UNIVERZITA KOMENSKÉHO V BRATISLAVE FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY



GRUPY AUTOMORFIZMOV LINEÁRNYCH KÓDOV

Diplomová práca

2022 Bc. Branislav Boráň

UNIVERZITA KOMENSKÉHO V BRATISLAVE FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY



GRUPY AUTOMORFIZMOV LINEÁRNYCH KÓDOV

Diplomová práca

Študijný program: Aplikovaná informatika

Študijný odbor: 2511 Aplikovaná informatika Školiace pracovisko: Katedra algebry a geometrie

Školiteľ: doc. RNDr. Róbert Jajcay, DrSc.

Bratislava, 2022

Bc. Branislav Boráň





Univerzita Komenského v Bratislave Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta:

Branislav Boráň

Študijný program:

aplikovaná informatika (Jednoodborové štúdium,

magisterský II. st., denná forma)

Študijný odbor:

informatika

Typ záverečnej práce:

diplomová anglický

Jazyk záverečnej práce: Sekundárny jazyk:

slovenský

Názov:

Automorphism groups of linear codes and linear codes with prescribed

automorphism groups

Grupy automorfizmov lineárnych kódov a lineárne kódy s predpísanou grupou

automorfizmov

Anotácia:

Lineárne kódy sú podpriestory konečnorozmerných vektorových priestorov nad konečnými poľami. Majú preto bohaté grupy automorfizmov, ktoré zároveň obsahujú množstvo informácií o uvažovanom kóde. Určenie úplnej grupy automorfizmov kódu je výpočtovo náročná úloha. Namiesto určenia grupy automorfizmov pre daný kód sa preto uvažuje obrátená úloha zostrojenia kódu s predpísanou grupou automorfizmov. Cieľom práce je preskúmať oba smery

tejto interakcie.

Ciel':

Cieľom navrhovanej problematiky je poskytnúť študentovi výpočtovo zložitý problém vyžadujúci dôkladné porozumenie štruktúry uvažovaných objektov

ako aj programátorské a organizačné schopnosti.

Literatúra:

R. Hill, A first course in coding theory, Oxford University Press, 1993

S. Roman, Coding and information theory, Springer, 1992

R. Jajcay, P. Potocnik and Stephen E. Wilson, Half-cyclic, dihedral and half-

dihedral codes.

J. of Applied Mathematics and Computing 64 (2020), 691-708.

Kľúčové

slová:

lineárny kód, grupa automorfizmov, konečné pole

Vedúci:

doc. RNDr. Róbert Jajcay, DrSc.

Katedra:

FMFI.KAG - Katedra algebry a geometrie

Vedúci katedry:

doc. RNDr. Pavel Chalmovianský, PhD.

Dátum zadania:

09.12.2020

Dátum schválenia: 10.12.2020

prof. RNDr. Roman Ďurikovič, PhD.

garant študijného programu

študent	vedúci práce

•	
1	V

Čestne prehlasujem, že túto diplomovú prácu som vypracoval samostatne len s použitím uvedenej literatúry a za pomoci konzultácií u môjho školiteľa.

•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•

Bratislava, 2022

Bc. Branislav Boráň

Poďakovanie

Chcel by som sa v prvom rade poďakovať môjmu školiteľovi doc. RNDr. Róbertovi Jajcayovi, DrSc. za odbornú pomoc a usmernenia pri písaní tejto práce, za materiály, cenné rady, ktoré mi veľmi pomohli pri riešení tejto diplomovej práce. V neposlednom rade chcem tiež poďakovať všetkým mojím kamarátom a celej mojej rodine za podporu počas môjho štúdia.

Abstrakt

Táto práca sa venuje problematike xxxxxxxxx. Súčasťou tejto práce je prehľad existujúcich riešení a ich krátke zhodnotenie. Ďalej je tu xxxxx. Čo sa tu rieši.

Kľúčové slová: automorfizmus grúp,

Abstract

english abstract

Keywords: Automorphism groups, \dots

Obsah

1	Úvo	od		1									
2	Motivácia												
3	Analýza problému												
	3.1	Lineái	rny kód	3									
		3.1.1	Generujúca matica lineárneho kódu	4									
		3.1.2	Kontrolná matica lineárneho kódu	4									
		3.1.3	LDPC kódy	4									
		3.1.4	Kvázicyklický kód	5									
	3.2	Grafo	vá reprezentácia LDPC kódov	5									
		3.2.1	Základné pojmy	6									
		3.2.2	Moorové grafy	7									
		3.2.3	Klietky	7									
		3.2.4	Automorfizmus grafu	11									
4	Náv	rh rie	šenia	12									
	4.1	Gener	ovanie Incidenčných matíc zo známych klietok a grupy										
		autom	norfizmov	12									
		4.1.1	Petersenov graf - $cage(3,5)$	13									
		4.1.2	Heawoodov graf - $cage(3,6)$	15									

ΟE	BSAF	I		ix
		4.1.3	McGeeho graf - $cage(3,7)$	17
		4.1.4	Tutte - Coxeterov graf - $cage(3,8)$	19
		4.1.5	Balabanov graf - $cage(3, 10)$	21
		4.1.6	Robertsonov graf - $cage(4,5)$	25
		4.1.7	Hoffman - Singletonov graf - $cage(7,5)$	28
	4.2	Gener	ovanie klietok a ich Incidenčných matíc spolu s grupami	
		auton	norfizmov	33
		4.2.1	cage(6,4)	33
5	Záv	er		36

$\mathbf{\acute{U}vod}$

XXXXXX

Motivácia

XXXXXX

Analýza problému

V tejto kapitole si popíšeme pojmy a problematiku, ktorú treba riešiť pri návrhu a implementácii xxxxx.

Problematiku tejto témy môžeme rozdeliť na 2 logické časti: Lineárny kód a grafovú reprezentáciu LDPC kódov.

3.1 Lineárny kód

Lineárny kód (n,k) je k-rozmerný lineárny podpriestor priestoru F_n^2 . F_n^2 je priestor n-rozmerných vektorov, kde koordináty berieme z poľa F^2 . k-rozmerný lineárny podpriestor obsahuje práve k lineárne nezávislých vektorov. Ak by sme zobrali k takých vektorov, potom tieto vektory generujú daný k-rozmerný podpriestor a hovoríme, že tvoria bázu podpriestoru. Ak je splnená vlastnosť modulo 2 (q) súčtu 2 kódových slov je kódové slovo, tak vieme nájsť Generačnú maticu lineárneho kódu.

