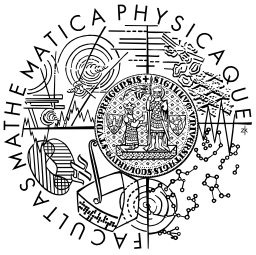


MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Michal Košek

Míchání karet a grupa Mathieu M12

Katedra algebry

Vedoucí bakalářské práce: prof. RNDr. Aleš Drápal, CSc., DSc.

Studijní program: Matematika

Studijní obor: Obecná matematika

Praha 2021

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Podpis autora

Na tomto místě bych rád poděkoval svému vedoucímu prof. RNDr. Aleši Drápalovi, CSc., DSc. za ochotu a trpělivost při vedení práce. Dále děkuji spolužačce Báře Tížkové za korekturu.

Název práce: Míchání karet a grupa Mathieu M12

Autor: Michal Košek

Katedra: Katedra algebry

Vedoucí bakalářské práce: prof. RNDr. Aleš Drápal, CSc., DSc., Katedra algebry

Abstrakt: Cílem práce je prezentovat dvojí popis vysoce tranzitivní grupy M_{12} a srovnání těchto přístupů. Prvním z nich je reprodukce popisu M_{12} v kontextu míchacích grup. Při této příležitosti popisujeme míchací grupy včetně známých výsledků i otevřených problémů. Druhou zvolenou možností je nová konstrukce pomocí rozšířených ternárních Golayových kódů nad projektivní rovinou řádu 3. Tímto získáme důkaz části známého tvrzení o vztahu monomiálních automorfismů Golayových kódů a Mathieuových grup. Část textu je proto také věnována seznámení s afinními a projektivními rovinami a samoopravnými kódy. V obou případech se využívá projekce monomiálních matic nad tříprvkovým tělesem na symetrickou grupu S_{12} zapomínající znaménka.

Klíčová slova: míchací grupa, rozšířený ternární Golayův kód, Mathieu grupa M12

Title: Card shuffling and the Mathieu group M12

Author: Michal Košek

Department: Department of Algebra

Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc., Department of Algebra

Abstract: The goal of this thesis is to present a description of a highly transitive group M_{12} in two different ways and a comparison of these methods. First of them is a reproduction of a construction of M_{12} in the context of shuffle groups. We use this opportunity to provide a description of shuffle groups including known results as well as open problems. The second method of choice is a new construction based on extended ternary Golay codes over a projective plane of order 3. This also gives us a proof of a part of a well known theorem linking monomial automorphisms of Golay codes and Mathieu groups. Part of the text is therefore dedicated to an introduction to affine and projective planes and error-correcting codes. Both approaches take advantage of a projection of monomial matrices over a field of order 3 onto the symmetric group S_{12} given by forgetting the signs.

Keywords: shuffle group, extended ternary Golay code, Mathieu group M12

Obsah

Úvod

Podstatou některých kouzelnických karetních triků je ovlivňování pořadí karet v balíku posloupností promíchání. Jedním typem takového míchání je takzvané „farao“, na které se v této práci omezíme. Při něm je balík $2n$ karet rozdělen na dva poloviční, které se následně po jednotlivých kartách proloží a vznikne tak nový balík. Pokud kouzelník znal původní stav balíku a provedl trik dokonale, dokáže přesně určit, na které pozici se každá karta nyní nachází. Nabízí se otázka, zda může uvažovat i opačně, tedy zda dokáže k dané kartě a pozici najít poslopnost míchání, po nichž bude tato karta v kýžené pozici. Obecněji jej může zajímat, jak a zda vůbec lze balík karet dostat z jedné konfigurace do jiné.

Matematicky lze situaci popsat jako množinu karet s grupou permutací generovanou jednotlivými promícháními, která na této množině působí. Očíslujeme-li karty přirozenými čísly podle jejich původního pořadí, můžeme zamíchaný balík chápat opět jako permutaci a ztotožnit jej s prvkem grupy. Tu nazveme *míchací grupou*, což bude základní objekt našeho zkoumání. Budeme-li znát její strukturu, dokážeme odpovědět na existenční část původní otázky. V situaci se dvěma balíčky závisí výsledek každého míchání na tom, ze kterého balíčku odebereme první kartu, a tedy máme dané dva generátory této grupy.

Diaconis, Graham a Kantor [1] ve své práci plně popsali strukturu míchací grupy v případě dvou balíčků a libovolného sudého počtu karet. Dalším možným krokem je zobecnění pro více balíčků, kde však není na první pohled jasné, co je takovým mícháním myšleno. Základní operace (permutace, kterou budeme dále značit σ) bude analogická té v případě dvou balíčků. Při ní rozdělíme balík do k menších po n kartách, které postupně stavíme do řady — vlevo budeme mít první (horní) balíček. Poté opakovaně procházíme balíčky zleva doprava a vždy sejmeme horní kartu a umístíme ji dospodu nového balíku. K tomu ale připustíme změny pořadí balíčků před provedením σ. Takové změny pořadí budeme chápat jako permutace na k prvcích. Pro jednoduchost předpokládáme, že tyto permutace tvoří grupu $P \leqslant S_k$[1]. Všimneme si, že pro $k = 2, P = S_2$ dostáváme původní příklad se dvěma balíčky.

Přirozenou volbou P je například celá symetrická grupa S_k, případně cyklická grupa C_k nebo dvouprvková grupa generovaná obrácením pořadí balíčků. Ukázalo se však, že je výhodné zkoumat obecnější případy, kde pouze klademe určitá omezení na strukturu P (například požadujeme, aby působila tranzitivně). To vedlo k objevení sktruktury míchací grupy pro několik tříd případů v závislosti na počtu karet, balíčků a povolených permutacích balíčků [2]. Obecně ovšem zůstává otázka struktury míchací grupy nevyřešena i při zdánlivě silných a přirozených omezeních.

Zajímavé je, že v popisu míchacích grup dvou balíčků figuruje vysoce tranzitivní grupa známá jako Mathieuova grupa M_{12}. Toto bylo hlavní motivací pro naši práci, ve které nejprve popíšeme tuto grupu jako míchací a následně ukážeme novou konstrukci M_{12} na základě článku [3].

V první kapitole zavedeme používané netriviální pojmy z teorie grup a popíšeme M_{12} jako vysoce tranzitivní grupu. Druhou kapitolu věnujeme seznámení s míchacími grupami a důkazu tvrzení o M_{12} jakožto míchací grupě. Třetí kapitola

[1] Obecně lze uvažovat libovolnou podmnožinu $A \subseteq S_k$.

je věnována afinním a projektvním rovinám nad konečnými tělesy a samoopravným kódům. Konečně ve čtvrté kapitole ukážeme vlastní konstrukci této grupy založenou na Golayových kódech nad projektivní rovinou.

1. Tranzitivita a grupa Mathieu M_{12}

Značení. Nechť $n \in \mathbb{N}$. Symetrickou grupu na $\{0, \dots, n-1\}$ značíme S_n. Alternující grupu na $\{0, \dots, n-1\}$ značíme A_n.

Definice 1.1 (působení grupy na množině)**.** *Nechť G je grupa, X je množina.* Působením *G na X rozumíme homomorfismus* $\mathrm{f}\colon G \to S_X$*, kde S_X je grupa permutací na X. V takovém případě můžeme pro $x \in X, g \in G$ psát $gx = g(x) \coloneqq \mathrm{f}(g)(x)$.*

Dále definujeme orbitu *prvku $x \in X$ jako $G(x) \coloneqq \{gx \mid g \in G\}$ a* stabilizátor *prvku $x \in X$ jako $G_x := \{g \in G \mid gx = x\}$. Orbity zřejmě tvoří třídy ekvivalence na X.*

Definice 1.2 (vlastnosti působení)**.** *Nechť G je grupa, X je množina, na které G působí. Řekneme, že působení je* věrné*, pokud je příslušný homomorfismus prostý.*

Řekneme, že působení je tranzitivní*, pokud pro každé dva prvky X existuje prvek G, který zobrazuje jeden na druhý. Ekvivalentně je působení tranzitivní, pokud má jedinou orbitu.*

*Řekneme, že působení je k-*tranzitivní *pro $k \in \mathbb{N}$, pokud $|G| \geq k$ a pro každé dvě k-tice vzájemně různých bodů*[2] *$(x_1, \dots, x_k), (y_1, \dots, y_k) \in X^k$ existuje prvek $g \in G$, pro který $g(x_i) = y_i \; \forall i \leq k$. Toto působení je* ostře *k-tranzitivní, pokud je toto g jednoznačně určeno.*

Grupa je k-tranzitivní*, pokud existuje množina, na které působí věrně a k-tranzitivně.*

Lemma 1.3 (vztah orbity a stabilizátoru)**.** *Nechť G je konečná grupa, X je množina, na které G působí, $x \in X$. Potom platí $|G| = |G(x)| \cdot |G_x|$.*

Speciálně pokud je působení tranzitivní, platí $|G| = |X| \cdot |G_x|$

Důkaz. G_x zřejmě tvoří podgrupu G. Z Lagrangeovy věty tedy máme $|G| = |G_x| \cdot [G : G_x]$. Dále máme bijekci mezi levými rozkladovými třídami G_x a orbitou $G(x)$ danou $gG_x \mapsto gx$.

