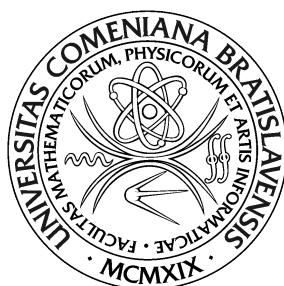


UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY



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
Jazyk záverečnej práce: anglický
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.

Cieľ: 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

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

Pod'akovanie

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 skúmaniu grúp automorfizmov lineárnych kódov ako aj lineárnym kódom s predpísanou grupou automorfizmov. V našej práci sa zameriavame na LDPC kódy.

Kľúčové slová: automorfizmus grúp, LDPC, kletky

Abstract

This thesis deals with the problem of examining groups of automorphisms of linear codes as well as linear codes with a prescribed group of automorphisms. In our work we focus on LDPC codes.

Keywords: Automorphism groups, LDPC, cages

Obsah

1	Úvod	1
2	Motivácia	2
3	Analýza problému	3
3.1	Lineárny kód	3
3.1.1	Generujúca matica lineárneho kódu	3
3.1.2	Kontrolná matica lineárneho kódu	4
3.1.3	LDPC kódy	4
3.2	Grafová reprezentácia LDPC kódov	5
3.2.1	Základné pojmy	5
3.2.2	Automorfizmus grafu	6
3.2.3	Klietky	7
4	Návrh riešenia	11
4.1	Generovanie incidenčných matíc, grúp automorfizmov zo za- daných klietok	11
4.2	Generovanie incidenčných matíc, grúp automorfizmov zo za- daného zoznamu susedností	12
4.3	Generovanie klietky a následne incidenčných matíc, grúp au- tomorfizmov	13

4.3.1	Generovanie $cage(6, 4)$	13
4.4	Experimentálne Generovanie incidenčných matíc	14
4.4.1	Generovanie incidenčnej matice z parametrov $cage(6, 4)$	14
5	Výsledky	15
5.1	Generovanie incidenčných matíc, grúp automorfizmov zo za- daných kliebok	15
5.1.1	Petersenov graf - $cage(3, 5)$	15
5.1.2	Heawoodov graf - $cage(3, 6)$	17
5.1.3	McGeeho graf - $cage(3, 7)$	18
5.1.4	Tutte - Coxeterov graf - $cage(3, 8)$	20
5.1.5	Balabanov graf - $cage(3, 10)$	21
5.1.6	Robertsonov graf - $cage(4, 5)$	23
5.1.7	Hoffman - Singletonov graf - $cage(7, 5)$	25
5.2	Generovanie incidenčných matíc, grúp automorfizmov zo za- daného zoznamu susedností	29
5.2.1	$cage(3, 11)$	29
5.2.2	$cage(3, 14)$	29
5.2.3	$cage(3, 16)$	29
5.2.4	$cage(3, 17)$	30
5.2.5	$cage(3, 18)$	30
5.2.6	$cage(3, 20)$	30
5.2.7	$cage(3, 23)$	30
5.2.8	$cage(3, 25)$	31
5.2.9	$cage(4, 7)$	31
5.2.10	$cage(4, 9)$	33
5.2.11	$cage(4, 10)$	34
5.2.12	$cage(5, 10)$	34

5.2.13	cage(7,7)	34
5.2.14	cage(7,8)	34
5.2.15	cage(10,5)	35
5.2.16	cage(11,5)	35
5.2.17	cage(12,5)	35
5.2.18	cage(13,5)	35
5.3	Generovanie kletky a následne incidenčných matíc, grúp automorfizmov	36
5.3.1	cage(6,4)	36
5.4	Vyhodnotenie výsledkov generovania incidenčných matíc z kletok a grúp automorfizmov	37
5.5	Experimentálne Generovanie incidenčných matíc	39
5.5.1	Generovanie Incidenčnej matice, ktorej výsledkom bude cage(6,4)	39
5.6	Vyhodnotenie výsledkov experimentálneho generovania incidenčných matíc	42

Kapitola 1

Úvod

xxxxxxx

Kapitola 2

Motivácia

xxxxxxx

Kapitola 3

Analýza problému

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.[MTSB13] [HP03] Ak je splnená vlastnosť, ktorá hovorí, že *modulo* $2(q)$ súčtu 2 kódových slov je kódové slovo, tak vieme nájsť Generačnú maticu lineárneho kódu.[Mal07]