3.1.1 Generujúca matica lineárneho kódu

Generujúca matica lineárneho kódu (G) je zostrojená z bázy lineárneho kódu tak, že riadky matice predstavujú prvky bázy. Riadky generujúcej matice sú lineárne nezávislé vektory dĺžky n. Nech \vec{m} je vstup (nekódované slovo), \vec{v} je výstup (kódované slovo), C je označenie lineárneho kódu, potom platí:

$$C = \{ \vec{m} \times G : \vec{m} \in F_2^k \}, \quad \vec{v} = \vec{m} \times G$$
(3.1)

3.1.2 Kontrolná matica lineárneho kódu

V k-rozmernom linearnom kóde (C) v F_n^2 potom existuje n-k lineárne nezávislých vektorov \vec{v} takých, že každé kódové slovo je kolmé na všetky tieto vektory. Keď týchto n-k vektorov zoberieme ako riadky matice, dostaneme kontrolnú maticu lineárneho kódu H. Ľubovoľný vektor \vec{v} je kódovým slovom práve vtedy, ak platí:

$$C = \{ \vec{v} \in F_2^n : H \times \vec{v}^T = 0 \}$$
(3.2)

3.1.3 LDPC kódy

LDPC kódy (z angl. low density parity check code) sú lineárne samoopravné kódy, ktoré jednak umožňujú prenos dát rýchlosťou blízkou kapacite kanálu a zároveň pre ne existujú vysoko účinné dekódovacie algoritmy. Kódy majú veľmi riedku kontrolnú maticu, pomocou ktorej sa dajú opraviť chyby v kódových slovách. Ich kontrolná matica obsahuje menej ako 1% jednotiek. Hlavnou nevýhodou väčšiny LDPC kódov je vysoká časová náročnosť ich kódovacieho algoritmu. Výhodou je paralelizmus pri dekódovaní a jednoduché výpočtové operácie. Dekódovacie výpočty sú rozdelené do 2 množín uzlov a

to do kontrolných uzlov a premenných uzlov. Uzol na jednej strane je spojený s uzlom na druhej strane, čo umožňuje paralelné výpočty na každej strane.

3.1.4 Kvázicyklický kód

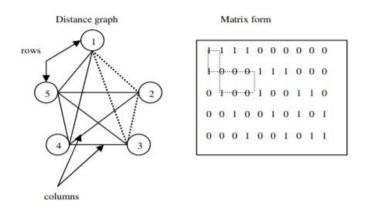
Lineárny kód (C) je kvázicyklický kód, ak existuje kontrolná matica H, ktorá má tvar:

$$H = (H_0|H_1|...|H_{n_0}^{-1}) (3.3)$$

 ${\cal H}_i$ sú cyklické matice. Ak sú LDPC kvázicyklické, nazývame ich QC-LDPC kódy.

3.2 Grafová reprezentácia LDPC kódov

Matica LDPC je reprezentovaná Moorovým grafom. Matica môže byť tiež reprezentovaná bipartitným grafom alebo grafom vzdialenosti, v ktorom riadky matice predstavujú vrcholy a stĺpce matice reprezentujú hrany grafu. Stĺpec je potom množina hrán formujúca kompletný graf medzi vrcholmi spojenými v stĺpci. Nasledujúci obrázok ilustruje grafovú reprezentáciu matice LDPC kódu:



Obr. 3.1: Vztah medzi grafom a maticou [Mal07]

Graf vzdialenosti je formovaný cestami hrán alebo vrcholov Cyklus dĺžky g v grafe korešponduje s cyklom dĺžky 2g v maticovej forme.

3.2.1 Základné pojmy

- Dĺžka kódu špecifikuje dimenzie $(M \times N)$ kontrolnej matice H. M predstavuje počet riadkov matice a N je počet stĺpcov.
- ullet Kódová váha a rate (R) predstavuje počet bitov (informácií) nad celkovým počtom prenesených bitov. Rate možno vyjadriť vzťahom:

$$R = (N - M)/N \tag{3.4}$$

- Kódová štruktúra onzačuje spojenia medzi riadkami a stĺpcami
- Minimálna Hammingová (kódová) vzdialenosť $minHW(\vec{u}, \vec{v})$ Nech sú vektory \vec{u} a \vec{v} kódové slová. Minimálna Hammingová vzdialenosť 2 vektorov $\vec{u} \in F_n^2$ a $\vec{v} \in F_n^2$ je počet koordinátov, na ktorých sa vektory \vec{u} a \vec{v} líšia.

• Obvod (g) - ovplyvňuje dekódovanie LDPC kódu. V grafovej reprezentácií LDPC kódu sa jedná o najmenší cyklus v grafe. Jeho dĺžku zrátavame iba pomocou vrcholov alebo hrán. V matici LDPC kódu je dĺžka obvodu 2g, pretože cyklus alternuje medzi riadkami a stĺpcami z čoho vyplýva, že cyklus grafu reprezentuje iba polovicu maticového kódu.

3.2.2 Moorové grafy

Pravidelný graf stupňa d a parametra k vo forme stromu vyhľadávania do šírky začínajúceho z ľubovoľného vrcholu V, ktorého počet vrcholov vieme dostať ako:

$$1 + d\sum_{i=0}^{k-1} (d-1)^i \tag{3.5}$$

3.2.3 Klietky

Klietka cage(k,g) je k-pravidelný graf obvodu g s najmenším možným počtom vrcholov m. Výpočet minimálneho počtu vrcholov pre klietku sa líši podľa toho, či je jej obvod párny alebo nepárny:

• q - nepárne:

$$m = 1 + \sum_{i=0}^{(g-3)/2} k(k-1)^i = \frac{k(k-1)^{(g-1)/2} - 2}{k-2}$$
 (3.6)

• g - párne:

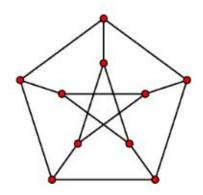
$$m = 2\sum_{i=0}^{(g-2)/2} k(k-1)^i = \frac{2(k-1)^{g/2} - 2}{k-2}$$
(3.7)

Klietka môže byť aj Moorov graf, pre ktorý platí:

$$d = k \tag{3.8}$$

Môžeme vypočítať najnižší počet vrcholov minimálneho stupňa k a jeho obvodu g. Aj keď neexistuje jednotná konštrukcia klietok, existuje niekoľko známych klietok pre stupeň vrchola k a obvod g. Ukážeme si niektoré z nich.

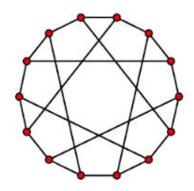
• Petersenov graf - cage(3, 5):



Obr. 3.2: Petersenov graf [EJ11]

Petersenov graf má rád 10.