Platí totiž $gx = hx \iff (h^{-1}g)x = x \iff h^{-1}g \in G_x$.

□

Díky klasifikaci konečných jednoduchých grup jsou známy všechny 2-tranzitivní grupy a jejich maximální tranzitivita [4]. Pro naše účely bude stačit klasifikace 5-tranzitivních grup a 2-tranzitivních grup daného řádu.

Příklad. Symetrická grupa S_n je n-tranzitivní. Alternující grupa A_n je $(n-2)$-tranzitivní.

Věta 1.4 ([5], vysoce tranzitivní grupy)**.** *Kromě $S_n, n \geq 5$ a $A_n, n \geq 7$ existují až na izomorfismus dvě 5-tranzitivní grupy. Tyto jsou řádů $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ a $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 16 \cdot 3$. Nazývají se pořadě Mathieuovy grupy M_{12}, M_{24}.*

Lemma 1.5 ([6], tranzitivní grupy řádu 95 040)**.** *M_{12} je jediná 2-tranzitivní grupa řádu $95\,040 = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$.*

[2] Tj. $x_i \neq x_j, y_i \neq y_j$ pro $i \neq j$.

2. Míchací grupy

Tato kapitola shrnuje poznatky z prací [1],[2],[7].

2.1 Definice a základní pozorování

V jazyce teorie grup definujeme pojmy z teorie míchacích grup, se kterými budeme dále pracovat, a formulujeme o nich jednoduchá tvrzení.

Značení. Nechť $a \in \mathbb{N}$. Pak definujeme $[a] \coloneqq \{0, \dots, a-1\}$. Množinu $[k]$ pak zpravidla chápeme jako množinu balíčků a $[n]$ jako možné pozice karty v jednom balíčku.

Úmluva. Permutace budeme skládat v pořadí zprava doleva.

Definice 2.1 (souřadnice)**.** *Nechť k,$n \in \mathbb{N}, x \in [k], y \in [n]$. Souřadnicemi karty $xn + y$ nazveme uspořádanou dvojici $(x,\ y)$. Tato karta se nachází na pozici y v balíčku x.*

Definujeme permutaci σ, která zprostředkovává „farao“. Při něm nejprve sejmeme první kartu z každého balíčku počínaje vrchním, poté všechny druhé karty, až nakonec poslední kartu posledního balíčku. Před kartou se souřadnicemi (x, y) jsme takto sejmuli $yk + x$ karet, což odpovídá i jejímu indexu v $[kn]$ po zamíchání.

Definice 2.2 (permutace σ)**.** *Nechť $k, n \in \mathbb{N}$. Zobrazením σ značíme permutaci na $[kn]$ danou předpisem*

$$\sigma(xn + y) = yk + x, \text{kde } x \in [k], y \in [n].$$

Lemma 2.3 ([7, Proposition 1], ekvivalentní definice σ)**.** *Nechť $k, n \in \mathbb{N}, a \in [kn]$. Platí*

$$\sigma(a) = \begin{cases} nk - 1, & \text{je-li } a = nk - 1, \\ ak \pmod{nk-1}, & \text{jinak.} \end{cases}$$

Důkaz. Pro $a = nk - 1$ máme

$$\begin{aligned} \sigma(nk-1) &= \sigma((k-1)n + (n-1)) = \\ &= (n-1)k + (k-1) = nk - k + k - 1 = nk - 1. \end{aligned}$$

Pro $a = xn + y \leq nk - 2$ máme:

$$\begin{aligned} \sigma(a) = \sigma(xn + y) = yk + x &\overset{(\mathrm{mod}\ nk-1)}{\equiv} yk + xnk = \\ &= (xn + y)k = ak. \end{aligned}$$

Navíc $\sigma(a) < nk - 1$, tedy $\sigma(a) = ak \pmod{nk-1}$.

□

K definici míchací grupy potřebujeme kromě σ také permutace karet indukované permutacemi balíčků. Pořadí karty v rámci balíčku se tímto nezmění, a proto indukovaná permutace odpovídá permutaci první souřadnice.

Definice 2.4 (permutace ρ)**.** *Nechť $k, n \in \mathbb{N}, \pi \in S_k$. Zobrazením ρ_π značíme permutaci na $[kn]$ danou předpisem*

$$\rho_\pi(xn + y) = \pi(x)n + y, \text{kde } x \in [k], y \in [n].$$

Definice 2.5 (míchací grupa)**.** *Nechť $k, n \in \mathbb{N}, P \leqslant S_k$.* Míchací grupou $\mathrm{Sh}(P, n)$ *(z anglického shuffle) nazveme podgrupu S_{kn} generovanou jednotlivými „farao“ mícháními s určenými pořadími balíčků, tedy*

$$\mathrm{Sh}(P, n) \coloneqq \langle \sigma\rho_\pi \mid \pi \in P \rangle.$$

Lemma 2.6 ([2], ekvivalentní definice míchací grupy)**.** *Nechť $k, n \in \mathbb{N}, P \leqslant S_k$. Potom*

$$\mathrm{Sh}(P, n) = \langle \sigma, \rho_\pi \mid \pi \in P \rangle.$$

Důkaz. Označme $\overline{\mathrm{Sh}(P, n)} = \langle \sigma, \rho_\pi \mid \pi \in P \rangle$. Zřejmě $\mathrm{Sh}(P, n) \leqslant \overline{\mathrm{Sh}(P, n)}$. Pro $\overline{\mathrm{Sh}(P, n)} \leqslant \mathrm{Sh}(P, n)$ stačí ukázat, že $\sigma \in \mathrm{Sh}(P, n)$ a $\rho_\pi \in \mathrm{Sh}(P, n)$ $\forall \pi \in P$.

Protože $\sigma = \sigma\rho_{\mathrm{id}}$, stačí položit $\pi = \mathrm{id}$ a dostaneme $\sigma \in \mathrm{Sh}(P, n)$.

Protože $\sigma\rho_\pi, \sigma^{-1} \in \mathrm{Sh}(P, n)$, máme $\rho_\pi = (\sigma^{-1})(\sigma\rho_\pi) \in \mathrm{Sh}(P, n)$.

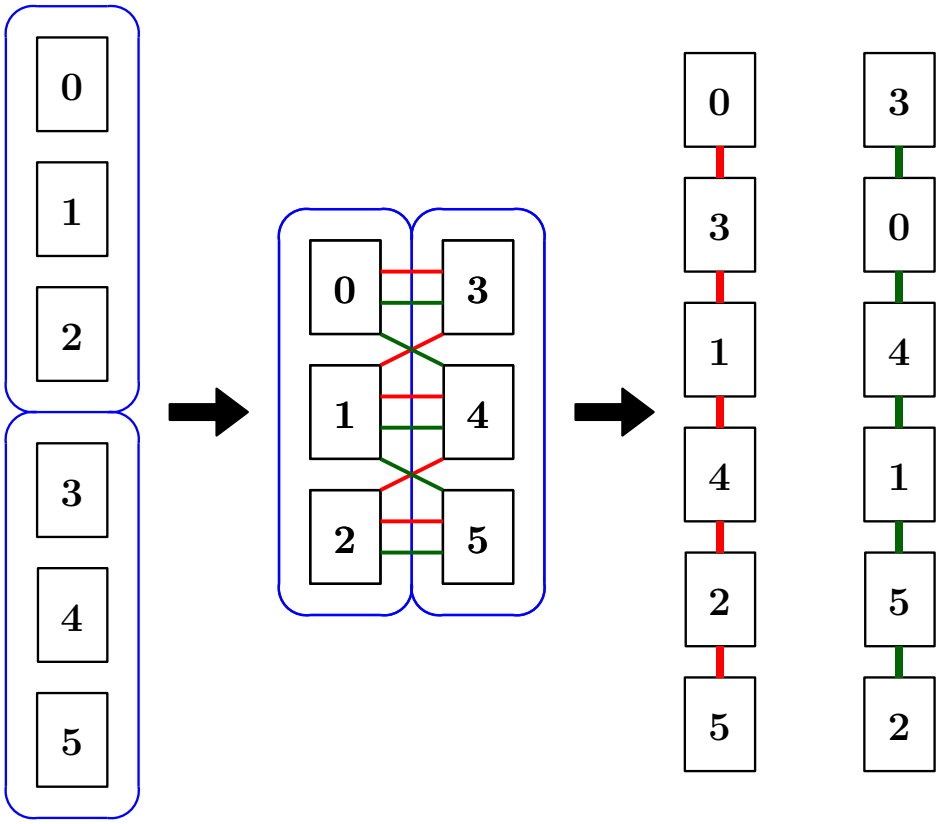
□

Na příkladu se šesti kartami a dvěma balíčky ilustrujeme práci s míchacími grupami.

