

**Úkol 3-1:** Z axiomů KPR ukažte následující

- $(\forall p_1, p_2, p_3 \in \mathcal{P})(\exists x \in \mathcal{X}) \quad x \notin p_1 \cup p_2 \cup p_3$  pokud uvažovaná KPR není Fanova rovina
- $(\forall x \in \mathcal{X})(\exists p_1, p_2, p_3 \in \mathcal{P}) \quad x \notin p_1 \cup p_2 \cup p_3$  kde  $p_1, p_2, p_3$  jsou vzájemně různé přímky

Kde  $\mathcal{X}$  je množina bodů a  $\mathcal{P}$  je množina přímek

**Řešení:** (příklady možných přístupů)

V prvním případě uvážíme čtveřici bodů  $C$  garantovanou axiomem (A3). Pokud některý z těchto bodů není na žádné z přímek, máme hotovo. V opačném případě uvážíme dvojici  $D = \{y, z\}$  bodů z  $C$ , která nepatří žádné ze zadaných přímek (dvojic na  $C$  je 6, pouze 3 mohou být zabrané přímkami) a vezmeme přímkou  $p$  procházející  $D$ . Z volby  $D$ ,  $y$  a  $z$  jsou každý incidentní s alespoň jednou ze zadaných přímek  $p_i$  (ale nemohou být incidentní se žádnou oba). Přímka  $p$  je tedy se tedy s dvěma z přímek (búno  $p_1, p_2$ ) protíná v bodech  $y$  a  $z$ . Protože uvažovaná KPR není Fanova rovina, obsahuje  $p$  minimálně dva další body. Jeden z nich může ležet na  $p_3$ , ale jeden už je nutně hledaný bod.

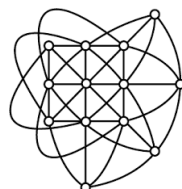
V postupu výše můžeme stejně tak zvolit  $y, z$  jako libovolné dva body na  $p_1$  a  $p_2$  které jsou různé od  $p_1 \cap p_2$ ,  $p_1 \cap p_3$  a  $p_2 \cap p_3$ . Protože každá přímka obsahuje minimálně 4 body, na každé je minimálně jeden vhodný bod.

Můžeme také dokázat prostě počítáním. Víme, že KPR obsahuje právě  $n^2 + n + 1$  bodů, z nichž  $p_1 \cup p_2 \cup p_3$  obsahuje nejvýše  $3n + 1$  bodů ( $3n$  pokud přímky tvoří trojúhelník a  $3n + 1$  pokud se protínají v jediném společném průniku). Existuje tedy alespoň  $n^2 - 2n$  nepokrytých vrcholů, což je nenulové množství pro všechny řády větší než 2.

V druhém případě uvážíme opět čtveřici  $C$  bodů garantovanou axiomem (A3). V  $C$  existují dva body  $y, z$  různé od  $x$ . Každý bod je incidentní s  $n + 1 \geq 3$  přímkami. Body  $y$  a  $z$  jsou dohromady incidentní s alespoň pěti přímkami (jedna přímka je incidentní s oběma). Nejvýše dvě z těchto přímek obsahují  $x$  (jedna z přímek procházejících  $y$  a jedna procházející  $z$ , může se jednat o tu samou přímkou pokud je to společná přímka). Zbývají tedy alespoň tři příčky incidentní s  $y$  a nebo  $z$ , které neobsahují  $x$ .

Argument je jednodušší pro řád alespoň 3, kde stačí uvážit svazek přímek kolem jednoho vrcholu různého od  $x$ , ty jsou alespoň 4 a nejvýše jedna z nich je incidentní s  $x$ . Fanovu rovinu můžeme vyřešit zvlášť.

Alternativně můžeme opět počítat. Bod  $x$  je incidentní s  $n + 1$  přímkami. Celkem KPR obsahuje  $n^2 + n + 1$  přímek, máme tedy  $n^2 \geq 4$  přímek neobsahujících  $x$ .



**Úkol 3-2:** Chceme zkonstruovat  $n - 1$  vzájemně ortogonálních latinských čtverců řádu  $n$  pro nějaké  $n$  alespoň 4. Načrtněte takovou konstrukci a explicitně sestavte tři takové čtverce (které lze zaručeně doplnit na plný počet čtverců pokud nejsou všechny). Nechceme řešit hrubou silou.

**Řešení:**

Čtverce sestavíme pomocí KPR stejného řádu. Pro úplnost si projdeme teorii proč něco takového lze udělat.