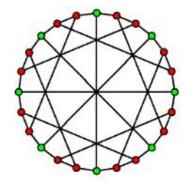
• Heawoodov graf - cage(3,6):



Obr. 3.3: Heawoodov graf [EJ11]

Heawoodov graf má rád 14 a počet grúp automorfizmov je 336.

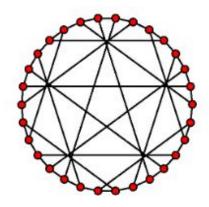
• McGeeho graf - cage(3,7):



Obr. 3.4: McGeeho graf [EJ11]

McGeeho graf má rád 24 a počet grúp automorfizmov je 32.

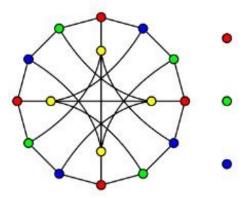
• Tutte-Coxeterov graf - cage(3, 8):



Obr. 3.5: Tutte-Coxeterov graf [EJ11]

Tutte-Coxterov graf má rád 30 a počet grúp automorfizmov je 1440.

- \bullet Balabanov graf cage(3,11): Balabanov graf má 112 vrcholov a počet grúp automorfizmov je 64.
- \bullet Bensonov graf cage(3,12): Bensonov graf má 126 vrcholov a počet grúp automorfizmov je 12096.
- Robertsonov graf cage(4, 5):



Obr. 3.6: Robertsonov graf [EJ11]

• ďalšie známe klitky: cage(4,7) - Exoo, McKay, a Nadonov graf, cages(5,5): počet grúp automorfizmov je 20,30 a 120, cage(7,5) - Hoffman - Singletonov graf, cage(7,6) - O'Keefe a Wongov graf

3.2.4 Automorfizmus grafu

Automorfizmus grafu je permutácia \varnothing všetkých vrcholov grafu, ktorá zachováva jeho štruktúru takým spôsobom, že akékoľvek 2 vrcholy U a V susedia iba vtedy a len vtedy ak platí:

$$\emptyset(U)V$$
 (3.9)

Jedná sa o bijektívne zobrazenie, pri ktorom sa každý vrchol grafu a každá hrana zobrazí na iný vrchol a hranu, hovoríme tiež, že ide o jeho obraz. Množina všetkých automorfizmov grafu G tvorí grupu automorfizmov Aut(G). Moorové grafy majú grupu automorfizmov, ktoré prechodne pôsobia na množinu vrcholov grafu.

Návrh riešenia

Problematiku riešime v programe Sage [sag], ktorý je založený na programovacom jazyku Python. Zvolili sme ho, pretože ponúka veľké množstvo vopred naimplementovaných funkcií, ktoré nám podstatne uľahčia prácu s grafmi, maticami a grupami automorfizmov. Využili sme online aplikáciu CoCalc [coc], ktorá nám umožňuje vytvárať Sage projekty priamo na internete. CoCalc prevádzkuje prostredie Ubuntu Linux, s ktorým je možné komunikovať cez terminál a taktiež poskytuje prístup k ďalším možnostiam Linuxu.

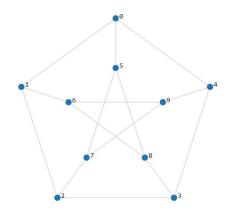
4.1 Generovanie Incidenčných matíc zo známych klietok a grupy automorfizmov

Uvažujeme známe klietky a na základe nich vygenerujeme incidenčnú maticu a zistíme grupu automorfizmov. Na základe výpočtov nezávislých od toho, či klietku vieme zostrojiť alebo je známa vieme pre danú klietku zistiť minimálny počet vrcholov, rozmer minimálnej matice kódu, obvod cyklu v matici a minimálny počet hrán. Na základe výpočtov nezávislých od toho, či klietku vieme zostrojiť alebo je známa vieme pre danú klietku zistiť minimálny počet

13

vrcholov, rozmer minimálnej matice kódu, obvod cyklu v matici a minimálny počet hrán.

4.1.1 Petersenov graf - cage(3,5)



Obr. 4.1: Petersenov graf 2D [coc]



Obr. 4.2: Petersenov graf 3D [coc]

• minimálny počet vrcholov: 10

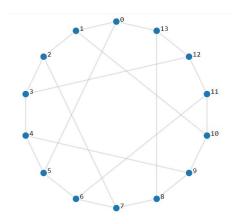
 $\bullet\,$ rozmer minimálnej matice kódu: $10\times15\,$

- obvod cyklu v matici: 10
- minimálny počet hrán: 15
- cykly v grafe: 6 cyklov [[1, 6, 8, 5, 0], [4, 9, 6, 8, 5, 0], [7, 9, 6, 8, 5], [4, 3, 8, 5, 0], [1, 2, 3, 8, 5, 0], [7, 2, 3, 8, 5]]
- hrany v grafe: 15 hrán $[(0,1,None),(0,4,None),(0,5,None),(1,2,None),(1,6,None),(2,3,None),\\(2,7,None),(3,4,None),(3,8,None),(4,9,None),(5,7,None),(5,8,None),\\(6,8,None),(6,9,None),(7,9,None)]$
- počet grúp automorfizmov: 120
- matica lineárneho kódu:

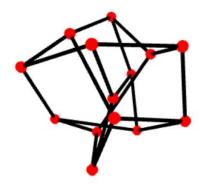
Obr. 4.3: Matica Petersenovho grafu [coc]

15

4.1.2 Heawoodov graf - cage(3,6)



Obr. 4.4: Heawoodov graf 2D [coc]



Obr. 4.5: Heawoodov graf 3D [coc]

• minimálny počet vrcholov: 14

 $\bullet\,$ rozmer minimálnej matice kódu: $14\times21\,$

• obvod cyklu v matici: 12

• minimálny počet hrán: 21

cykly v grafe: 8 cyklov
[[1, 10, 11, 12, 13, 0], [8, 9, 10, 11, 12, 13], [3, 4, 9, 10, 11, 12],
[5, 4, 9, 10, 11, 12, 13, 0], [5, 6, 11, 12, 13, 0], [8, 7, 6, 11, 12, 13],

• hrany v grafe: 21 hrán

[1, 2, 7, 6, 11, 12, 13, 0], [3, 2, 7, 6, 11, 12]]

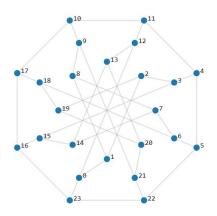
$$[(0,1,None),(0,5,None),(0,13,None),(1,2,None),(1,10,None),(2,3,None),\\(2,7,None),(3,4,None),(3,12,None),(4,5,None),(4,9,None),(5,6,None),\\(6,7,None),(6,11,None),(7,8,None),(8,9,None),(8,13,None),\\(9,10,None),(10,11,None),(11,12,None),(12,13,None)]$$