Příklad. Nechť $k = 2, n = 3, P = S_2$. Potom

$$P = \{\mathrm{id}_2, (0\ 1)\}, \rho_{\mathrm{id}_2} = \mathrm{id}_6, \rho_{(0\ 1)} = (0\ 3)(1\ 4)(2\ 5), \sigma = (0)(1\ 2\ 4\ 3)(5)$$

a tedy $\mathrm{Sh}(P, n) = \langle (0\ 3)(1\ 4)(2\ 5), (1\ 2\ 4\ 3) \rangle \leqslant S_6$, což je grupa řádu 24 izomorfní S_4. Následující obrázek znázorňuje obě možná míchání, tj. generátory $\sigma, \sigma\rho_{(0\ 1)}$.



Obrázek 2.1: Generátory Sh(S_2,3).

2.2 Známé výsledky a otevřené otázky

Formulujeme klíčovou hypotézu 2.8 o struktuře $\mathrm{Sh}(S_k, n)$, podle které je tato grupa ve většině případů „největší možná“ při omezení, které dává následující jednoduché lemma.

Lemma 2.7 ([2, Corollary 2.4], parita $\mathrm{Sh}(P, n)$)**.** *Nechť $k, n \in \mathbb{N}$, $P \leqslant S_k$. Potom $\mathrm{Sh}(P, n) \leqslant A_{kn}$, právě když $n(n-1)k(k-1) \equiv 0 \pmod 4$ a platí alespoň jedno z následujících:*

- $n \equiv 0 \pmod 2$,
- $P \leqslant A_k$.

Důkaz. Platí $\mathrm{Sh}(P, n) \leqslant A_{kn}$, právě když všechny prvky dané množiny generátorů $\mathrm{Sh}(P, n)$ jsou sudé. Uvažujme generátory z lemmatu 2.6.

Permutace ρ_π je tvořena np cykly, kde p je počet cyklů v rozkladu π. Tedy ρ_π je sudá, právě když n je sudé nebo $\pi \in A_k$.

Ukážeme, že permutaci σ lze zapsat jako složení $\frac{n(n-1)k(k-1)}{4}$ transpozic. Tedy že je sudá, právě když jedno z čísel $n, n-1, k, k-1$ je dělitelné čtyřmi.

Značí-li $\mathrm{f}(a) := |\{b \mid a < b \wedge \sigma(b) < \sigma(a)\}|$, platí $\mathrm{f}(xn + y) = y(k - 1 - x)$,

a tedy

$$\sum_{i=0}^{kn-1} \mathrm{f}(i) = \sum_{x=0}^{k-1}\sum_{y=0}^{n-1} \mathrm{f}(xn+y) = \sum_{x=0}^{k-1}\sum_{y=0}^{n-1} y(k-1-x) =$$
$$= \sum_{x=0}^{k-1} \frac{n(n-1)}{2}(k-1-x) = \frac{n(n-1)k(k-1)}{4}.$$

Navíc počet transpozic odpovídá $\sum \mathrm{f}(i)$.

□

Hypotéza 2.8 ([2, Conjecture 1.3], o struktuře $\mathrm{Sh}(S_k, n)$)**.** *Nechť* $k, n \in \mathbb{N}, k \geq 3$, $P \leqslant S_k, n \neq k^f, (k,n) \neq (4, 2^f)$ *pro všechna* $f \in \mathbb{N}$. *Potom*

$$\mathrm{Sh}(S_k, n) = \begin{cases} A_{kn}, & \text{pokud } n \equiv 0 \pmod 4 \text{ nebo } (k,n) \pmod 4 \in \{(0,2),(1,2)\}, \\ S_{kn}, & \text{jinak.} \end{cases}$$

Pravdivost tohoto tvrzení v plné obecnosti je otevřený problém. Uvedeme však několik tříd dvojic (k, n), pro které již bylo dokázáno viz [2].

- $k > n$,
- $k = 2^e, n \neq 2^f$, kde $e, f \in \mathbb{N}, e \geq 2$,
- $k = l^e, n = l^f$, kde $l, e, f \in \mathbb{N}, l \geq 2, k \neq 4, e \nmid f$.

Všimněme si, že hypotéza nic neříká o situaci, kdy $P = S_2$. Pro tu máme následující tvrzení popisující strukturu $\mathrm{Sh}(S_2, n)$ v závislosti na n. Pro detailní popis a vysvětlení symbolů viz [1].

Tvrzení 2.9 ([1, Theorem 1], o struktuře $\mathrm{Sh}(S_2, n)$)**.** *Struktura* $\mathrm{Sh}(S_2, n)$ *je dána následující tabulkou:*

Tvar n	$\mathrm{Sh}(S_2, n)$
$n = 2^f$	$C_2 \wr C_{f+1}$
$n \equiv 0 \pmod 4, n \geq 20, n \neq 2^f$	$\mathrm{Ker}(\mathrm{sgn}) \cap \mathrm{Ker}(\overline{\mathrm{sgn}})$
$n \equiv 1 \pmod 4, n \geq 5$	$\mathrm{Ker}(\overline{\mathrm{sgn}})$
$n \equiv 2 \pmod 4, n \geq 10$	$C_2 \wr S_n$
$n \equiv 3 \pmod 4$	$\mathrm{Ker}(\mathrm{sgn}\,\overline{\mathrm{sgn}})$
$n = 6$	$C_2^6 \rtimes PGL(2,5)$
$n = 12$	$C_2^{11} \rtimes M_{12}$

Tabulka 2.1: Tvar $\mathrm{Sh}(S_2, n)$.

Zde C_k *je cyklická grupa na* $[k]$, $\wr$ *značí věncový součin,* $\rtimes$ *semidirektní součin,* $\mathrm{sgn}\colon C_2 \wr S_k \to \{-1, 1\}$ *je homomorfismus daný znaménkem permutace* $2k$ *karet (běžné znaménko permutace),* $\overline{\mathrm{sgn}}\colon C_2 \wr S_k \to \{-1, 1\}$ *je homomorfismus daný znaménkem permutace* k *dvojic karet (v působení popsaném v následujícím oddílu),* $\mathrm{sgn}\,\overline{\mathrm{sgn}}(g) := \mathrm{sgn}(g)\overline{\mathrm{sgn}}(g)$. *Konečně* $\mathrm{PGL}(n, p)$ *je projektivní lineární grupa z definice 3.9.*

2.3 Míchací grupy a grupa Mathieu M_{12}

Z posledního řádku tabulky 2.1 vidíme $S \coloneqq \mathrm{Sh}(S_2, 12) \cong C_2^{11} \rtimes M_{12}$. Tedy že míchací grupa pro 24 karet rozdělených do dvou balíků je izomorfní semidirektnímu součinu $C_2^{11} \rtimes M_{12}$. V tomto oddíle tento výsledek na základě [1] reprodukujeme.

Nejprve si rozmyslíme, že S zachovává dvojice karet $\{i, 23-i\}$. To nám dovolí uvážit homomorfismus $\pi\colon S \to S_{12}$ slučující tyto dvojice[3]. Označíme-li $K \coloneqq \mathrm{Ker}(\pi), H \coloneqq \mathrm{Im}(\pi)$, platí $S = K \rtimes H$. Navíc protože zřejmě $K \leqslant C_2^{12}$, stačí ukázat $H \cong M_{12}$ a ověřit řád K.

Lemma 2.10 (dvojice)**.** $\mathrm{Sh}(S_2, n)$ *zachovává dvojice karet* $\{i, 2n-1-i\}$*, tj.*

$$\forall s \in \mathrm{Sh}(S_2, n)\ \forall i < n\ \exists j < n\colon s(\{i, 2n-1-i\}) = \{j, 2n-1-j\}.$$

Důkaz. Tvrzení stačí ověřit pro $s \in \{\sigma, \rho_{(0\,1)}\}$. Ať $i < n$.

Pro $s = \rho_{(0\,1)}$ máme

$$\begin{aligned} s(i) &= s(0n+i) = n+i, \\ s(2n-1-i) &= s(n+(n-1-i)) = n-1-i \end{aligned}$$

z definice 2.4. Ale $2n-1-(n-1-i) = n+i$ a tudíž pro s tvrzení platí.

Pro $s = \sigma$ máme

$$\begin{aligned} s(i) &= s(0n+i) = 2i, \\ s(2n-1-i) &= s(n+(n-1-i)) = 2(n-1-i)+1 \end{aligned}$$

z definice 2.2. Ale $2n-1-(2n-1-2i) = 2i$ a tudíž pro s tvrzení platí.

□

Věta 2.11 ([1, Lemma 5], obraz π)**.** *Platí* $H = \mathrm{Im}(\pi) \cong M_{12}$.

Důkaz. H je generována permutacemi $\varphi = (0)(1\ 2\ 4\ 8\ 7\ 9\ 5\ 10\ 3\ 6\ 11)$ a $\psi = (4\ 9)(0\ 1\ 3\ 7\ 8\ 6\ 10\ 2\ 5\ 11)$, kde i odpovídá dvojici karet $\{i, 23-i\}$. Pomocí výpočetního softwaru zjistíme, že tyto permutace generují grupu řádu $95\,040 = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$.