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 . [MTSB13] [HP03] Nech \vec{m} je vstup (nekódované slovo), \vec{v} je výstup (kódované slovo), C je označenie lineárneho

kódu, potom platí:

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

3.1.2 Kontrolná matica lineárneho kódu

V k -rozmernom linearnom kóde (C) v F_2^n 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 . [MTSB13] [HP03] Ľubovoľný vektor \vec{v} je kódovým slovom práve vtedy, ak platí:

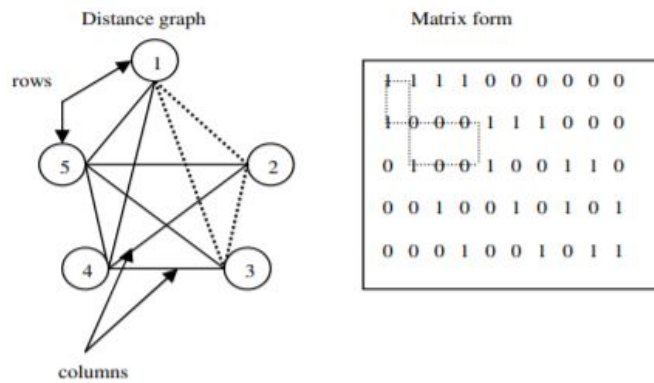
$$C = \{\vec{v} \in F_2^n : H \times \vec{v}^T = 0\} \quad (3.2)$$

3.1.3 LDPC kódy

LDPC kódy (z angl. low density parity check code) sú lineárne samoopravne 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.[MTSB13] 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.[Mal07]

3.2 Grafová reprezentácia LDPC kódov

Matica LDPC je reprezentovaná Tannerovým grafom. Matica môže byť tiež reprezentovaná nebipartitným 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 odvodenú z grafu vzdialenosti:[Mal07]



Obr. 3.1: Vzťah 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.
- Kódová váha a rate (R) - predstavuje počet bitov (informácií) nad celkovým počtom prenesených bitov. Rate možno vyjadriť vzťahom:

[MTSB13]

$$R = (N - M)/N \quad (3.3)$$

- Minimálna Hammingová (kódová) vzdialenosť $\min HW(\vec{u}, \vec{v})$ - 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.[MTSB13] [HP03]
- Obvod (g) - ovplyvňuje dekódovanie LDPC kódu. V grafovej reprezentácii LDPC kódu sa jedná o najmenší cyklus v grafe. Jeho dĺžku zráčavame 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.[Mal07]
- Moorov graf - Pravidelný graf stupňa d a parametra k vo forme stromu vyhľadávania do šírky začínajúceho z ľubovoľného vrcholu V , ktorého počet vrcholov vieme dostať ako:

$$1 + d \sum_{i=0}^{k-1} (d-1)^i \quad (3.4)$$

- Rád grafu - Predstavuje počet vrcholov daného grafu

3.2.2 Automorfizmus grafu

Automorfizmus grafu je permutácia ϕ všetkých vrcholov grafu, ktorá zachováva jeho štruktúru takým spôsobom, že akékoľvek 2 vrcholy U a V susedia iba vtedy a len vtedy ak platí, že $\phi(U)$ susedí s $\phi(V)$. [EJ13] Zjednodušene môžeme povedať, že sa jedná 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 vlastnia grupu automorfizmov, ktorá prechodne pôsobí na vrcholy daného grafu.[EJ13]

3.2.3 Klietky

Na konštrukciu LDPC kódov môžeme využiť grafy vzdialenosti. Tieto grafy delíme na regulárne s vrcholmi rovnakého stupňa (napr. Moorové grafy) a neregulárne s vrcholmi rôznych stupňov.[Mal07]. V našej práci sa budeme venovať regulárnym grafom vzdialenosti. Klietka $cage(k, g)$ je k -regulárny graf obvodu g s najmenším možným počtom vrcholov $M(k, g)$ [Mal07]. Výpočet minimálneho počtu vrcholov pre klietku sa líši podľa toho, či je jej obvod párný alebo nepárny:

- g - nepárne:

$$M(k, g) \leq 1 + \sum_{i=0}^{(g-3)/2} k(k-1)^i = \frac{k(k-1)^{(g-1)/2} - 2}{k-2} \quad (3.5)$$

- g - párne:

$$M(k, g) \leq 2 \sum_{i=0}^{(g-2)/2} k(k-1)^i = \frac{2(k-1)^{g/2} - 2}{k-2} \quad (3.6)$$

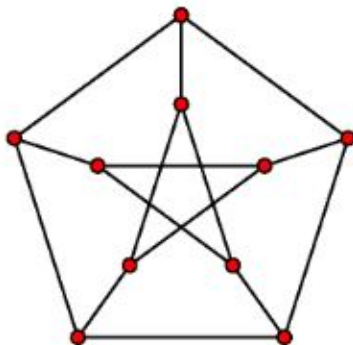
Dolné ohraničenie počtu vrcholov $M(k, g)$ sa tiež nazýva Moorové ohraničenie.[EJ13]

Pre klietku ako Moorov graf platí:

$$d = k \quad (3.7)$$

Aj keď neexistuje jednotná konštrukcia kliebok, existuje niekoľko známych kliebok pre stupeň vrchola k a obvod g . Ukážeme si niektoré z nich:

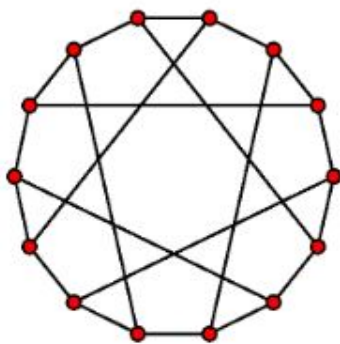
- Petersenov graf - cage(3,5):



Obr. 3.2: Petersenov graf [EJ13]

Petersenov graf má rád 10. Automorfizmus grúp je izomorfný k $\text{Sym}(5)$.
Graf je vrcholovo tranzitívny.[EJ13]

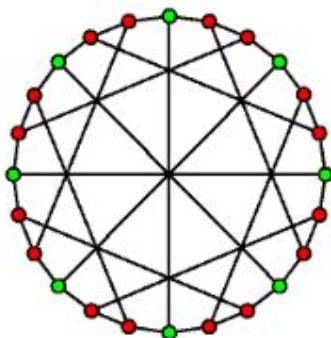
- Heawoodov graf - cage(3,6):



Obr. 3.3: Heawoodov graf [EJ13]

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

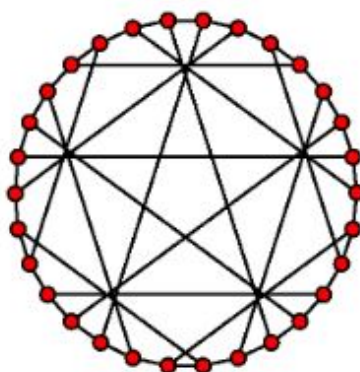
- McGeeho graf - $\text{cage}(3,7)$:



Obr. 3.4: McGeeho graf [EJ13]

McGeeho graf má rád 24 a počet grúp automorfizmov je 32. Graf nie je vrcholovo tranzitívny.[EJ13]

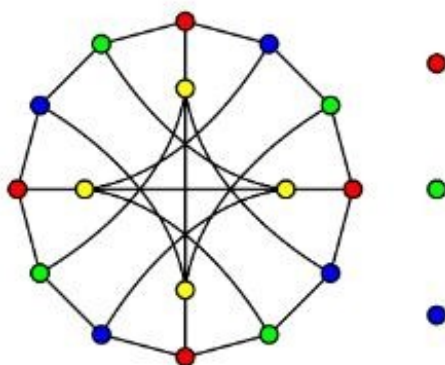
- Tutte-Coxeterov graf - $\text{cage}(3,8)$:



Obr. 3.5: Tutte-Coxeterov graf [EJ13]

Tutte-Coxterov graf má rád 30 a počet grúp automorfizmov je 1440. Graf je vrcholovo tranzitívny.[EJ13]