- počet grúp automorfizmov: 336
- matica lineárneho kódu:

Obr. 4.6: Matica Heawoodovho grafu [coc]

17

4.1.3 McGeeho graf - cage(3,7)



Obr. 4.7: McGeeho graf 2D [coc]



Obr. 4.8: McGeeho graf 3D [coc]

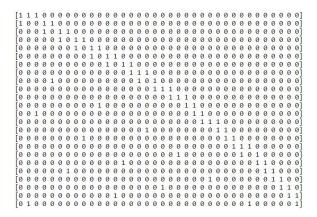
 $\bullet\,$ minimálny počet vrcholov: 22

 $\bullet\,$ rozmer minimálnej matice kódu: $22\times33\,$

• obvod cyklu v matici: 14

• minimálny počet hrán: 33

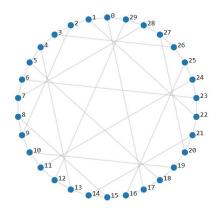
- cykly v grafe: 13 cyklov $[[23,16,15,14,13,12,0],[20,19,18,17,16,15,14,13],[1,2,19,18,17,16,\\ 15,14,13,12,0],[3,2,19,18,17,16,15],[7,6,18,17,16,15,14],[23,22,5,6,18,17,16],\\ [20,21,22,5,6,18,17,16,15,14,13],[10,9,21,22,5,6,18,17],\\ [1,8,9,21,22,5,6,18,17,16,15,14,13,12,0],[7,8,9,21,22,5,6],[3,4,5,6,\\ 18,17,16,15],[11,4,5,6,18,17,16,15,14,13,12],[11,10,17,16,15,14,13,12]]$
- hrany v grafe: 36 hrán
 [(0,1,None), (0,12,None), (0,23,None), (1,2,None), (1,8,None), (2,3,None),
 (2,19,None), (3,4,None), (3,15,None), (4,5,None), (4,11,None), (5,6,None),
 (5,22,None), (6,7,None), (6,18,None), (7,8,None), (7,14,None), (8,9,None),
 (9,10,None), (9,21,None), (10,11,None), (10,17,None), (11,12,None),
 (12,13,None), (13,14,None), (13,20,None), (14,15,None), (15,16,None),
 (16,17,None), (16,23,None), (17,18,None), (18,19,None), (19,20,None),
 (20,21,None), (21,22,None), (22,23,None)]
- počet grúp automorfizmov: 32
- matica lineárneho kódu:



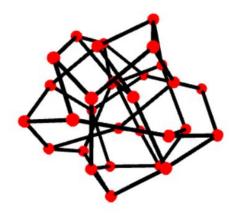
Obr. 4.9: Matica McGeeho grafu [coc]

19

4.1.4 Tutte - Coxeterov graf - cage(3,8)



Obr. 4.10: Tutte-Coxeterov graf 2D [coc]



Obr. 4.11: Tutte-Coxeterov graf 3D [coc]

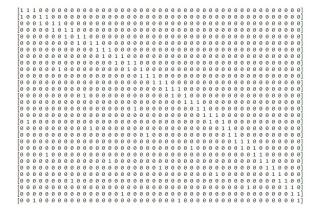
 $\bullet\,$ minimálny počet vrcholov: 30

 $\bullet\,$ rozmer minimálnej matice kódu: $30\times45\,$

• obvod cyklu v matici: 16

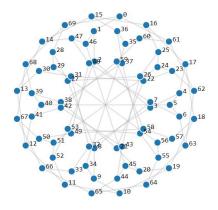
• minimálny počet hrán: 45

- cykly v grafe: 16 cyklov $[[1,22,23,24,25,26,27,28,29,0],[20,21,22,23,24,25,26,27],[16,15,14,21,22,23,24,25],[7,8,15,14,21,22,23,24,25,26,27,28],[11,10,9,8,15,14,21,22,23,24], \\ [20,19,10,9,8,15,14,21],[17,18,19,10,9,8,15,14,21,22,23,24,25,26,27,28,29,0], \\ [6,5,18,19,10,9,8,15,14,21,22,23],[3,4,5,18,19,10,9,8,15,14,21,22,23,24,25,26], \\ [13,4,5,18,19,10,9,8,15,14],[1,2,9,8,15,14,21,22], \\ [3,2,9,8,15,14,21,22,23,24,25,26],[12,13,14,21,22,23,24,25,26,27,28,29], \\ [7,6,23,24,25,26,27,28],[12,11,24,25,26,27,28,29],[17,16,25,26,27,28,29,0]]$
- hrany v grafe: 45 hrán
 [(0,1, None), (0,17, None), (0,29, None), (1,2, None), (1,22, None), (2,3, None),
 (2,9, None), (3,4, None), (3,26, None), (4,5, None), (4,13, None), (5,6, None),
 (5,18, None), (6,7, None), (6,23, None), (7,8, None), (7,28, None), (8,9, None),
 (8,15, None), (9,10, None), (10,11, None), (10,19, None),
 (11,12, None), (11,24, None), (12,13, None), (12,29, None),
 (13,14, None), (14,15, None), (14,21, None),
 (15,16, None), (16,17, None), (16,25, None), (17,18, None), (18,19, None),
 (19,20, None), (20,21, None), (20,27, None), (21,22, None), (22,23, None),
 (23,24, None), (24,25, None), (25,26, None), (26,27, None),
 (27,28, None), (28,29, None)]
- počet grúp automorfizmov: 1440
- matica lineárneho kódu:

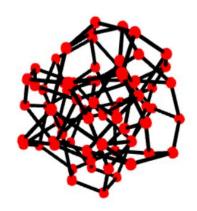


Obr. 4.12: Matica Tutte - Coxeterovho grafu [coc]

4.1.5 Balabanov graf - cage(3, 10)



Obr. 4.13: Balabanov(10) graf 2D [coc]



Obr. 4.14: Balabanov(10) graf 3D [coc]

• minimálny počet vrcholov: 62

• rozmer minimálnej matice kódu: 62 × 93

• obvod cyklu v matici: 20

• minimálny počet hrán: 93

• cykly v grafe: 36 cyklov

[[69, 68, 67, 66, 65, 64, 63, 62, 61, 0], [60, 59, 42, 41, 40, 39, 68, 67, 66, 65, 64, 63, 62, 61],

