho bloku a všechny bloky mají mohutnost alespoň 2. Nechť $\alpha : V \rightarrow V$ je permutace, $\bar{\alpha} : V \cup \mathcal{B} \rightarrow V \cup 2^V$ takové, že $\bar{\alpha}(x) = \alpha(x)$ a $\bar{\alpha}(B) = \alpha[B]$. Pak následující jsou ekvivalentní:*

1. α je automorfismus

2. $\bar{\alpha}$ je kolineace

3. α zachovává kolinearitu

Důkaz. TODO □

Poznámka 5.30 (Kolineace a obrazy přímek). Je-li α kolineace prostoru, pak $\forall x \neq y \in P : \alpha(xy) = \alpha(x)\alpha(y)$.

Důkaz. TODO □

Definice 5.31 (Fixace). $A \subseteq P$: α fixuje všechny body A , jestliže $\forall x \in A : \alpha(x) = x$
 $l \in \mathcal{L}$: α fixuje l , jestliže $\alpha[l] = l$.

Lemma 5.32 (Kolineace fixující nadrovinu). Buď α kolineace fixující všechny body nadroviny $H \subseteq P$. Pak existuje $C \in P$ tak, že α fixuje všechny přímky procházející bodem C .

Lemma 5.33 (Rozšíření kolineace). Mějme $q_0 \in \mathcal{L} \rightarrow (P', \mathcal{L}'), P' = P \setminus q_0$ množinový systém. Pak každou kolineaci α množinového systému (P', \mathcal{L}') je možno rozšířit na kolineaci α^* prostoru (P, \mathcal{L}) právě jedním způsobem, a tato kolineace fixuje q_0 .

Definice 5.34 (Centrální kolineace). Centrální kolineace (P, \mathcal{L}) je kolineace, pro niž existuje nadrovina H (nazývaná osa kolineace), jejíž všechny body jsou fixované kolineací α , a bod $C \in P$ (nazývaný střed kolineace) takový, že všechny přímky jím procházející jsou zobrazením α fixované.

(Pozor, může nastat $C \in H$ i $C \notin H$.)

Lemma 5.35 (Centrální kolineace jsou grupa). Centrální kolineace s osou H a středem C tvoří grupu vzhledem ke skládání, jednotkou je identita.

Lemma 5.36 (Vlastnosti centrální kolineace). Buď α centrální kolineace s osou H a středem C . Potom

1. $P \notin H \cup \{C\} \Rightarrow \forall x : \alpha(x)$ jednoznačně určuje $\alpha(P) : \alpha(x) = CX \cap F\alpha(P)$, kde $F = PX \cap H$
2. Není-li α identická kolineace, pak každý bod mimo $H \cup \{C\}$ není fixovaný
3. Centrální kolineace α je jednoznačně určena kteroukoliv dvojicí $P \neq \alpha(P)$.

Důsledek 5.37 (Jednoznanost středu i osy kolineace). Je-li α neidentická kolineace, pak její osa i střed jsou jednoznačně určeny.

Věta 5.38 (Baerova). Buď H nadrovina v Desargovském prostoru (P, \mathcal{L}) a buďte P, P', C tři různé kolineární body takové, že $P, P' \notin H$. Pak existuje právě jedna centrální kolineace α taková, že H je osa, C je střed a $\alpha(P) = P'$.

List of Theorems

1.1	Definice (Množinový systém)	2
1.2	Definice (Konečná projektivní rovina)	2
1.10	Definice (Konečná afinní rovina)	4
1.14	Definice (Desargova vlastnost)	6
1.15	Definice (Desargovská projektivní rovina)	6
2.1	Definice (Latinský obdélník)	6
2.4	Definice (Kolmost LČ)	7
2.5	Značení (NOLČ(n))	7
2.8	Definice (Ortogonální tabulka)	9
3.1	Definice (Blokové schéma (BIBD))	12
3.9	Definice (Symetrické blokové schéma)	14
3.13	Definice (Konstrukce blokových schémat ze symetrických)	16
3.20	Definice (Steinerův systém trojic)	20
3.22	Definice (Komutativní idempotentní kvazigrupa (KIK))	20
3.30	Definice (Hadamardova matice (HM))	24
3.32	Definice (Normální forma HM)	24
3.36	Definice (Tenzorový součin)	25
3.43	Definice (Charakterová matice Q)	26
4.1	Definice (Trochu méně pravidelné blokové schéma)	29
4.3	Definice (Průhledná množina)	30
4.4	Definice (BIBD se středníkem)	30
4.10	Definice (Řešitelný systém)	31
4.14	Definice (Skupinově rozložitelný systém)	33
5.1	Definice (Konečný projektivní prostor, kolinearita)	35
5.3	Definice (Podprostor)	35
5.7	Definice (Obal)	36
5.10	Definice (Projektivně nezávislá množina)	37
5.14	Definice (Projektivní báze)	38
5.16	Definice (Dimenze)	39
5.26	Definice (Automorfismus)	40
5.28	Definice (Kolineace)	40
5.31	Definice (Fixace)	41
5.34	Definice (Centrální kolineace)	41