Zbývá ověřit, že je tato grupa 2-tranzitivní. Z lemmatu 1.5 je pak $H \cong M_{12}$.

K rozšíření $(x_1, x_2) \mapsto (y_1, y_2)$ nejprve vhodnou kombinací φ, ψ zobrazíme $(x_1, x_2) \mapsto (0, z_2)$. Poté iterací φ zobrazíme $(0, z_2) \mapsto (0, \psi^{-k}(y_2))$, pro které $\psi^{-k}(y_1) = 0$. To lze, protože 0 je pevným bodem φ. Konečně aplikací ψ^k máme celkem $(x_1, x_2) \mapsto (y_1, y_2)$.

□

K ověření řádu K stačí pomocí generátorů S přímo spočítat (opět pomocí známých generátorů a výpočetního softwaru) (viz [1, Table 1]) $|S| = \frac{2^{12} \cdot 12!}{7! \cdot 2}$, a proto $|K| = |S|/|H| = 2^{11}$.

[3] Toto navíc obhajuje $C_2 \wr S_k$ a $\overline{\mathrm{sgn}}$ z předchozí tabulky.

3. Golayův kód nad projektivní rovinou

Zavedeme řadu pojmů a formulujeme tvrzení týkající se afinních a projektivních prostorů a lineárních a afinních kódů. Konkrétně budeme hovořit o afinní a projektivní rovině řádu 3 a o Golayových kódech.

3.1 Afinní a projektivní roviny

Začneme formalizací afinních rovin.

Značení. $\mathbb{F}_p$ značí těleso o p prvcích.

Definice 3.1 (afinní rovina)**.** *Afinní rovinou nazveme dvojici* (A, L)*, kde platí:*

- $L \subseteq \mathcal{P}(A)$*, kde* $\mathcal{P}$ *značí potenční množinu,*
- $\forall p \neq q \in A\ \exists! l \in L \colon \{p, q\} \subseteq l$*,*
- $\forall l \in L\ \forall p \in A \setminus l\ \exists m \in L \colon p \in m \wedge l \cap m = \emptyset$*,*
- $\exists p_1, p_2, p_3 \in A\ \forall l \in L \colon \{p_1, p_2, p_3\} \not\subseteq l$*.*

Prvky A *nazýváme* body *afinní roviny a prvky* L *nazýváme* přímky*. Vztah* $p \in l$ *nazýváme* incidencí *bodu a přímky. Přímky, ktere nemají společný bod, se nazývají* rovnoběžné*.*

Poznámka.

- Je-li A konečná, existuje $n \in \mathbb{N}$, že pro všechna $l \in L \colon |l| = n$. Toto n nazveme *řádem* afinní roviny.
- Relace „být rovnoběžný“ je ekvivalence na L.
- Pro afinní rovinu řádu n je $|A| = n^2$.

Definice 3.2 (model afinní roviny řádu 3)**.** *Nechť* V *značí vektorový prostor* $\mathbb{F}_3^2$*.*

Modelem afinní roviny řádu 3 *rozumíme dvojici* (V, L)*, kde* L *jsou afinní přímky* V*, tj. afinní podprostory dimenze* 1*. Snadno lze ověřit, že taková konstrukce opravdu dává afinní rovinu řádu* 3 *ve smyslu definice 3.1.*

Lemma 3.3 (jednoznačnost afinní roviny řádu 3)**.** *Nechť* A, B *jsou afinní roviny řádu* 3*. Potom* $A \cong B$*, tedy existuje bijekce mezi množinami bodů, která zachovává incidenci.*

Důkaz. Ať (A, L) je afinní rovina řádu 3. Ukážeme, že (A, L) je izomorfní modelu afinní roviny z předchozí definice. Protože $|A| = 3^2 = 9$, můžeme uvážit bijekci $A \to \mathbb{F}_3^2$ a příslušné body můžeme ztotožnovat. Dále budeme postupně konstruovat jednotlivé přímky L, které jsou vynucené axiomy afinní roviny.

Nejprve přidáme 3 rovnoběžné přímky (množiny vektorů se stejnou první souřadnicí) a poté další 3 vzájemně rovnoběžné přímky (množiny vektorů se stejnou

druhou souřadnicí)[4]. Každou volnost v této konstrukci lze snadno obhájit bijekcí zachovávající incidenci. Zbylých 6 přímek je už vynucených druhým axiomem z definice 3.1.

Konečně zkontrolujeme, že žádnou další přímku už přidat nelze.

□

Definice 3.4 (afinní grupa)**.** *Nechť $\mathbb{F}_p$ je těleso, $n \in \mathbb{N}$.* Afinní grupou *nazveme grupu* $\mathrm{AGL}(n,p) \coloneqq T \rtimes \mathrm{GL}(n,p)$*, kde* $\mathrm{GL}(n,p)$ *je grupa automorfismů* $\mathbb{F}_p^n$ *a* T *je grupa permutací* $\mathbb{F}_p^n$ *tvaru* $x \mapsto x + \lambda$ *(translací).*

Nás bude zajímat $\mathrm{AGL}(2,3)$ a její působení na afinní rovinu řádu 3.

Pozorování 3.5 (působení $\mathrm{AGL}(2,3)$)**.** *Prvky* $\mathrm{AGL}(2,3)$ *odpovídají složením lineárních automorfismů* $\mathbb{F}_3^2$ *a translací. Toto dává přirozené působení* $\mathrm{AGL}(2,3)$ *na* $\mathbb{F}_3^2$*.*

Lemma 3.6 (ekvivalentní definice $\mathrm{AGL}(2,3)$)**.** $\mathrm{AGL}(2,3)$ *jsou právě automorfismy* $\mathbb{F}_3^2$ *zachovávající afinní přímky.*

Důkaz. Prvky $\mathrm{AGL}(2,3)$ z definice zachovávají afinní přímky.

K automorfismu f zachovávajícímu přímky máme translaci t, že $tf(0,0) = (0,0)$. Protože automorfismy vektorového prostoru jsou afinní zobrazení, existuje $h \in \mathrm{AGL}(2,3)$, že $(0,0), (1,0), (0,1)$ jsou pevné body htf. Ze zachování přímek lze snadno vidět, že $htf = \mathrm{id}$. Protože $\mathrm{AGL}(2,3)$ tvoří grupu, máme $f \in \mathrm{AGL}(2,3)$.

□

Podobně jako v afinním případě formalizujeme projektivní roviny.

Definice 3.7 (projektivní rovina)**.** *Projektivní rovinou nazveme dvojici* (P, L)*, kde platí:*

- $L \subseteq \mathcal{P}(P)$*, kde* $\mathcal{P}$ *značí potenční množinu,*
- $\forall p \neq q \in P\ \exists! l \in L \colon \{p,q\} \subseteq l$*,*
- $\forall l \neq m \in L \colon |l \cap m| = 1$*,*
- $\exists p_1, \ldots, p_4 \in P\ \forall l \in L \colon \{p_1, \ldots, p_4\} \not\subseteq l$*.*

Prvky P *nazýváme* body *projektivní roviny a prvky* L *nazýváme* přímky*. Vztah* $p \in l$ *nazýváme* incidencí *bodu a přímky.*

Je-li P konečná, existuje $n \in \mathbb{N}$, že pro všechna $l \in L \colon |l| = n + 1$. Toto n nazveme *řádem* projektivní roviny.

Definice 3.8 (model projektivní roviny řádu 3)**.** *Na množině* $V = \mathbb{F}_3^3 \setminus \{(0,0,0)\}$ *zavedeme relaci ekvivalence danou* $x \sim y$*, pokud* $x = ky$ *pro* $k \in \{1,2\}$*.*

Modelem projektivní roviny řádu 3 *rozumíme faktormnožinu* $V/\sim$*. Prvky faktoru odpovídají bodům a přímky v tomto modelu definujeme jako obrazy dvourozměrných podprostorů* V *při faktorizaci* $\sim$*. Snadno lze ověřit, že taková konstrukce opravdu dává projektivní rovinu řádu* 3 *ve smyslu definice 3.7.*

Body $V/\sim$ *značíme* $1, \ldots, 12, \infty$*.*

[4]Každá třída ekvivalence rovnoběžnosti je právě tříprvková.

Definice 3.9 (projektivní lineární grupa)**.** *Nechť $\mathbb{F}_p$ je těleso, $n \in \mathbb{N}$.* Projektivní lineární grupou *nazveme faktorgrupu* $\mathrm{PGL}(n,p) \coloneqq \mathrm{GL}(n,p)/H$*, kde* $\mathrm{GL}(n,p)$ *je grupa automorfismů* $\mathbb{F}_p^n$ *a* $H \leqslant \mathrm{GL}(n,p)$ *je grupa automorfismů tvaru* $x \mapsto \lambda x$*.*

Nás bude zajímat $\mathrm{PGL}(3,3)$ a její působení na projektivní rovinu řádu 3.