[55, 56, 57, 58, 59, 42, 41, 40, 39, 68, 67, 66, 65, 64],

[33, 32, 31, 30, 29, 56, 57, 58, 59, 42, 41, 40, 39, 68, 67, 66],

[5, 4, 3, 32, 31, 30, 29, 56, 57, 58, 59, 42, 41, 40],

[18, 17, 4, 3, 32, 31, 30, 29, 56, 57],

[43, 26, 25, 16, 17, 4, 3, 32, 31, 30, 29, 56, 57, 58, 59, 42],

[28, 27, 26, 25, 16, 17, 4, 3, 32, 31, 30, 29],

[12, 11, 10, 9, 8, 27, 26, 25, 16, 17, 4, 3, 32, 31, 30, 29, 56, 57, 58, 59, 42, 41],

[2, 53, 52, 11, 10, 9, 8, 27, 26, 25, 16, 17, 4, 3],

[55, 54, 53, 52, 11, 10, 9, 8, 27, 26, 25, 16, 17, 4, 3, 32, 31, 30, 29, 56],

[38, 37, 54, 53, 52, 11, 10, 9, 8, 27, 26, 25, 16, 17, 4, 3, 32, 31,

[44, 43, 42, 41, 40, 39, 68, 67, 66, 65],

[6, 5, 40, 39, 68, 67, 66, 65, 64, 63]

```
30, 29, 56, 57, 58, 59, 42, 41, 40, 39, [15, 36, 37, 54, 53, 52, 11, 10, 9, 8, 27, 26, 25, 16],
[34, 35, 36, 37, 54, 53, 52, 11, 10, 9],
[60, 35, 36, 37, 54, 53, 52, 11, 10, 9, 8, 27, 26, 25, 16, 17, 4, 3, 32, 31, 30, 29, 56, 57, 58, 59],
[24, 51, 52, 11, 10, 9, 8, 27, 26, 25],
[50, 51, 52, 11, 10, 9, 8, 27, 26, 25, 16, 17, 4, 3, 32,
31, 30, 29, 56, 57, 58, 59, 42, 41, 40, 39, 68, 67, [18, 19, 10, 9, 8, 27, 26, 25, 16, 17],
[44, 45, 20, 19, 10, 9, 8, 27, 26, 25, 16, 17, 4, 3, 32, 31, 30,
29, 56, 57, 58, 59, 42, 41, 40, 39, 68, 67, 66, 65],
[1, 46, 45, 20, 19, 10, 9, 8, 27, 26, 25, 16, 17, 4, 3, 32, 31, 30, 29, 56, 57, 58, 59, 42, 41, 40,
39, 68, 67, 66, 65, 64, 63, 62, 61, 0, [7, 48, 47, 46, 45, 20, 19, 10, 9, 8],
[49, 48, 47, 46, 45, 20, 19, 10, 9, 8, 27, 26, 25, 16, 17, 4, 3, 32, 31, 30, 29, 56, 57, 58],
[13, 14, 47, 46, 45, 20, 19, 10, 9, 8, 27, 26, 25, 16, 17, 4, 3, 32, 31, 30],
[15, 14, 47, 46, 45, 20, 19, 10, 9, 8, 27, 26, 25, 16],
[22, 21, 20, 19, 10, 9, 8, 27, 26, 25, 16, 17, 4, 3, 32, 31],
[38, 21, 20, 19, 10, 9, 8, 27, 26, 25, 16, 17, 4, 3, 32, 31, 30, 29, 56, 57, 58, 59, 42, 41, 40, 39],
[33, 34, 9, 8, 27, 26, 25, 16, 17, 4, 3, 32],
[6, 7, 8, 27, 26, 25, 16, 17, 4, 3, 32, 31,
30, 29, 56, 57, 58, 59, 42, 41, 40, 39, 68, 67, 66, 65, 64, 63],
[23, 24, 25, 16, 17, 4, 3, 32, 31, 30, 29,
56, 57, 58, 59, 42, 41, 40, 39, 68, 67, 66, 65, 64, 63, 62],
[1, 2, 3, 32, 31, 30, 29, 56, 57, 58, 59, 42, 41, 40, 39, 68, 67, 66, 65, 64, 63, 62, 61, 0],
[23, 22, 31, 30, 29, 56, 57, 58, 59, 42, 41, 40, 39, 68, 67, 66, 65, 64, 63, 62],
[12, 13, 30, 29, 56, 57, 58, 59, 42, 41],
[69, 28, 29, 56, 57, 58, 59, 42, 41, 40, 39, 68],
[50, 49, 58, 59, 42, 41, 40, 39, 68, 67],
```

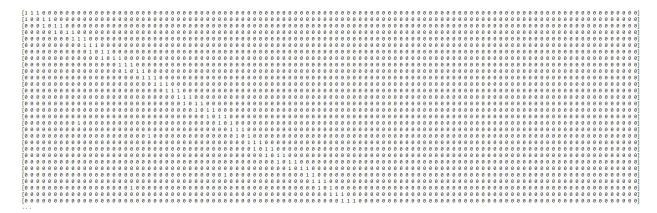
24

```
• hrany v grafe: 105 hrán
  [(0, 1, None), (0, 61, None), (0, 69, None), (1, 2, None), (1, 46, None), (2, 3, None),
  (2, 53, None), (3, 4, None), (3, 32, None), (4, 5, None), (4, 17, None), (5, 6, None),
  (5, 40, None), (6, 7, None), (6, 63, None), (7, 8, None), (7, 48, None), (8, 9, None),
  (8, 27, None), (9, 10, None), (9, 34, None), (10, 11, None), (10, 19, None),
  (11, 12, None), (11, 52, None), (12, 13, None), (12, 41, None), (13, 14, None),
  (13, 30, None), (14, 15, None), (14, 47, None), (15, 16, None), (15, 36, None),
  (16, 17, None), (16, 25, None), (17, 18, None), (18, 19, None), (18, 57, None),
  (19, 20, None), (20, 21, None), (20, 45, None), (21, 22, None), (21, 38, None),
  (22, 23, None), (22, 31, None), (23, 24, None), (23, 62, None), (24, 25, None),
  (24, 51, None), (25, 26, None), (26, 27, None), (26, 43, None), (27, 28, None),
  (28, 29, None), (28, 69, None), (29, 30, None), (29, 56, None), (30, 31, None),
  (31, 32, None), (32, 33, None), (33, 34, None), (33, 66, None), (34, 35, None),
  (35, 36, None), (35, 60, None), (36, 37, None), (37, 38, None), (37, 54, None),
  (38, 39, None), (39, 40, None), (39, 68, None), (40, 41, None), (41, 42, None),
  (42, 43, None), (42, 59, None), (43, 44, None), (44, 45, None), (44, 65, None),
  (45, 46, None), (46, 47, None), (47, 48, None), (48, 49, None), (49, 50, None),
  (49, 58, None), (50, 51, None), (50, 67, None), (51, 52, None), (52, 53, None),
  (53, 54, None), (54, 55, None), (55, 56, None), (55, 64, None), (56, 57, None),
  (57, 58, None), (58, 59, None), (59, 60, None), (60, 61, None), (61, 62, None),
  (62, 63, None), (63, 64, None), (64, 65, None), (65, 66, None), (66, 67, None),
```