Obecně postup vypadá následovně. Zafixujeme jednu přímku  $p$ , a dva její body  $x, y$ , ostatní body označíme jako  $a, b, c, \dots$ . Označme si svazky přímek procházející jednotlivými body (vyjma  $p$ ) jako  $X, Y, A, B, C, \dots$ , resp. Svazky  $X$  a  $Y$  budou tvořit mřížku čtverce, přímky v obou svazcích libovolně očíslovme a asociujeme s řádky/sloupci příslušného indexu. Body ve kterých se přímky z  $X$  protínají s přímkami z  $Y$  odpovídají jednotlivým pozicím čtverce. Na obrázku výše máme KPR řádu 3 znázorněnou jako mřížku, přímka  $p$  je napravo, její body shora dolů odpovídají  $a, x, b, y$ .

Z každého svazku  $A, B, C, \dots$  nyní extrahujeme jeden čtverec. Vezměme např. svazek  $A$ . Přímky opět libovolně očíslovme, a každému políčku ve čtverci přiřadíme číslo přímky, která obsahuje bod asociovaný s daným políčkem. Proč je takto vyplněný čtverec latinský? Fixní přímka  $q$  ze svazku  $A$  protíná každou z přímek ze svazků  $X, Y$  právě jednou, a to právě v mřížce (mimo  $p$ ). Každé číslo se tedy objeví v právě jednom sloupci a právě jednom řádku. Navíc dvě přímky  $q_1, q_2$  ze stejného svazku se nemohou ve mřížce protnout, protože již sdílí bod na  $p$ , vyplnění polí je tedy takto dobře definováno.

Zbývá nahlédnout, že čtverce definované  $A$  a  $B$  jsou ortogonální. Ortogonalita by byla narušena, pokud by se stejný (uspořádaný) pár čísel sešel na dvou pozicích. To by ale znamenalo, že příslušné přímky z  $A$  a  $B$  obsahují oba body asociované s daným polem, což je spor.

Abychom mohli postup aplikovat, potřebujeme konkrétní KPR. Vezměme tedy třeba KRP získanou pomocí konstrukce z modulárního tělesa  $\mathbf{F}_7$ . Každá přímka je zde asociovaná s dvojicí  $a, b \in \mathbf{F}_7 \cup \{\star\}$  a její body jsou dvojice  $(x, y)$  splňující vztah  $ax + b = y$  (vše v tělese  $\mathbf{F}_7$ ), resp.  $x = b$  pro přímky s nekonečným / 'vertikálním' sklonem ( $a = \star$ ). Pro úplnou definici KPR musíme ještě doplnit body v nekonečnu odpovídající průsečíkům všem sklonům ' $a$ ', a speciální přímku  $p$  procházející všemi body v nekonečku. Poznamenejme, že každý sklon (hodnota  $a$ ) představuje jeden svazek, kde svazek  $X$  je definovaný přímkami s  $a = 0$  a  $Y$  je definovaný přímkami s  $a = \star$  (rovností  $x = b$ ). Jako svazek  $A$  si vezměme přímky se sklonem 1. Pro hodnoty  $b \in \{0, 1, 2, 3, 4, 5, 6\}$  dostáváme přímky

$\{(0, 0), (1, 1), (2, 2), \dots\}, \{(0, 1), (1, 2), (2, 3), \dots\}, \dots$

Postup můžeme interpretovat algebraicky i jinak. Pomocí přímk se sklonem  $a$  definujeme  $a$ -tý čtverec. Na přímce  $p_{a,b}$  leží body  $(x, y)$  splňující  $ax + b = y$ , a ty dostanou v  $a$ -tém čtverci hodnotu  $b$ . Naopak se tedy můžeme zeptat, jaká je hodnota  $b$  pro danou souřadnici  $x, y$  a čtverec s indexem  $a$ ? Algebraickou eliminací  $b$  dostáváme, že  $b = ax - y$  (v tělese  $\mathbf{F}_7$ ).

Celý čtverec "1" je vlevo nahoře (čtverec reprezentujeme jako 1. kvadrant, tedy  $(0, 0)$  vlevo dole). Další čtverce zkonstruujeme obdobně.

1	2	3	4	5	6	0
2	3	4	5	6	0	1
3	4	5	6	0	1	2
4	5	6	0	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5
0	1	2	3	4	5	6

4	5	6	0	1	2	3
1	2	3	4	5	6	0
5	6	0	1	2	3	4
2	3	4	5	6	0	1
6	0	1	2	3	4	5
3	4	5	6	0	1	2
0	1	2	3	4	5	6

6	0	1	2	3	4	5
5	6	0	1	2	3	4
4	5	6	0	1	2	3
3	4	5	6	0	1	2
2	3	4	5	6	0	1
1	2	3	4	5	6	0
0	1	2	3	4	5	6

5	6	0	1	2	3	4
3	4	5	6	0	1	2
1	2	3	4	5	6	0
6	0	1	2	3	4	5
4	5	6	0	1	2	3
2	3	4	5	6	0	1
0	1	2	3	4	5	6

Můžeme si všimnout, že čtverce z modulárních KPR mají hezkou strukturu, každý sloupec/řádek je cyklický posun předchozího sloupce/řádku o fixní počet pozic (posun je jiný pro každý čtverec a odpovídá sklonu přímek). Přirozeně, KPR vzniklé z modulárních aritmetik jsou speciální podtřída KPR, čtverce definované ostatními KPR takovou strukturu nemají. Jako příklad uveďme jeden z NOLČ získaný z KPR řádu 4, kde výběrem reprezentace lze uspořádat sloupce jako cyklické posuny jednoho vzoru, ale tyto posuny nejsou pravidelné, a řádky už jednotnou strukturu nemají.