Pozorování 3.10 (působení $\mathrm{PGL}(3,3)$)**.** *Uvažme grupu* $\mathrm{PGL}(3,3)$*. Potom H z 3.9 odpovídá grupě generované zobrazením $x \mapsto 2x$. Protože H zachovává ekvivalenční třídy $\sim$ z 3.8, máme přirozené věrné působení* $\mathrm{PGL}(3,3)$ *na projektivní rovinu.*

Konečně uvedeme zásadní souvislost afinních a projektivních rovin.

Lemma 3.11 (souvislost afinních a projektivních rovin)**.** *Odstraněním přímky projektivní roviny (spolu s jejími body) získáme afinní rovinu. Naopak přidáním bodů odpovídajících třídám ekvivalence rovnoběžnosti k afinní rovině, prodloužením přímek do příslušného bodu a přidáním přímky obsahující všechny tyto třídy získáme projektivní rovinu. O přidaných bodech a přímce mluvíme jako o bodech a přímce v nekonečnu.*

Konkrétně přidáním 4 *bodů k modelu afinní roviny řádu* 3 *získáme model projektivní roviny řádu* 3*. Navíc každý prvek* $\mathrm{AGL}(2,3)$ *lze přirozeně rozšířit na prvek* $\mathrm{PGL}(3,3)$ *zachovávající přímku v nekonečnu.*

Důsledek 3.12 (jednoznačnost projektivní roviny řádu 3)**.** *Nechť P, Q jsou projektivní roviny řádu* 3*. Potom $P \cong Q$, tedy existuje bijekce mezi množinami bodů, která zachovává incidenci.*

Důkaz. Přímo plyne z jednoznačnosti afinní roviny řádu 3 (3.3) a souvislosti afinních a projektivních rovin (3.11).

□

Úmluva. Ve zbytku textu budeme projektivní (afinní) rovinou rozumět model projektivní (afinní) roviny řádu 3 z definice 3.8 (3.2). Body $1, \ldots, 9$ chápeme jako afinní (resp. afinní část projektivní roviny), $10, 11, 12, \infty$ jsou pak body v nekonečnu.

3.2 Samoopravné kódy

Úmluva. Nechť $n, p \in \mathbb{N}$, $\mathbb{F} = \mathbb{F}_p$ je p-prvkové těleso, $V = \mathbb{F}^n$.

Definice 3.13 (blokový kód a slova)**.** Blokovým kódem (*také jen* kódem) *rozumíme libovolnou podmnožinu V. Řekneme, že kód je* afinní (lineární)*, pokud tvoří afinní (lineární) podprostor V.*

Prvky prostoru V nazýváme také slova*. Souřadnici i slova s budeme značit* $s^{(i)}$[5]. Délkou *slova, případně kódu, nazveme dimenzi vektorového prostoru n.* Nosičem *slova s nazveme množinu nenulových souřadnic s, značíme* $\mathrm{supp}(s)$. Váhou *slova s nazveme počet nenulových souřadnic s, značíme* $|s| \coloneqq |\mathrm{supp}(s)|$. Vzdáleností *slov s, r nazveme hodnotu* $|s - r|$.

[5]Zde indexujeme od 1.

Pozorování 3.14 (vlastnosti váhy)**.** *Zobrazení* $w\colon V \to \mathbb{N}$ *dané* $s \mapsto |s|$ *splňuje:*

- $\forall s, r \in V\colon w(s+r) \leq w(s) + w(r)$,
- $w(s) = 0 \iff s = \mathbf{0}$, *kde* $\mathbf{0}$ *je nulový vektor.*

Definice 3.15 (bodový součin a samodualita)**.** *Zavedeme operaci* bodového součinu $\cdot\colon V \times V \to \mathbb{F}$ *danou* $u \cdot v = \sum u^{(i)} v^{(i)}$.

Řekneme, že kód C *ve* V *je* samoduální*, pokud*

$$C = C^{\perp} \coloneqq \{v \in V \mid \forall c \in\ C\colon v \cdot c = 0\}.$$

Definice 3.16 (parametry afinních kódů)**.** *Nechť* C *je afinní kód ve* V*. Řekneme, že* C *je* (n, k, d) *kód, pokud* $k = \dim C, d = \min_{r \neq t \in C} |r - t|$*. Parametr* $d = \mathrm{d}(C)$ *nazýváme* (minimální) vzdálenost *kódu.*

Definice 3.17 (rozšiřování a propichování)**.** *Nechť* $n \in \mathbb{N}, i \leq n, C$ *je kód v* $\mathbb{F}^n$*. Definujeme* propíchnutí *kódu* C *v souřadnici* i *jako kód* $\pi(C) = \{\pi(c) \mid c \in C\}$*, kde* π *značí projekci na souřadnice různé od* i*.*

Naopak rozšíření *kódu* C *definujeme jako kód* $\sigma(C) = \{\sigma(c) \mid c \in C\}$*, kde* σ *značí přidání souřadnice* $n+1$ *tak, aby* $\sum_{1 \leq i \leq n+1} \sigma(c)^{(i)} = 0$*.*

Definice 3.18 (Perfektní kód)**.** *Kód* C *ve* V *s minimální vzdáleností* d *je* perfektní*, pokud existuje* $r \in \mathbb{N}$*, pro které* $V = \bigcup_{c \in C} \mathrm{S}(c, r)$*, kde* $\mathrm{S}(c, r) \coloneqq \{v \in V \mid |v - c| \leq r\}$*, a* $\mathrm{S}(c, r)$ *jsou po dvou disjunktní.*

V takovém případě je r *určeno jednoznačně a* $2r = d - 1$*.*

3.3 Golayovy kódy a jejich automorfismy

V této sekci zkonstruujeme z přímek v projektivní rovině model rozšířeného ternárního Golayova kódu.

Pro úplnost zavedeme běžné binární i ternární Golayovy kódy. Dále se však budeme zabývat převážně konkrétními modely rozšířeného ternárního Golayova kódu.

Definice 3.19 (Golayovy kódy)**.** Perfektním binárním Golayovým kódem *nazveme lineární kód nad* $\mathbb{F}_2$ *s parametry* $(23, 12, 7)$. Rozšířeným binárním Golayovým kódem *nazveme lineární kód nad* $\mathbb{F}_2$ *s parametry* $(24, 12, 8)$.

Perfektním ternárním Golayovým kódem *nazveme lineární kód nad* $\mathbb{F}_3$ *s parametry* $(11, 6, 5)$. Rozšířeným ternárním Golayovým kódem *nazveme lineární kód nad* $\mathbb{F}_3$ *s parametry* $(12, 6, 6)$.

Lemma 3.20 ([8], vlastnosti Golayových kódů)**.** *Každý ze čtyř Golayových kódů existuje a je určen jednoznačně až na* monomiální *transformaci (danou složením permutace souřadnic a přenásobením každé souřadnice nenulovou konstantou).*

Perfektní binární a ternární Golayovy kódy jsou perfektní ve smyslu definice 3.18. Rozšířené Golayovy kódy jsou samoduální.

Rozšířením perfektních Golayových kódů získáme rozšířené Golayovy kódy. Naopak propíchnutím rozšířených Golayových kódů získáme perfektní Golayovy kódy.

Lemma 3.21 ([8], perfektní kódy daných parametrů)**.** *Perfektní kód nad* $\mathbb{F}_2$ *s parametry* $(23, 12, 7)$ *je lineární. Perfektní kód nad* $\mathbb{F}_3$ *s parametry* $(11, 6, 5)$ *je lineární. Jde tedy o Golayovy kódy.*

Úmluva. Dále budeme Golayovým kódem myslet rozšířený ternární, pokud neuvedeme jinak.

Uvážíme vektory incidence přímek v projektivní rovině, tj. vektory délky 13, které mají na j-té pozici 1, právě když bod j leží na této přímce. V opačném případě je na pozici j 0.

Označíme S' množinu incidenčních vektorů s nenulovou souřadnicí ∞. Zbylé označíme P'. Odstraněním této souřadnice z vektorů S' a P' získáme množiny S a P. Konečně $2P$ bude značit množinu $\{2p \mid p \in P\}$.

Definice 3.22 (kód $[A]$)**.** *Při značení výše definujeme kód* $[A]$*, kde* $A \coloneqq S \cup 2P$ *a* $[X]$ *značí afinní obal množiny* X*, tj.*

$$[X] \coloneqq \{\sum_{x \in X} a_x x \mid \sum_{x \in X} a_x = 1, a_x \in \mathbb{N}\}.$$

Tvrzení 3.23. *Kód* $[A]$ *a kódy tvaru* $[A] - v = \{w - v \mid w \in [A]\}, v \in [A]$ *mají parametry* $(12, 6, 6)$*. Kódy* $[A] - v$ *jsou navíc lineární a tedy jde o rozšířené ternární Golayovy kódy.*

Důkaz. Délky kódů jsou jasné z konstrukce. Translace zachovávají dimenzi i vzdálenost kódu, stačí tedy určit $\dim[A] - v$ pro zvolený $v \in [A]$ a $\mathrm{d}([A])$.