• počet grúp automorfizmov: 80

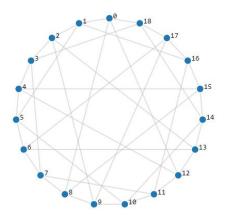
(67, 68, None), (68, 69, None)

• matica lineárneho kódu:

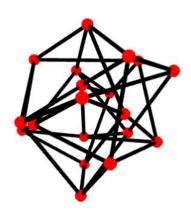


Obr. 4.15: Matica Balabanovho(10) grafu [coc]

4.1.6 Robertsonov graf - cage(4,5)



Obr. 4.16: Robertsonov graf 2D [coc]



Obr. 4.17: Robertsonov graf 3D [coc]

• minimálny počet vrcholov: 17

 $\bullet\,$ rozmer minimálnej matice kódu: 17 × 34

• obvod cyklu v matici: 10

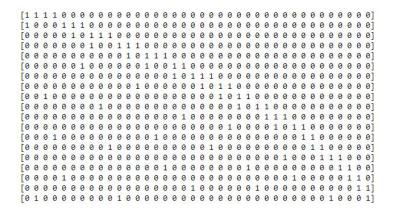
• minimálny počet hrán: 34

cykly v grafe: 20 cyklov
[[18, 14, 13, 12, 0], [4, 15, 14, 13, 12], [8, 15, 14, 13, 12, 0],
[1, 16, 15, 14, 13, 12, 0], [11, 16, 15, 14, 13, 12], [6, 17, 16, 15, 14, 13],
[18, 17, 16, 15, 14], [2, 9, 17, 16, 15, 14, 13], [8, 9, 17, 16, 15],
[10, 9, 17, 16, 15, 14], [11, 10, 14, 13, 12], [1, 5, 10, 14, 13, 12, 0],
[4, 5, 10, 14, 13, 12], [6, 5, 10, 14, 13], [8, 7, 6, 13, 12, 0],
[11, 7, 6, 13, 12], [2, 3, 7, 6, 13], [18, 3, 7, 6, 13, 12, 0],
[4, 3, 7, 6, 13, 12], [1, 2, 13, 12, 0]]

hrany v grafe: 38 hrán
[(0,1,None), (0,8,None), (0,12,None), (0,18,None), (1,2,None), (1,5,None),
(1,16,None), (2,3,None), (2,9,None), (2,13,None), (3,4,None), (3,7,None),

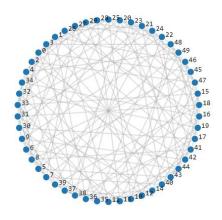
```
(3, 18, None), (4, 5, None), (4, 12, None), (4, 15, None), (5, 6, None), (5, 10, None), \\ (6, 7, None), (6, 13, None), (6, 17, None), (7, 8, None), (7, 11, None), (8, 9, None), \\ (8, 15, None), (9, 10, None), (9, 17, None), (10, 11, None), (10, 14, None), (11, 12, None), \\ (11, 16, None), (12, 13, None), (13, 14, None), (14, 15, None), (14, 18, None), (15, 16, None), \\ (16, 17, None), (17, 18, None)]
```

- počet grúp automorfizmov: 24
- matica lineárneho kódu:

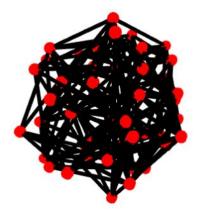


Obr. 4.18: Matica Robertsonovho grafu [coc]

4.1.7 Hoffman - Singletonov graf - cage(7,5)



Obr. 4.19: Hoffman - Singletonov graf 2D [coc]



Obr. 4.20: Hoffman - Singletonov graf 3D [coc]

