Kombinatorické struktury

prof. RNDr. Jan Kratochvíl, CSc.

3. července 2021

Obsah

1 Konečné/Afinní projektivní roviny

Definice 1.1 (Množinový systém). Nechť 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. □

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 □

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

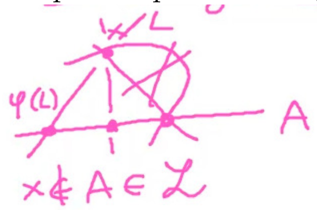
- $\forall A \in \mathcal{L} : |A| = m + 1$
- $\forall x \in X : |\{A \in \mathcal{L} : x \in A\}| = m + 1$
- $|X| = |\mathcal{L}| = m^2 + m + 1$

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:

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

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

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

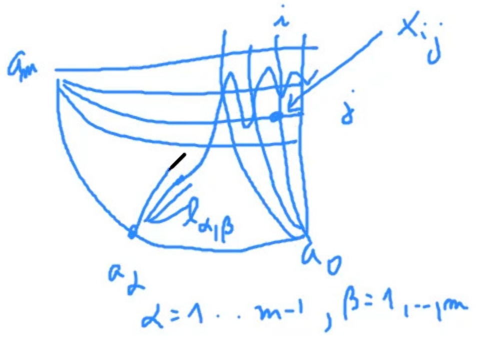
Důkaz. Konstruktivně pomoci $\mod$ aritmetiky. Z algebry $\exists GF(m)$ napíšeme jako

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

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

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

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



Šikmé přímky taky lze vyjádřit pomoci vzorečku (1):

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

Ověříme axiomy definition 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. Taky 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. Těmto 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 geometrii 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:

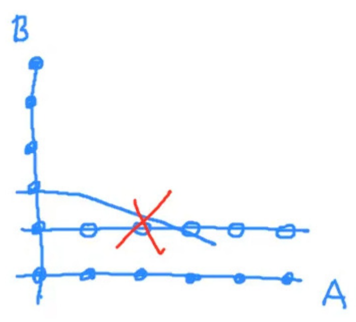
$$\varphi(L) = L \cap A, \varphi : \{L : x \in L \in \mathcal{L}, L \nparallel A\} \to A$$

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:

$$|A| + 1 = \# \text{ přímek obsahujících } x \tag{2}$$

Vezmeme 2 přímky $A, B : A \nparallel B$. Dle AF1, AF2, AF3 $\Rightarrow$ nejde pokryt 2ma různoběžnými přímkami. Pak $\exists t \notin A \cup B$, zobrazeni 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):

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

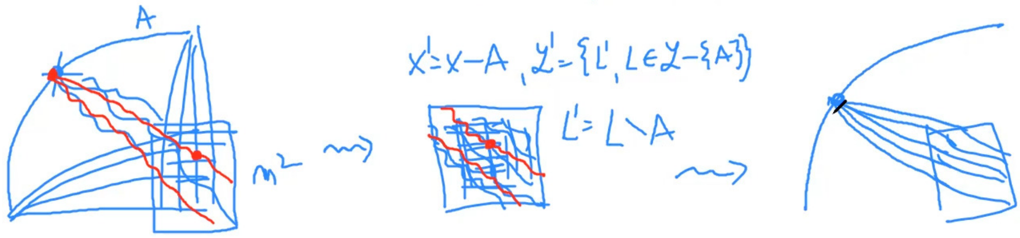


Vezmeme libovolnou přímku A, má m bodů. Přes libovolný bod $a \in A$ prochází další přímka B. Dle AF2 najdeme ke každému bodu $b_i \in B$ rovnoběžku k A která má dalších $(m-1)$ bodů. Konstrukce dává m rovnoběžek a m^2 bodů. Dohromady $|X| = m^2$.
Na jedné straně, počet bodu je m^2. Každým bodem prochází $(m+1)$ 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 řádku 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 extremální 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 neopakuji ani ve sloupcích ani v řádcích. Kde X je n-prvková množina. Typický $\{1, ..., n\} := [n]$.
Na řádky lze nahlížet jako na permutace.