- *Dimenze* $[A] - v$*:* Lze ověřit přímo. (známe generující množinu)
- *Minimální vzdálenost* $[A]$*:* Viz [3, Proposition 4].

□

Odtud dále zafixujeme $s \in S$ a položíme $L \coloneqq [A] - s$.

Objektem zkoumání budou automorfismy Golayových kódů. Pro naše potřeby se omezíme na monomiální automorfismy, které nyní definujeme.

Definice 3.24 (automorfismus lineárního kódu)**.** *Nechť* C *je lineární kód ve vektorovém prostoru* V*.* Automorfismem *kódu* C *rozumíme automorfismus* φ *prostoru* V *daný* monomiální *maticí (tj. obsahující právě jednu nenulovou souřadnici v každém řádku i sloupci) splňující* $\varphi(C) \subseteq C$*. Zobrazení dané monomiální maticí nazveme* monomiální[6]*.*

Automorfismy kódu C *tvoří grupu, kterou značíme* $\mathrm{Aut}(C)$*.*

Konečně formulujeme a dokážeme dvě technická lemmata o rozšířených ternárních Golayových kódech.

Lemma 3.25 ([3, Lemma 5])**.** *Nechť* $C \subseteq \mathbb{F}_3^{12}$ *a existuje* $c \in C$*, že* $C - c$ *je (rozšířený ternární) Golayův kód. Nechť* $w \in \mathbb{F}_3^{12}$*,* $|w| = 3$*.*

Pak buď existuje $v \in C$ *takové, že* $|w - v| \leq 2$*, nebo existují* $v_i \in C, i \in \{1, 2, 3, 4\}$ *taková, že* $|v_i - w| = 3$*,* $|(\sum v_i) - w| = 12$*. V takovém případě neexistují jiná* $v \in C$*:* $|v - w| \leq 3$*.*

[6]Toto odpovídá definici v lemmatu 3.20.

Důkaz. Předpokládejme, že neexistuje $v \in C\colon\ |w - v| \leq 2$.

Jednoznačnost: Pokud pro $u, v \in C$ platí $|w - v| = |w - u| = 3$ a existuje souřadnice i taková, že $(w - v)^{(i)} \neq 0, (w - u)^{(i)} \neq 0$, platí $|v - u| \leq 5$, a tedy $v = u$ z minimální vzdálenosti Golayových kódů. Všechny takové vektory se tudíž od w liší na vzájemně různých souřadnicích. Proto mohou existovat nejvýše 4 vektory $v_i \in C\colon\ |v_i - w| = 3$. Navíc pokud existují, platí

$$\left|(\sum v_i) - w\right| = \left|(\sum v_i - w)\right| = 12.$$

Existence: Zvolme souřadnici $1 \leq i \leq 12$. Stačí ukázat, že existuje $v_i \in C$ takové, že $v_i^{(i)} \neq w^{(i)}$ a $|w - v_i| = 3$. Propíchnutím i-té souřadnice získáme z kódu C perfektní ternární Golayův kód C' a ze slova w slovo w', pro které (viz lemma 3.20) existuje $v_i' \in C'\colon\ |v_i' - w'| = 2$, kde v_i' vzniklo propíchnutím z $v_i \in C$. Potom ale $|v_i - w| \leq 3$ a z předpokladu důkazu $|v_i - w| = 3$.

□

Lemma 3.26 ([3, Lemma 6])**.** *Nechť $r \in \mathbb{F}_3^{12}, |r| = 3, r^{(i)} \in \{0, 1\}\ \forall i \leq 12$.*

Potom existuje $\delta = \pi\varrho \in \mathrm{Aut}(L)$, kde π je příslušná permutace souřadnic a ϱ přenásobení souřadnic nenulovými konstantami, pro které $\delta(L + r) = [A]$, $\varrho(r) = r$ a $\delta(r) = s$.

Důkaz. Z lemmatu 3.23 víme, že $\min_{v \in L} |v| \geq \mathrm{d}([A]) = 6$, protože slova z L jsou rozdíly slov z $[A]$. Díky tomu a trojúhelníkové nerovnosti pro váhu (3.14) neexistuje $v \in L\colon\ |-r - v| \leq ||r| - |v|| = 2$.

Použijeme lemma 3.25 na vektor $-r$ a kód L. Tím získáme slova $v_1, \ldots, v_4$. Protože $|0 - r| = 3$, máme z jednoznačnosti $v_i = \mathbf{0}$ pro nějaké i. Bez újmy na obecnosti položíme $v_4 = \mathbf{0}$.

Dále z lemmatu 3.25 máme

$$12 = \left|\sum(v_i) + r\right| = \left|\sum(v_i + r)\right| \leq \sum |v_i + r| = 4 \cdot 3 = 12.$$

To je možné pouze pokud $\mathrm{supp}(v_i + r)$ jsou disjunktní množiny.

Položíme $w_i \coloneqq v_i + r$. Máme tedy jednoznačně dané zobrazení ϱ, pro které platí $\mathrm{supp}(\varrho(w_i)) = \mathrm{supp}(w_i)$ a všechny nenulové souřadnice $\varrho(w_i)$ jsou rovné 1, tj. ϱ je zobrazení dané přenásobením souřadnic, které vektory w_i zobrazuje na příslušné incidenční. Navíc zřejmě $\varrho(r) = \varrho(v_4 + r) = \varrho(w_4) = w_4 = r$.

V kódu $\varrho(L + r)$ nyní najdeme množinu 9 vektorů $2\mathcal{P} \coloneqq \{\varrho(w_5), \ldots, \varrho(w_{13})\}$, jejichž nosiče spolu s nosiči $\mathcal{S} \coloneqq \{\varrho(w_1), \ldots, \varrho(w_4)\}$ tvoří přímky projektivní roviny řádu 3 (kde přímky odpovídající $\mathcal{S}$ se protínají v ∞). Potom se totiž kódy $[A]$ a $\varrho(L + r)$ liší pouze permutací souřadnic, tedy existuje permutace souřadnic $\pi\colon\ \pi(\varrho(L+r)) = [A]$. Pak položíme $\delta = \pi\varrho$. Navíc lze π zvolit tak, aby $\pi(\varrho(r)) = s$, přičemž lze navíc předepsat libovolné ze 6 zobrazení nenulových souřadnic r na nenulové souřadnice s.

Konečně $[A] = \delta(L + r) = \delta(L) + \delta(r) = \delta(L) + s$, a tedy $L = [A] - s = \delta(L)$. Odtud $\delta \in \mathrm{Aut}(L)$.

Zbývá tedy najít množinu $2\mathcal{P}$ a dokázat, že s $\mathcal{S}$ tvoří projektivní rovinu. Propíchnutím $\varrho(L+r)$ v libovolné souřadnici získáme perfektní kód, který obsahuje 6 slov váhy 3[7]. Protože $\varrho(L + r)$ neobsahuje jiná slova váhy 3 než $\varrho(w_1), \ldots, \varrho(w_4)$,

[7] Viz zdroj, pomocí váhových polynomů.

vznikla 3 z těchto propíchnutých slov ze slov váhy 4. Navíc kód $\varrho(L+r)$ neobsahuje jiná slova váhy 4 s nenulovou propíchnutou souřadnicí. Takto můžeme propíchnout každou souřadnici a získáme tak celkem 9 slov váhy 4 v kódu $\varrho(L+r)$ [8]. Těchto 9 slov označíme $\varrho(w_5), \ldots, \varrho(w_{13})$.

Zvolíme $i \leq 4, j \neq k \geq 5$ a označíme $p = \varrho(w_i), q_1 = \varrho(w_j), q_2 = \varrho(w_k)$. Ukážeme, že:

- $q_1^{(k)} = 2 \; \forall k \in \mathrm{supp}(q_1)$,
- nosiče p, q_1 a q_1, q_2 se protínají v právě jednom bodě,
- každými dvěma souřadnicemi prochází právě jeden nosič $\varrho(w_1), \ldots, \varrho(w_{13})$,
- $[\mathcal{S} \cup 2\mathcal{P}] = \varrho(L+r)$.

Tím ověříme axiomy projektivní roviny 3.7 (bodem ∞ a zvolenou souřadnicí prochází prvek $\mathcal{S}$) a ukážeme, že se $[A]$ a $\varrho(L+r)$ liší pouze permutací souřadnic.

Kódy tvaru $\varrho(L+r) - v, v \in \varrho(L+r)$ jsou samoduální. Odtud je $|\varrho(w_k) - q_1|$ pro $k \leq 4$ dělitelné třemi, a proto se musejí nosiče $\varrho(w_k), q_1$ protínat v alespoň jednom bodě. Protože jsou nosiče $\varrho(w_k)$ disjunktní, musí nosič q_1 protínat každý právě jednou.

Opět ze samoduality platí $(q_1 - p) \cdot (q_1 - p) = 0$, a tedy q_1 má na společné nenulové souřadnici s p hodnotu 2. Protože každá nenulová souřadnice q_1 je společná s nějakým prvkem $\mathcal{S}$, jsou všechny nenulové souřadnice q_1 rovny 2.