List of Theorems

1.5	Věta (O řádu KPR)	2
1.6	Věta (Existence KPR)	3
1.8	Věta (KPR(6), Dk později)	4
1.12	Věta (O řádu KAR)	5
1.13	Důsledek (O vztahu KAR a KPR)	6
2.2	Věta (Latinské čtverce)	6
2.3	Důsledek	7
2.6	Věta (Horní odhad NOLČ)	7
2.7	Věta (Extremální NOLČ a KPR)	7
2.10	Věta (Ortogonální tabulka a NOLČ)	9
2.11	Věta (Tenz produkt Ortogonálních tabulek)	9
2.12	Věta (Dolní odhad NOLČ)	10
2.13	Důsledek	10
2.14	Lemma (OA $3m + 1$)	10
2.15	Věta (Dolní odhad NOLČ - 2)	11
3.2	Vlastnosti (BIBD)	12
3.3	Věta (Struktura BIBDu)	12
3.4	Vlastnosti (Struktura BIBDu)	13
3.6	Věta (Wilson (1975) BD)	13
3.7	Věta (Fisherová nerovnost)	13
3.8	Důsledek	13
3.10	Věta (Ekvivalence BIBD)	14
3.11	Věta (SBIBD ekvivalence)	14
3.12	Důsledek (Duální SBIBD)	15
3.15	Lemma (Lineární formy)	16
3.16	Věta (Bruck-Ryser-Chowla)	16
3.17	Důsledek (\nexists KPR(6))	18
3.18	Věta (Teorie čísel (BD))	18
3.19	Věta (\exists KPR \square)	19
3.21	Věta (Existence STS a počet prvků)	20
3.23	Věta (STS a speciální kvazigrupa)	20
3.24	Věta (Kombinace STS)	21
3.25	Důsledek (STS(9))	21
3.27	Věta (Nutná podmínka je i postačující pro STS)	21
3.28	Lemma (Tabulkový důkaz 1)	23
3.29	Lemma (Tabulkový důkaz 2)	23
3.31	Lemma (Transpozice Hadamardovy matice)	24
3.34	Věta (Hadamardova matice a řád dělitelný čtyřmi)	24
3.35	Věta (Hadamardova matice a symetrické BIBDy)	25
3.37	Věta (Kombinace Hadamardových matic)	25
3.38	Důsledek (Sylvester)	25
3.40	Důsledek (Exponenciální Hadamardovy matice)	25
3.41	Věta (Payleyho konstrukce)	25
3.42	Lemma (Posunutí χ)	26
3.44	Lemma (O tenzorovém součinu (BD))	27
3.46	Věta (Kombinace HM alternativní)	27
3.48	Věta (Payleyho konstrukce revisited)	28
3.49	Lemma (Williamson)	28

3.50	Věta (Williamsonova konstrukce)	29
4.5	Věta (Dolní odhad na NOLČ)	30
4.7	Věta $((v, k, 1)$ -BIBD a NOLČ)	31
4.8	Věta $((v, k, 1)$ -BIBD a NOLČ $(v - 3)$)	31
4.12	Věta (Řešitelnost a odhady na NOLČ)	32
4.15	Věta (NOLČ a existence GD)	33
4.16	Věta (Řešitelný GD a NOLČ)	33
4.17	Důsledek (O násobení NOLČ)	34
4.18	Lemma (Dolní odhad pro NOLČ)	34
4.19	Věta (NOLČ je aspoň 2)	35
5.5	Lemma (Průnik podprostorů je podprostor)	35
5.8	Lemma (O přidání prvku do podprostoru)	36
5.9	Lemma (Sjednocení podprostorů)	36
5.11	Lemma (Přidání prvku do projektivně nezávislé množiny)	37
5.13	Věta (O výměně)	38
5.15	Důsledek (Projektivně nezávislá množina a báze)	38
5.19	Věta (Singerova konstrukce)	40
5.20	Věta (O dimenzi průniku a spojení)	40
5.21	Věta (Modularita)	40
5.22	Důsledek (Průnikem dvou rovin v prostoru je přímka)	40
5.23	Věta (Roviny si jsou podobné)	40
5.24	Věta (Nadroviny KPP tvoří BIBD)	40
5.25	Věta (KPP dimenze alespoň 3 mají Desargovskou vlastnost)	40
5.29	Věta (Automorfismy a kolineace)	40
5.32	Lemma (Kolineace fixující nadrovinu)	41
5.33	Lemma (Rozšíření kolineace)	41
5.35	Lemma (Centrální kolineace jsou grupa)	41
5.36	Lemma (Vlastnosti centrální kolineace)	41
5.37	Důsledek (Jednoznačnost středu i osy kolineace)	41
5.38	Věta (Baerova)	41