• minimálny počet vrcholov: 50

 $\bullet\,$ rozmer minimálnej matice kódu: $50\times175\,$

• obvod cyklu v matici: 10

• minimálny počet hrán: 175

[36, 9, 7, 5, 49, 4, 34, 12], [48, 9, 7, 5, 49],

```
• cykly v grafe: 126 cyklov
  [[45, 24, 22, 35, 0], [30, 21, 24, 22, 35, 0], [39, 21, 24, 22, 35], [2, 47, 21, 24, 22, 35, 0],
  [8, 47, 21, 24, 22, 35], [48, 47, 21, 24, 22], [44, 15, 47, 21, 24, 22], [25, 15, 47, 21, 24, 22, 35, 0],
  [36, 15, 47, 21, 24, 22, 35], [33, 15, 47, 21, 24], [31, 18, 15, 47, 21, 24, 22], [45, 18, 15, 47, 21, 24],
  [39, 18, 15, 47, 21], [3, 28, 18, 15, 47, 21, 24, 22, 35, 0], [23, 28, 18, 15, 47, 21],
  [27, 28, 18, 15, 47, 21, 24, 22], [8, 28, 18, 15, 47],
  [29, 28, 18, 15, 47, 21, 24], [46, 13, 28, 18, 15, 47],
  [44, 13, 28, 18, 15], [11, 13, 28, 18, 15, 47, 21, 24, 22, 35],
  [30, 13, 28, 18, 15, 47, 21], [37, 13, 28, 18, 15, 47, 21, 24],
  [25, 10, 13, 28, 18, 15], [41, 10, 13, 28, 18, 15, 47, 21, 24], [48, 10, 13, 28, 18, 15, 47],
  [39, 10, 13, 28, 18], [43, 12, 10, 13, 28, 18, 15, 47, 21],
  [45, 12, 10, 13, 28, 18], [14, 12, 10, 13, 28, 18, 15, 47],
  [27, 12, 10, 13, 28], [36, 12, 10, 13, 28, 18, 15], [16, 34, 12, 10, 13, 28, 18], [8, 34, 12, 10, 13, 28],
  [33, 34, 12, 10, 13, 28, 18, 15], [30, 34, 12, 10, 13],
  [20, 34, 12, 10, 13, 28, 18, 15, 47, 21, 24, 22],
  [44, 4, 34, 12, 10, 13],
  [2, 4, 34, 12, 10, 13, 28, 18, 15, 47], [29, 4, 34, 12, 10, 13, 28],
  [39, 4, 34, 12, 10], [31, 1, 4, 34, 12, 10, 13, 28, 18],
  [46, 1, 4, 34, 12, 10, 13], [3, 1, 4, 34, 12, 10, 13, 28], [26, 1, 4, 34, 12, 10, 13, 28, 18, 15, 47, 21],
  [41, 1, 4, 34, 12, 10], [36, 1, 4, 34, 12], [17, 49, 4, 34, 12, 10, 13, 28, 18, 15],
  [23, 49, 4, 34, 12, 10, 13, 28], [45, 49, 4, 34, 12], [11, 49, 4, 34, 12, 10, 13], [48, 49, 4, 34, 12, 10],
  [31, 5, 49, 4, 34, 12, 10, 13, 28, 18], [43, 5, 49, 4, 34, 12], [25, 5, 49, 4, 34, 12, 10],
  [8, 5, 49, 4, 34], [37, 5, 49, 4, 34, 12, 10, 13], [46, 7, 5, 49, 4, 34, 12, 10, 13], [33, 7, 5, 49, 4, 34],
  [40, 7, 5, 49, 4, 34, 12, 10, 13, 28, 18, 15, 47, 21, 24, 22, 35, 0], [27, 7, 5, 49, 4, 34, 12],
  [39, 7, 5, 49, 4], [30, 9, 7, 5, 49, 4, 34],
  [42, 9, 7, 5, 49, 4, 34, 12, 10, 13, 28, 18],
```

```
[29, 9, 7, 5, 49, 4], [44, 6, 9, 7, 5, 49, 4], [45, 6, 9, 7, 5, 49],
  [26, 6, 9, 7, 5, 49, 4, 34, 12, 10, 13, 28, 18, 15, 47, 21], [8, 6, 9, 7, 5],
  [32, 6, 9, 7, 5, 49, 4, 34, 12, 10], [17, 38, 6, 9, 7, 5, 49], [14, 38, 6, 9, 7, 5, 49, 4, 34, 12],
  [37, 38, 6, 9, 7, 5], [20, 38, 6, 9, 7, 5, 49, 4, 34], [3, 38, 6, 9, 7, 5, 49, 4, 34, 12, 10, 13, 28],
  [39, 38, 6, 9, 7], [31, 32, 10, 13, 28, 18], [23, 32, 10, 13, 28], [2, 32, 10, 13, 28, 18, 15, 47],
  [33, 32, 10, 13, 28, 18, 15], [19, 32, 10, 13, 28, 18, 15, 47, 21, 24, 22, 35], [43, 42, 18, 15, 47, 21],
  [2, 42, 18, 15, 47], [11, 42, 18, 15, 47, 21, 24, 22, 35], [41, 42, 18, 15, 47, 21, 24],
  [20, 42, 18, 15, 47, 21, 24, 22], [40, 16, 18, 15, 47, 21, 24, 22, 35, 0], [37, 16, 18, 15, 47, 21, 24],
  [19, 16, 18, 15, 47, 21, 24, 22, 35], [48, 16, 18, 15, 47], [26, 16, 18, 15, 47, 21],
  [30, 17, 15, 47, 21], [41, 17, 15, 47, 21, 24],
  [27, 17, 15, 47, 21, 24, 22], [19, 17, 15, 47, 21, 24, 22, 35],
  [31, 14, 47, 21, 24, 22], [11, 14, 47, 21, 24, 22, 35],
  [29, 14, 47, 21, 24], [40, 14, 47, 21, 24, 22, 35, 0],
  [20, 46, 47, 21, 24, 22], [45, 46, 47, 21, 24], [19, 46, 47, 21, 24, 22, 35],
  [11, 26, 21, 24, 22, 35], [25, 26, 21, 24, 22, 35, 0], [27, 26, 21, 24, 22], [40, 23, 21, 24, 22, 35, 0],
  [20, 23, 21, 24, 22], [36, 23, 21, 24, 22, 35], [44, 43, 21, 24, 22], [3, 43, 21, 24, 22, 35, 0],
  [19, 43, 21, 24, 22, 35], [25, 29, 24, 22, 35, 0], [19, 29, 24, 22, 35], [2, 37, 24, 22, 35, 0],
  [36, 37, 24, 22, 35], [3, 33, 24, 22, 35, 0], [11, 33, 24, 22, 35], [8, 41, 24, 22, 35],
  [40, 41, 24, 22, 35, 0], [3, 48, 22, 35, 0], [2, 27, 22, 35, 0], [25, 20, 22, 35, 0],
  [40, 44, 22, 35, 0], [30, 31, 22, 35, 0]
• hrany v grafe: 175 hrán
  [(0, 2, None), (0, 3, None), (0, 25, None), (0, 30, None),
```

```
(0, 35, None), (0, 40, None), (0, 45, None), (1, 3, None),
(1, 4, None), (1, 26, None), (1, 31, None), (1, 36, None),
(1,41,None), (1,46,None), (2,4,None), (2,27,None),
(2, 32, None), (2, 37, None), (2, 42, None), (2, 47, None),
```

```
(3, 28, None), (3, 33, None), (3, 38, None), (3, 43, None),
```

$$(3, 48, None), (4, 29, None), (4, 34, None), (4, 39, None),$$

$$(4, 44, None), (4, 49, None), (5, 7, None), (5, 8, None),$$

$$(5, 25, None), (5, 31, None), (5, 37, None), (5, 43, None),$$

$$(5, 49, None), (6, 8, None), (6, 9, None), (6, 26, None),$$

$$(6, 32, None), (6, 38, None), (6, 44, None), (6, 45, None),$$

$$(7, 9, None), (7, 27, None), (7, 33, None), (7, 39, None),$$

$$(8, 35, None), (8, 41, None), (8, 47, None), (9, 29, None),$$

$$(9, 30, None), (9, 36, None), (9, 42, None), (9, 48, None),$$

$$(10, 12, None), (10, 13, None), (10, 25, None), (10, 32, None),$$

$$(10, 39, None), (10, 41, None), (10, 48, None), (11, 13, None),$$

```
(21, 24, None), (21, 26, None), (21, 30, None), (21, 39, None), \\ (21, 43, None), (21, 47, None), (22, 24, None), (22, 27, None), \\ (22, 31, None), (22, 35, None), (22, 44, None), (22, 48, None), \\ (23, 28, None), (23, 32, None), (23, 36, None), (23, 40, None), \\ (23, 49, None), (24, 29, None), (24, 33, None), (24, 37, None), \\ (24, 41, None), (24, 45, None), (25, 26, None), (25, 29, None), \\ (26, 27, None), (27, 28, None), (28, 29, None), (30, 31, None), \\ (30, 34, None), (31, 32, None), (32, 33, None), (33, 34, None), \\ (35, 36, None), (35, 39, None), (36, 37, None), (37, 38, None), \\ (38, 39, None), (40, 41, None), (40, 44, None), (41, 42, None), \\ (42, 43, None), (43, 44, None), (45, 46, None), (45, 49, None), \\ (46, 47, None), (47, 48, None), (48, 49, None)]
```

- počet grúp automorfizmov: 252000
- matica lineárneho kódu:

Obr. 4.21: Matica Hoffman - Singletonovho grafu [coc]

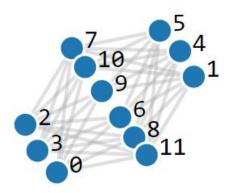
4.2 Generovanie klietok a ich Incidenčných matíc spolu s grupami automorfizmov

Uvažujeme existujúce klietky, ktoré je potrebné zostrojiť spoločne s grafom, na základe nich potom vygenerujeme incidenčnú maticu a zistíme grupu automorfizmov. Pre vygenerovanú klietku vieme zistiť všetky potrebné informácie ako v predošlom prípade.