- Balabanov graf - $\text{cage}(3,11)$: Balabanov graf má 112 vrcholov a počet grúp automorfizmov je 64. Graf nie je vrcholovo tranzitívny.[EJ13]
- Bensonov graf - $\text{cage}(3,12)$: Bensonov graf má 126 vrcholov a počet grúp automorfizmov je 12096. Graf je vrcholovo tranzitívny.[EJ13]
- Robertsonov graf - $\text{cage}(4,5)$:



Obr. 3.6: Robertsonov graf [EJ13]

- Ďalšie známe kletky: $\text{cage}(4,7)$ - Exoo, McKay, a Nadonov graf, $\text{cage}(5,5)$: počet grúp automorfizmov je 20, 30 a 120, $\text{cage}(7,5)$ - Hoffman - Singletonov graf, $\text{cage}(7,6)$ - O'Keefe a Wongov graf[EJ13]

Kapitola 4

Návrh riešenia

Problematiku riešime v programe Sage [The], ktorý je založený na programovacím 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 matic, grúp automorfizmov zo zadaných kliebok

Program Sage ponúka zopár vopred naimplementovaných grafov, ktoré môžeme využiť ako kliebky. Jedná sa o Petersenov graf - $cage(3, 5)$, Heawoodov graf - $cage(3, 6)$, McGeeho graf - $cage(3, 7)$, Tutte - Coxeterov graf - $cage(3, 8)$, Balabanov graf - $cage(3, 10)$, Robertsonov graf - $cage(4, 5)$, Hoffman - Singletonov graf - $cage(7, 5)$. Z týchto grafov vieme zistiť cykly formujúce daný graf. Na zistenie týchto cyklov je potrebné naimplementovať metódu, ktorá získa

utriedený zoznam vrcholov v cykloch (pomocou `graph.minimum_cycle_basis()` [The]) a následne z grafu vytvoríme podgrafy obsahujúce tieto vrcholy (pomocou metódy `subgraph()` [The], zoznam vrcholov bude parameter). Takýto podgraf obsahuje len 1 cyklus (získame pomocou metódy `cycle_basis()` [The]), ktorý pridáme do nášho zoznamu cyklov, ktoré sledujeme. ďalej vieme získať incidenčnú maticu (pomocou metódy `incidence_matrix()` [The]), zoznam všetkých vrcholov (pomocou metódy `vertices()` [The]), zoznam všetkých hrán (pomocou metódy `edges()` [The]) a zoznam všetkých grúp automorfizmov (pomocou `automorphism_group()` [The]). Pre výpočet počtu vrcholov, počtu hrán a počtu grúp automorfizmov nám stačí iba zistiť veľkosť ich zoznamov. Na verifikáciu existencie kliebok bude potrebné vytvoriť metódu, ktorá z parametrov kliebky zistí Moorove ohraničenie a na jej základe vieme otestovať počet vrcholov, hrán, minimálny rozmer incidenčnej matice. Na verifikáciu ako aj výpočet bude potrebné zostrojiť samostatné metódy.

4.2 Generovanie incidenčných matíc, grúp automorfizmov zo zadaného zoznamu susedností

Uvažujeme existujúce vstupné textové súbory, ktoré nesú informácie o susednostiach všetkých uvažovaných vrcholov jednotlivo pre 1 kliebku. Tieto vstupné súbory sme získali na stránke p. Exooa. Je potrebné vytvoriť metódu, ktorá nám rozdelí tieto dáta na zoznamy vrcholov a vieme si z nich vytvoriť hrany, ktoré postupne popridávame prázdnomu grafu (vytvorený pomocou metódy `EmptyGraph()` [The]) a tým z neho vytvoríme požadovanú kliebku, ktorú využijeme na spracovanie a získanie informácií ako v predchá-

dzajúcom návrhu zo zadaných klieťok. Rovnako aj testovanie s validáciou.