Navíc $(q_1 - q_2) \cdot (q_1 - q_2) = 0$, a tedy se nosiče q_1, q_2 shodují, a tedy protínají, právě v jednom bodě. Tímto jsou dokázány první dva body.

K třetímu bodu zbývá dokázat, že dvěma souřadnicemi n, m z nosičů různých prvků $\mathcal{S}$ prochází nosič alespoň jednoho prvku $2\mathcal{P}$. Bez újmy na obecnosti předpokládejme $m \in \mathrm{supp}(p)$. Souřadnicí n procházejí 3 nosiče prvků $2\mathcal{P}$. Kdyby žádný z nich neprocházel souřadnicí m, existuje souřadnice $k \in \mathrm{supp}(p)$, kterou procházejí dva z těchto tří nosičů. To je ale spor s jednoznačností průniku dvou nosičů.

Konečně $[\mathcal{S} \cup 2\mathcal{P}] = \varrho(L+r)$ lze snadno ukázat spočtením $|[\mathcal{S} \cup 2\mathcal{P}]|$.

□

[8] Protože každé propíchnutí dá 3 slova váhy 4, dává jednoznačnost v předchozí větě odstavce $9 = \frac{12 \cdot 3}{4}$ slov.

4. Golayovy kódy a grupa Mathieu M_{12}

V této kapitole popíšeme vlastní konstrukci grupy M_{12} založenou na projektivní rovině řádu 3 a Golayových kódech. Tato konstrukce staví na práci [3]. Jiné možné přístupy lze nalézt například v [9], [10], [11].

Věta 4.1 (Hlavní věta: tvar $\mathrm{Aut}(L)$)**.** *K* $\mathrm{Aut}(L)$ *existuje* $a \in \mathrm{Aut}(L)$ *řádu* 2*, pro které* $M \coloneqq \mathrm{Aut}(L)/(a) \cong M_{12}$*.*

Prvním krokem v důkazu této věty bude nalezení vhodného homomorfismu φ, jehož jádro bude generované vhodným prvkem a. Poté z první věty o izomorfismu máme $M \cong \varphi(L)$[9].

Hledaným homomorfismem bude projekce do S_{12}. Každý monomiální automorfismus g dává permutací souřadnic π, ze které se skládá. Položíme $\varphi(g) = \pi$. Toto je dobře definovaný homomorfismus $\mathrm{Aut}(L) \to S_{12}$.

Pro $H \subseteq \mathrm{Aut}(L), g \in \mathrm{Aut}(L)$ značíme $\overline{H} \coloneqq \varphi(H), \overline{g} \coloneqq \varphi(g)$.

Lemma 4.2 (o jádru φ)**.** $\mathrm{Ker}(\varphi) = \{\mathrm{id}, m\}$*, kde* m *je automorfismus daný maticí* $-I$ *a* I *značí jednotkovou matici řádu* 12*.*

Důkaz. Zřejmě $\{\mathrm{id}, m\} \subseteq \mathrm{Ker}(\varphi)$.

Ať $g \in \mathrm{Ker}(\varphi) \setminus \{\mathrm{id}, m\}$. Pak g nepermutuje souřadnice (působí identicky) a existují indexy i, j, že g mění znaménko[10] souřadnice i a zachovává souřadnici j. Díky lemmatu 3.26 obsahuje kód L slovo c váhy 6, že $i, j \in \mathrm{supp}(c)$. Ale pro $d \coloneqq g(c) - c \in L$ platí $i \in \mathrm{supp}(c), j \notin \mathrm{supp}(c)$, tedy $1 \leq |d| \leq 5$, což je spor. □

4.1 Řád M

Dalším důležitým krokem v důkazu věty 4.1 je určení řádu M. K tomu využijeme lemmatu 1.3 o vztahu orbity a stabilizátoru.

Konkrétně uvážíme přirozené působení M jakožto permutační grupy na tříprvkových množinách souřadnic. Označíme $H \leqslant \mathrm{Aut}(L)$ největší podgrupu, že $\overline{H}$ je stabilizátor množiny nenulových pozic s. Tuto množinu budeme dále značit $\mathcal{K}$. Množinu zbylých souřadnic značíme $\mathcal{J}$.

Lemma 3.26 dává tranzitivitu tohoto působení a tedy

$$|M| = |M_{\mathcal{K}}| \cdot |M(\mathcal{K})| = |\overline{H}| \binom{12}{3}. \tag{4.1}$$

Zbývá tedy určit řád $\overline{H}$. K tomu si snadno uvědomíme, že $|\mathrm{AGL}(2,3)| = |T| \cdot |\mathrm{GL}(2,3)| = |\mathbb{F}_3^2| \cdot (3^2 - 1) \cdot (3^2 - 3) = 9 \cdot 8 \cdot 6$, kde T je grupa translací z definice 3.4, a stačí dokázat $\overline{H} \cong \mathrm{AGL}(2,3)$.

Začneme formulací a důkazem technického lemmatu, které nám pomůže vnořit $\overline{H}$ do $\mathrm{AGL}(2,3)$.

[9] Tyto grupy budeme ztotožňovat, tj. budeme určovat vlastnosti $\varphi(L)$.

[10] Pokládáme $-1 = 2$.

Lemma 4.3 (afinní rovina nad $\mathcal{J}$)**.** *Slova c kódu L váhy 6, pro které $\mathcal{K} \subseteq \mathrm{supp}(c)$, odpovídají přímkám afinní roviny (řádu 3), jejíž množina bodů je $\mathcal{J}$.*

Důkaz. Označme

$$\widetilde{A} \coloneqq \{c + s \mid c \in L, |c| = 6, \mathcal{K} \subseteq \mathrm{supp}(c)\}.$$

Potom platí $\widetilde{A} \subseteq [A]$ a jsou to právě slova $[A]$, která mají 0 nebo 2 na souřadnicích $\mathcal{K}$ a právě tři nenulové souřadnice $\mathcal{J}$.

Zřejmě platí $A \setminus \{s\} \subseteq \widetilde{A}$. Uvážíme množiny $\mathrm{supp}_{\mathcal{J}}(a) \coloneqq \mathrm{supp}(a) \cap \mathcal{J}$ pro $a \in A \setminus \{s\}$. Chápeme-li je jako množiny bodů $\mathcal{J}$, dostáváme tak díky lemmatu 3.11 afinní přímky z definice afinní roviny 3.1.

Ukážeme, že $\widetilde{A}$ nedá další podmnožiny $\mathcal{J}$. Tedy, že neexistuje $c \in L, |c| = 6$, $\mathcal{K} \subseteq \mathrm{supp}(c)$, pro které $\mathrm{supp}_{\mathcal{J}}(c)$ neodpovídá afinní přímce.

Zvolme takové c. Uvažme dvě nenulové pozice c v $\mathcal{J}$. Tyto jsou spojeny afinní přímkou, která je z předpokladu různá od $\mathrm{supp}_{\mathcal{J}}(c)$. Této afinní přímce odpovídá projektivní přímka $p \in A \setminus \{s\}$. Proto existuje $d \in L$ váhy 6, jehož nosič se shoduje s nosičem c na pozicích $\mathcal{K}$ a na právě dvou pozicích $\mathcal{J}$. Potom ale $|d - c| \leq 5$ nebo $|d + c| \leq 5$ a z minimální vzdálenosti kódu L máme $c = d$ nebo $c = -d$, což je spor.

Celkem máme surjektivní zobrazení z množiny slov kódu L váhy 6, pro které $\mathcal{K} \subseteq \mathrm{supp}(c)$, na afinní přímky nad $\mathcal{J}$.

□

Lemma 4.4 (vnoření $\overline{H}$)**.** *Existuje vnoření $\overline{H} \hookrightarrow \mathrm{AGL}(2, 3)$.*

Důkaz. Protože H zachovává množinu slov z lemmatu 4.3, zachovává $\overline{H}$ v působení na $\mathcal{J}$ (se strukturou afinní roviny) afinní přímky. Díky lemmatu 3.6 je tedy působení $\overline{H}$ na $\mathcal{J}$ podgrupou $\mathrm{AGL}(2, 3)$.

Ukážeme navíc, že pro $h \in \overline{H}$ odpovídá rozšíření tohoto působení na projektivní rovinu působení h na dvanáctiprvkové množině souřadnic[11].

Zvolme $i \in \mathcal{K}$ a uvažme vektor s_i, který z s vznikne přičtením 1 k souřadnici i. K s_i uvážíme v_{ij} z lemmatu 3.25. Z jednoznačnosti v tomto lemmatu máme $v_{i4} = 0, v_{ij} = p_{ij} - s, p_{ij} \in P$ pro $j \leq 3$. Tato p_{ij} jsou z definice incidenční vektory projektivních přímek, které navíc procházejí bodem i.

Pro $g \in H$ takové, že $\overline{g} = h$ víme, že g permutuje slova $v_{ij}, i \in \mathcal{K}, j \leq 3$. Proto h permutuje souřadnice $\mathcal{K}$ způsobem odpovídajícím permutaci tříd rovnoběžnosti afinních přímek.