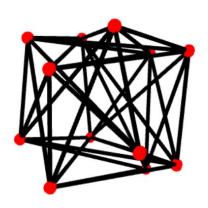
4.2.1 cage(6,4)

Klietku vygenerujeme ako bipartitný graf. V Sage použijeme metódu DegreeSequenceBipartite(s,s), ktorá bude mať 2 rovnaké parametre s, pričom každý predstavuje zoznam vrcholov. Najskôr je potrebné si vypočítať minimálny počet vrcholov m klietky cage(6,4) a na základe výpočtu viem určiť parameter. Každý zoznam obsahuje m/2 vrcholov stupňa k a teda platí:

$$s = [k, k, k, k, k, k] \ len(s) = \frac{m}{2}$$
 (4.1)



Obr. 4.22: Cage(6,4) graf 2D [coc]



Obr. 4.23: Cage(6,4) graf 3D [coc]

• minimálny počet vrcholov: 12

 \bullet rozmer minimálnej matice kódu: 12×36

• obvod cyklu v matici: 8

• minimálny počet hrán: 36

cykly v grafe: 25 cyklov
[[6,5,11,0],[7,5,11,0],[8,5,11,0],[9,5,11,0],[10,5,11,0],[6,4,11,0],
[7,4,11,0],[8,4,11,0],[9,4,11,0],[10,4,11,0],[6,3,11,0],[7,3,11,0],
[8,3,11,0],[9,3,11,0],[10,3,11,0],[6,2,11,0],[7,2,11,0],[8,2,11,0],
[9,2,11,0],[10,2,11,0],[6,1,11,0],[7,1,11,0],[8,1,11,0],[9,1,11,0],[10,1,11,0]]

hrany v grafe: 36 hrán
[(0,6, None), (0,7, None), (0,8, None), (0,9, None), (0,10, None), (0,11, None),
(1,6, None), (1,7, None), (1,8, None), (1,9, None), (1,10, None), (1,11, None),
(2,6, None), (2,7, None), (2,8, None), (2,9, None), (2,10, None), (2,11, None),
(3,6, None), (3,7, None), (3,8, None), (3,9, None), (3,10, None), (3,11, None),
(4,6, None), (4,7, None), (4,8, None), (4,9, None), (4,10, None), (4,11, None),
(5,6, None), (5,7, None), (5,8, None), (5,9, None), (5,10, None), (5,11, None)]

35

• počet grúp automorfizmov: 1036800

• matica lineárneho kódu:

Obr. 4.24: Matica klietky Cage(6,4) [coc]

Kapitola 5

Záver

XXXXXX

Literatúra

```
[bra]
    [bus]
[CBS+15] Chao Chen, Baoming Bai, Guangming Shi, Xiaotian Wang, and
          Xiaopeng Jiao. Nonbinary ldpc codes on cages: Structural pro-
          perty and code optimization. IEEE Transactions on Communica-
          tions, 63(2):364-375, 2015.
    [cho]
     [cle]
    [coc] Cocalc. https://cocalc.com/projects?session=default.
   [dura]
   [durb]
   [EJ11] Geoffrey Exoo and Robert Jajcay. Dynamic cage survey. The
          Electronic Journal of Combinatorics [electronic only], 1, 01 2011.
     [glf]
    [gre]
```

LITERATÚRA 38

```
[her]
 [hona]
 [honb]
  [kim]
 [kraa]
 [krab]
  [kue]
[Mal07] Gabofestwe Alafang Malema. Low-Density Parity-Check Codes:
        Construction and Implementation. School of Electrical and Elect-
        ronic Engineering, Faculty of Engineering, Computer and Mathe-
        matical Sciences The University of Adelaide, Australia, 2007.
  [mih]
  [ope]
   [pia]
   [pla]
  [red]
  [sag] Sage. https://www.sagemath.org/.
  [sun]
  [tay]
  [thu]
```

LITERATÚRA 39

[tnt]

[vie]

[wea]

[zhe]

Zoznam obrázkov

3.1	Vztah medzi grafom a maticou [Mal07]	6
3.2	Petersenov graf [EJ11]	8
3.3	Heawoodov graf [EJ11]	9
3.4	McGeeho graf [EJ11]	9
3.5	Tutte-Coxeterov graf [EJ11]	10
3.6	Robertsonov graf [EJ11]	10
4.1	Petersenov graf 2D [coc]	13
4.2	Petersenov graf 3D [coc]	13
4.3	Matica Petersenovho grafu [coc]	14
4.4	Heawoodov graf 2D [coc]	15
4.5	Heawoodov graf 3D [coc]	15
4.6	Matica Heawoodovho grafu [coc]	16
4.7	McGeeho graf 2D [coc]	17
4.8	McGeeho graf 3D [coc]	17
4.9	Matica McGeeho grafu [coc]	18
4.10	Tutte-Coxeterov graf 2D [coc]	19
4.11	Tutte-Coxeterov graf 3D [coc]	19
4.12	Matica Tutte - Coxeterovho grafu [coc]	21
4.13	Balabanov(10) graf 2D [coc]	21

ZOZNAM OBRÁZKOV	41
4.14 Balabanov(10) graf 3D [coc]	22
4.15 Matica Balabanovho(10) grafu [coc]	25
4.16 Robertsonov graf 2D [coc]	25
4.17 Robertsonov graf 3D [coc]	26
4.18 Matica Robertsonovho grafu [coc]	27
4.19 Hoffman - Singletonov graf 2D [coc]	28
4.20 Hoffman - Singletonov graf 3D [coc]	28
4.21 Matica Hoffman - Singletonovho grafu [coc]	32
4.22 Cage(6,4) graf 2D [coc]	33
4.23 $\operatorname{Cage}(6,4) \operatorname{graf} 3D [\operatorname{coc}] \dots \dots \dots \dots \dots \dots$	34
4.24 Matica klietky Cage(6,4) [coc]	35