4.3 Generovanie klieťky a následne incidenčných matíc, grúp automorfizmov

Generovanie klieťok nemá jednotný prístup, je potrebné k nim pristupovať jednotlivo alebo preskúmať skupiny, ktoré sa generujú podobným spôsobom.[EJ13]

4.3.1 Generovanie $cage(6, 4)$

Klieťku vygenerujeme ako bipartitný graf. V Sage použijeme metódu `DegreeSequenceBipartite(s,s)[The]`, ktorá bude mať 2 rovnaké parametre s , pričom každý predstavuje zoznam vrcholov. Najskôr je potrebné si vypočítať Moorovo ohraňenie pre minimálny počet vrcholov, ktorú už máme implementovanú. $Cage(6, 4)$ je taký typ klieťky, ktorej počet vrcholov m je rovnaký ako minimálny počet vrcholov z Moorovho ohraňenia.[Mal07] Tieto vrcholy rozdelím na 2 zoznamy takým spôsobom, že každý zoznam bude obsahovať $\frac{m}{2}$ vrcholov stupňa k a teda platí:

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

Grafu nastavíme vrcholy pomocou metódy `set_vertex()`[The]. Výsledný graf bude $cage(6, 4)$ ku ktorému potom pristupujeme rovnako ako v predošlých prípadoch.

4.4 Experimentálne Generovanie incidenčných matíc

4.4.1 Generovanie incidenčnej matice z parametrov $cage(6, 4)$

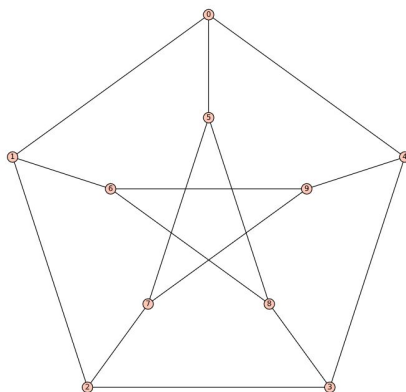
Využijeme parametre stupeň $k = 6$, počet vrcholov $m = 12$ a počet hrán $pocetHran = 36$. Potrebujeme metódu na vytvorenie vektora s počtom jednotiek k a počtom núl $pocetHran - k$. Tento vektor rovnomerne náhodne permutujeme (pomocou metódy `numpy.random.shuffle()`[The] s parametrom vektora) a získame náhodný vektor s Hammingovou váhou k . Incidenčnú maticu môžeme skontroštruovať takým spôsobom, že do nej postupne pridávame takéto náhodné vektory avšak musí platiť, že v každom stĺpci musí byť maximálna Hammingová váha 2. Na túto podmienku si vytvoríme ďalšiu samostatnú metódu, kde si inicializujeme nulový vektor (pomocou `zero_vector(SR, pocetHran)`[The]). V prípade, že táto podmienka nie je splnená je potrebné vymazať posledný vektor a vygenerovať ho nanovo. Takýmto spôsobom vieme naplniť všetky riadky matice avšak môže obsahovať aj duplicitné hrany. Tie odstránime tým, že si maticu vložíme do grafu, získame z neho všetky hrany, ktoré v množine set zbavíme duplicitných výskytov a následne ich opäť vložíme do grafu, z ktorého získame neúplnú incidenčnú maticu. Niekedy je duplicitných hrán viac niekedy menej. Pomocou cyklu získavame opakovane hrany ošetrené o duplicitu až kým nedostaneme $pocetHran - 2$ jedinečných hrán. Posledné 2 hrany si na základe aktuálneho stavu už vieme dopočítať a dopočítame posledné 2 stĺpce matice tak aby mal každý riadok Hammingovú váhu k a každý stĺpec 2. Výslednú maticu opäť preverím na duplicitu a získavam konečný tvar potencionalnej incidenčnej matice. Keďže tento postup nie je overený, budeme ho realizovať v pokusoch a na záver vyhodnotíme, či sa nám podarilo získať maticu incidencie $cage(6, 4)$ alebo nie.

Kapitola 5

Výsledky

5.1 Generovanie incidenčných matíc, grúp automorfizmov zo zadaných kliebok

5.1.1 Petersenov graf - cage(3,5)



Obr. 5.1: Petersenov graf [The]

- Cykly formujúce graf:

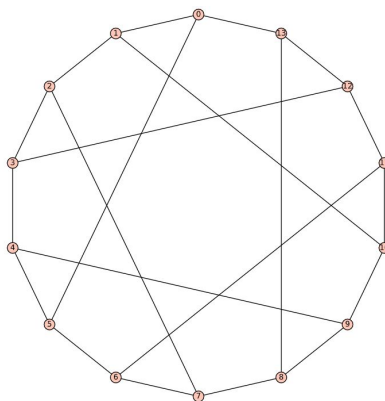
$[[4, 3, 8, 5, 0]], [[1, 2, 3, 4, 0]], [[1, 6, 8, 5, 0]], [[1, 2, 7, 5, 0]], [[4, 9, 7, 5, 0]], [[1, 6, 9, 4, 0]]$