3	0	2	1
2	3	1	0
1	2	0	3
0	1	3	2

KPR tohoto řádu zkonstruujeme stejným algebraickým předpisem, ale místo prvků  $\{0, 1, 2, 3\}$  použijeme prvky  $\{0, 1, x, 1+x\}$  představující  $\mathbf{F}_2^2$  jako polynomy stupně nejvýše 1. Sčítání funguje jako u standardních polynomů, násobení také, ale výsledky jsou moduleny nějakým polynomem stupně 2 ireducibilním nad tělesem  $\mathbf{F}_2$ , v tomto tělese existuje jediný,  $x^2 + x + 1$ .

**Úkol 3-3:** První dva axiomy KPR, (A1) a (A2), hovoří o právě jedné přímce (" $= 1$ "), a právě jednom bodě (" $= 1$ ").

Uvažte všechny možnosti uvolnění jednoho nebo obou axiomů na nerovnosti (" $\leq 1$ " a " $\geq 1$ "). Pro každou možnost ukažte, že po příslušné změně axiomů stále dostáváme právě KPR, nebo ukažte protipříklad. Existuje celkem 8 možností jak axiomy uvolnit, některé kombinace lze vyřešit dohromady.

**Řešení:**

Uvažme nejprve uvolnění axiomů na "nejvýše jeden".

Pro ( $\leq$ A2) dostáváme mimo jiného vlastnosti klasické geometrie. Jako konkrétní příklad můžeme vzít 4 vrcholy čtverce, a 6 přímkou tvořících jeho strany a diagonály. Protože protipříklad splňuje (A3) a (A1) dokonce rovností, funguje i pro jakékoliv současné uvolnění (A1).

Pro ( $\leq$ A1) můžeme třeba vzít nějakou KPR a vhodně z ní ubrat přímky, třeba všechny přímky procházející jedním bodem. Jako více konkrétní příklad můžeme vzít třeba opět 4 body, na třech vybudovat trojúhelník třemi přímkami, a jeden bod nechat zcela bez přímkou. Nebo jako více extrémní příklad můžeme mít libovolnou množinu (alespoň čtyř) bodů, zcela bez přímkou. Opět všechny protipříklady fungují pro jakékoliv současné uvolnění (A2).

Uvažme současné uvolnění obou axiomů nahoru ( $\geq$ A1)+(A2).

Jako protipříklad poslouží třeba KPR, ve které všechny přímky zdvojíme. Každé dva body definují přímku (dokonce několik), a každé dvě přímky se protínají - pokud vznikly z různých přímkou KPR, potom v jednom bodě, pokud se jedná o kopie té samé přímky, potom ve všech bodech.

Nelíbí-li se nám uvažovat multimnožinový systém přímkou, můžeme do Fanovy roviny například přidat přímku  $q$  na čtyřech bodech, která je nadmnožina jiné přímky  $p$  ( $q = p \cup \{x\}$  pro bod  $x$ ,  $x \notin p$ ). Nahlédneme, že axiom (A3) je splněn. Obecně v KPR můžeme uvážit libovolný bod, dvě přímky jím procházející, a vzít dva jiné body z každé přímky - tato čtveřice bude splňovat (A3), jak jsme vypořizovali na cvičení. Uvažme tedy čtveřici  $C$  získanou jako ostatní body dvou přímkou procházejících  $x$ . Ve Fanově rovině  $C$  splňuje (A3), v novém systému může (A3) porušit pouze  $q$ , ale  $C \cap q = C \cap p$  a tento průnik má nejvýše dva body.

Zbývá pouze uvážit uvolnění jednoho z axiomů na "alespoň 1".

( $\geq$ A1) : Uvažme dvojici bodů  $x, y$ , které dávají dvě přímky  $p, q$ . Potom ale  $p \cap q \supset \{x, y\}$ , a tedy axiom (A2) je porušen, což je spor. Axiom (A1) tedy platí s rovností a dostáváme původní axiomy KPR.

( $\geq$ A2) : Také musí dávat právě KPR, což plyne z předchozího dualitou. Pokud dokážeme přímo, argument je skoro totožný.