□

Lemma 4.5 (dolní odhad $|H|$)**.** *Platí odhad $|H| \geq 9 \cdot 8 \cdot 6 \cdot 2$.*

Důkaz. Uvažme normální podgrupu translací grupy $\mathrm{AGL}(2, 3)$. Tyto lze rozšířit na projektivní automorfismy zachováním bodů v nekonečnu, což při vnoření do S_{12} odpovídá zachování souřadnic $\mathcal{K}$. Navíc v tomto vnoření zachovává množiny

[11] Kde $\mathcal{J}$ chápeme jako afinní body a $\mathcal{K} \cup \{\infty\}$ jako body v nekonečnu.

S a P. Uvažujeme-li translace jako monomiální zobrazení, je grupa translací tedy (normální) podgrupou H. Takových translací je $3^2 = 9$.

Konečně $m\colon (a, b) \mapsto (2a, 2b)$ je afinní zobrazení zachovávající každou třídu rovnoběžnosti a tedy jeho rozšíření na projektivní automorfismus zachovává každý bod v nekonečnu. Opět jako monomiální zobrazení dává prvek H.

Uvažme podgrupu H řádu 18 generovanou translacemi a zobrazením m. Z lemmatu 3.26 můžeme každé monomiální zobrazení na $\mathcal{K}$ rozšířit na prvek H. Takových zobrazení je $2^3 \cdot 3! = 8 \cdot 6$ a každá dvě leží v různých rozkladových třídách této podgrupy, protože její prvky působí identicky na $\mathcal{K}$. Odtud máme $|H| \geq 9 \cdot 8 \cdot 6 \cdot 2$. □

Kombinací předchozích dvou lemmat získáváme požadovaný izomorfismus.

Důsledek 4.6 (tvar $\overline{H}$)**.** *Platí* $|\overline{H}| \geq 9 \cdot 8 \cdot 6$ *a tedy* $\overline{H} \cong \mathrm{AGL}(2, 3)$.

Nyní už lze snadno spočítat řád grupy M.

Lemma 4.7 (řád M)**.** $|M| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$.

Důkaz. Dosazením $|\overline{H}| = 9 \cdot 8 \cdot 6$ do rovnosti 4.1 dostáváme

$$|M| = 9 \cdot 8 \cdot 6 \cdot 12 \cdot 11 \cdot 10/(3 \cdot 2) = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8.$$

□

4.2 Tranzitivita M a hlavní věta

Díky klasifikaci vysoce tranzitivních grup z věty 1.4 zbývá už jen určit tranzitivitu H. To uděláme v rámci důkazu hlavní věty 4.1.

Věta (Hlavní věta: tvar $\mathrm{Aut}(L)$)**.** *K* $\mathrm{Aut}(L)$ *existuje* $a \in \mathrm{Aut}(L)$ *řádu* 2*, pro které* $M \coloneqq \mathrm{Aut}(L)/(a) \cong M_{12}$.

Důkaz. Položíme $a = m$ z lemmatu 4.2. Potom $|\mathrm{Aut}(L)/(a)| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ díky lemmatu 4.7.

Ukážeme, že M je 5-tranzitivní grupa. Potom díky větě 1.4 a znalosti řádu M dostaneme $M \cong M_{12}$. K tomu uvážíme věrné působení M na dvanáctibodové množině dané vnořením $M \hookrightarrow S_{12}$. Z definice tranzitivity grupy stačí ukázat, že toto působení je 5-tranzitivní.

Nejprve ukážeme, že jediný prvek M zachovávající 5 souřadnic je identita. Ať g je takový prvek. Pomocí konjugace zobrazením z lemmatu 3.26 můžeme předpokládat, že 3 ze zachovaných souřadnic jsou právě prvky $\mathcal{K}$. Speciálně je tedy $g \in \overline{H}$ a můžeme uvážit působení g na projektivní rovinu jako v lemmatu 4.4.

Protože g zachovává prvky $\mathcal{K}$, dané projektivní působení zachovává každý bod v nekonečnu. Navíc g působí identicky na dvou bodech mimo přímku v nekonečnu a tedy zachovává všechny přímky. Takové zobrazení je zřejmě identitou na projektivní rovině.

Konečně dvě různá rozšíření $(x_1,...,x_5) \mapsto (y_1,...,y_5)$ na prvek M dají neidentické rozšíření $(x_1,...,x_5) \mapsto (x_1,...,x_5)$. Proto pro libovolné dvě pětice existuje nejvýše jedno takové rozšíření. Ale $|M| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ a tedy každé takové zobrazení musí jít rozšířit na prvek M.

M je proto 5-tranzitivní grupa řádu $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ a jako taková je díky 1.4 izomorfní M_{12}.

□

Přímým důsledkem hlavní věty a jednoznačnosti Golayových kódů (3.20) je známá charakterizace grupy M_{12}.

Důsledek 4.8. *Ať G je rozšířený ternární Golayův kód. Pak existuje $a \in \mathrm{Aut}(G)$ řádu 2, pro které $\mathrm{Aut}(G)/(a) \cong M_{12}$.*

Závěr

Hlavním cílem práce bylo srovnání konstrukcí grupy M_{12}. Míchací grupy daly M_{12} jako obraz $\mathrm{Sh}(S_2, 12)$ při homomorfismu, který odpovídal zapomenutí „znamének“ dvojic protějších karet. To bylo umožněno pozorováním, že $\mathrm{Sh}(S_2, 12)$ tyto dvojice zachovává. Přímým ověřením řádu a 2-tranzitivity tohoto obrazu lze s využitím klasifikace vysoce tranzitivních grup snadno ukázat, že jde o požadovanou grupu.

Na druhou stranu naše originální konstrukce pomocí Golayových kódů nad projektivní rovinou dala M_{12} jako obraz $\mathrm{Aut}(L)$ při homomorfismu, který odpovídal zapomenutí znamének monomiálních transformací. Konstruktivním ověřením řádu a 5-tranzitivity tohoto obrazu bylo opět s využitím klasifikace vysoce tranzitivních grup ukázáno, že jde o požadovanou grupu.

Na první pohled je mezi těmito postupy řada paralel. Tou pravděpodobně nejzajímavější je, že v obou případech je Mathieuova grupa obrazem podgrupy B_{12} (grupa matic nad $\mathbb{F}_3$ s právě jedním nenulovým prvkem v každém řádku i sloupci)[12] při homomorfismu $B_{12} \to S_{12}$ odpovídajícímu zapomenutí znamének. Bohužel výchozí grupy $\mathrm{Sh}(S_2, 12)$ a $\mathrm{Aut}(L)$ jsou různých řádů a jsou popsány zásadně odlišnými způsoby — jedna pomocí generátorů a druhá konstrukcí. To samé platí pro jejich obrazy a navíc není jasné, jak generátory popsané ve větě 2.11 působí v kontextu našich Golayových kódů. Z tohoto důvodu nebyla nalezena přímá korespondence mezi těmito konstrukcemi[13].

Hlavním přínosem této práce je tedy především nový a kompletní důkaz známé věty 4.8 o M_{12} jako faktoru grupy automorfismů rozšířeného ternárního Golayova kódu.

[12] Tato grupa odpovídá monomiálním transformacím nad $\mathbb{F}_3$.

[13] Což samozřejmě nevylučuje její exitenci.

Seznam použité literatury

[1] Persi Diaconis, RL Graham, and William M Kantor. The mathematics of perfect shuffles. *Advances in applied mathematics*, 4(2):175–196, 1983.

[2] Cheryl E Praeger Carmen Amarra, Luke Morgan. Generalised shuffle groups. 2019.

[3] Aleš Drápal. Yet another approach to the extended ternary golay code. *Discrete mathematics*, 256(1-2):459–464, 2002.

[4] Arjeh M Cohen and H Zantema. A computation concerning doubly transitive permutation groups. 1984.

[5] Peter J Cameron. Finite permutation groups and finite simple groups. *Bulletin of the London Mathematical Society*, 13(1):1–22, 1981.

[6] Charles C Sims. Computational methods in the study of permutation groups. In *Computational problems in abstract algebra*, pages 169–183. Elsevier, 1970.

[7] Steve Medvedoff, Kent Morrison, and Aldous Huxley. Groups of perfect shuffles. *Mathematics Magazine*, 60(1):3–14, 1987.

[8] John Horton Conway and Neil James Alexander Sloane. *Sphere packings, lattices and groups*, volume 290. Springer Science & Business Media, 2013.

[9] Andries E Brouwer. The witt designs, golay codes and mathieu groups. *Unpublished notes, https://www. win. tue. nl/˜ aeb/2WF02/Witt. pdf*, 1982.

[10] Maro Kimizuka, Ryuji Sasaki, et al. m-matrices of the ternary golay code and the mathieu group $m\_\{12\}$. *Tokyo Journal of Mathematics*, 31(1):111–125, 2008.

[11] Jeremy L Martin. The mathieu group m12 and conway's m13-game. 1996.