- Vrcholy v grafe: 10 vrcholov
 $[0, 1, 2, 3, 4, 5, 6, 7, 8, 9]$
- Hrany v grafe: 15 hrán
 $[(0, 1), (0, 4), (0, 5), (1, 2), (1, 6), (2, 3), (2, 7), (3, 4),$
 $(3, 8), (4, 9), (5, 7), (5, 8), (6, 8), (6, 9), (7, 9)]$
- Počet grúp automorfizmov: 120
- Incidenčná matica:

$$\begin{bmatrix}
 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1
 \end{bmatrix}$$

Obr. 5.2: Incidenčná matica Petersenovho grafu

5.1.2 Heawoodov graf - cage(3,6)



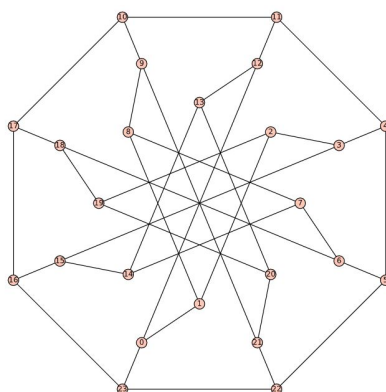
Obr. 5.3: Heawoodov graf [The]

- Cykly formující graf:
 $[[5, 6, 11, 12, 13, 0]], [[1, 2, 3, 12, 13, 0]], [[1, 10, 11, 6, 5, 0]], [[1, 2, 7, 8, 13, 0]],$
 $[[5, 4, 3, 12, 13, 0]], [[1, 10, 9, 4, 5, 0]], [[5, 6, 7, 8, 13, 0]], [[1, 10, 9, 8, 13, 0]]$
- Vrcholy v grafe: 14 vrcholov
 $[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13]$
- Hrany v grafe: 21 hrán
 $[(0, 1), (0, 5), (0, 13), (1, 2), (1, 10), (2, 3), (2, 7), (3, 4), (3, 12), (4, 5), (4, 9), (5, 6),$
 $(6, 7), (6, 11), (7, 8), (8, 9), (8, 13), (9, 10), (10, 11), (11, 12), (12, 13)]$
- Počet grup automorfizmov: 336
- Incidenčná matica:

[1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0]
[1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0]
[0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0]
[0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0]
[0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0]
[0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0]
[0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0]
[0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0]
[0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0]
[0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0]
[0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0]
[0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1]
[0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1]
[0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1]

Obr. 5.4: Incidenčná matica Heawoodovho grafu

5.1.3 McGeeho graf - cage(3,7)



Obr. 5.5: McGeeho graf[The]

- Cykly formujúce graf:

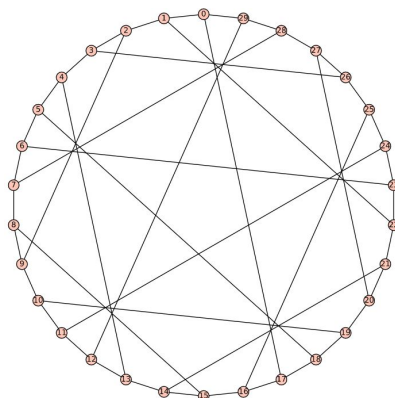
$[[[23, 22, 21, 20, 13, 12, 0]], [[1, 2, 3, 15, 16, 23, 0]], [[1, 8, 9, 10, 11, 12, 0]],$
 $[[1, 2, 19, 20, 13, 12, 0]], [[1, 2, 3, 4, 11, 12, 0]], [[23, 22, 5, 4, 11, 12, 0]],$
 $[[3, 4, 5, 6, 18, 19, 2]], [[2, 19, 18, 6, 7, 8, 1]], [[1, 8, 7, 14, 13, 12, 0]],$
 $[[1, 8, 9, 21, 22, 23, 0]], [[23, 16, 17, 10, 11, 12, 0]], [[23, 16, 15, 14, 13, 12, 0]],$
 $[[3, 15, 16, 17, 18, 19, 2]]]$