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

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

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

Teď 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 párovaní, které určuje SRR. □

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

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

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

Pak dle věty každý obdélník lze doplnit na čtverec. □

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)). $NOL\check{C}(n)$ značíme největší počet navzájem ortogonálních Latinských čtverců řádu n.

Věta 2.6 (Horní odhad NOLČ).

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

Důkaz. Nechť

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

BUNO: přejmenujeme prvky v každém LČ tak, aby v prvním řádku bylo $\{1, 2, ..., n\}$. Takto vyrobíme LČ $L^{1\prime}, ..., L^{t\prime}$.
Tvrdíme ale, že ortogonalita je zachovaná. Obecně pro libovolná permutace π aplikovaná ne 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 pozice $(2, 1)$ můžou být prvky $\{2, ..., n\}$ po 2 různé. Takže $NOL\check{C}(n) \leq n - 1$. □

Kdy máme extremální řešení?

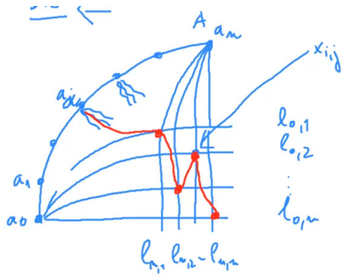
Věta 2.7 (Extremální NOLČ a KPR).

$$NOL\check{C}(n) = n - 1 \iff \exists KPR(n)$$

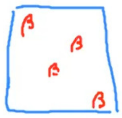
Z předchozí přednášky platí pro mocniny prvočísla.

Důkaz. $KRP \Rightarrow L\check{C}$. 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 neopakuji v rádcích 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.

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

$L\check{C} \Rightarrow KPR$. Nechť máme LČ

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

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 určené 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 # 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 2cí bodů prochází *právě 1* přímka.

□

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

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

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

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

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

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

Věta 2.10 (Ortogonální tabulka a NOLČ).

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

Důkaz. BUNO první řádek má bloky $i,i,...,i$ velikosti n. Druhý řádek bloky $1,2,...,n$ taky velikosti n. Jinak zvolíme vhodnou permutaci.
Pak vezmeme libovolný další řádek. Přemístíme blok velikosti n na řádek LČ.

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

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 pozice 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 ortogonální 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 $(d-2)$.
Obraceně, pokud máme $(d-2)$ LČ, tak je poskládáme do OA. □

Věta 2.11 (Tenz produkt Ortogonálních 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 $OA(n_1) : a_1, a_2, ..., a_n$ a řádek z $OA(n_2) : b_1, b_2, ..., b_n$.
Uděláme výsledný řádek pomoci tenzorového součinu:

$$(a_1, b_1)(a_1, b_2), ...(a_1, b_{n_2^2})(a_2, b_1)...$$

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

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

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

Důkaz. Nechť
$$s = \min_{i=1}^{k} \{p_i^{r_i} - 1\}$$
Z věty 2.6
$$NOL\check{C}(p_i^{r_i}) \geq p_i^{r_i} - 1$$
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

$$\exists OA(\prod_1^k p_i^{r_i}, s + 2) = OA(n, s + 2) \Rightarrow NOL\check{C}(n) \geq s$$

□

Důsledek 2.13.
$$\forall n \in \mathbb{N}, n > 2 \wedge n \not\equiv 2 \mod 4 : NOL\check{C}(n) \geq 2$$

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

Lemma 2.14 (OA 3m + 1).

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

Důkaz. Nechť $X = \{x_1, x_2, ..., x_m\}$. 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

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

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

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

Počet sloupců je

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

Teď 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 $0,1,...,m$.
- $z_{i,j}$ 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).

$$\forall k > 0 : NOL\check{C}(12k+10) \geq 2$$

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

$$\exists OA(4k+3,4) \overset{lemma\ 2.14}{\Rightarrow} \exists OA(3(4k+3)+1,4) = OA(12k+10,4) \iff NOL\check{C}(12k+10) \geq 2$$

□

Poznámka 2.16. Ortogonální tabulky se používají např pro rozvrhovaní 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 (BIDB)).

Definice 3.2 (Symetrické blokové schéma).

Věta 3.3 (Struktura BIBDu).

Důkaz. □

List of Theorems

List of Theorems