- Vrcholy v grafe: 24 vrcholov
 $[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23]$
- Hrany v grafe: 36 hrán
 $[(0, 1), (0, 12), (0, 23), (1, 2), (1, 8), (2, 3), (2, 19), (3, 4), (3, 15),$
 $(4, 5), (4, 11), (5, 6), (5, 22), (6, 7), (6, 18), (7, 8), (7, 14), (8, 9),$
 $(9, 10), (9, 21), (10, 11), (10, 17), (11, 12), (12, 13), (13, 14), (13, 20), (14, 15),$
 $(15, 16), (16, 17), (16, 23), (17, 18), (18, 19), (19, 20), (20, 21), (21, 22), (22, 23)]$
- Počet grúp automorfizmov: 32
- Incidenčná matica:

[illegible]

Obr. 5.6: Incidenčná matica McGeeho grafu

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



Obr. 5.7: Tutte-Coxeterov graf [The]

- Cykly formující graf:

$[[17, 18, 19, 10, 11, 12, 29, 0]], [[1, 2, 3, 26, 25, 16, 17, 0]],$
 $[[1, 22, 23, 6, 7, 28, 29, 0]], [[1, 2, 9, 8, 7, 28, 29, 0]],$
 $[[1, 2, 3, 4, 13, 12, 29, 0]], [[17, 18, 5, 4, 13, 12, 29, 0]],$
 $[[17, 18, 5, 6, 7, 28, 29, 0]], [[1, 22, 21, 20, 19, 18, 17, 0]],$
 $[[1, 2, 9, 10, 19, 18, 17, 0]], [[17, 16, 15, 8, 7, 28, 29, 0]],$
 $[[17, 16, 25, 24, 11, 12, 29, 0]], [[17, 18, 19, 20, 27, 28, 29, 0]],$
 $[[17, 16, 15, 14, 13, 12, 29, 0]], [[1, 22, 21, 14, 13, 12, 29, 0]],$
 $[[17, 16, 25, 26, 27, 28, 29, 0]], [[1, 22, 23, 24, 25, 16, 17, 0]]]$

- Vrcholy v grafe: 30 vrcholov

$[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15,$
 $16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29]$

- Hrany v grafe: 45 hrán

$[(0, 1), (0, 17), (0, 29), (1, 2), (1, 22), (2, 3), (2, 9), (3, 4), (3, 26),$
 $(4, 5), (4, 13), (5, 6), (5, 18), (6, 7), (6, 23), (7, 8), (7, 28), (8, 9),$

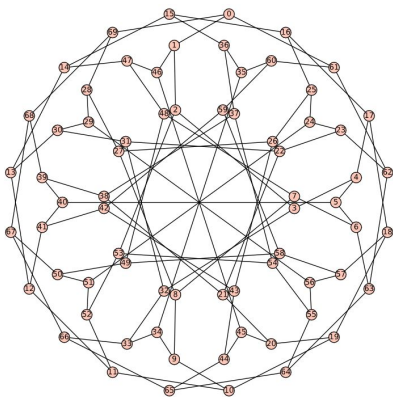
$$(8, 15), (9, 10), (10, 11), (10, 19), (11, 12), (11, 24), (12, 13), (12, 29), (13, 14),$$
$$(14, 15), (14, 21), (15, 16), (16, 17), (16, 25), (17, 18), (18, 19), (19, 20), (20, 21),$$
$$(20, 27), (21, 22), (22, 23), (23, 24), (24, 25), (25, 26), (26, 27), (27, 28), (28, 29)]$$

- Počet grúp automorfizmov: 1440
- Incidenčná matica:

[illegible]

Obr. 5.8: Incidenčná matica Tutte - Coxeterovho grafu

5.1.5 Balabanov graf - cage(3,10)



Obr. 5.9: Balabanov(10) graf[The]

- Cykly formující graf:

$[[1, 46, 47, 14, 13, 30, 29, 28, 69, 0]], [[1, 2, 53, 52, 51, 24, 23, 62, 61, 0]],$
 $[[1, 2, 53, 54, 37, 38, 39, 68, 69, 0]], [[1, 2, 3, 32, 33, 34, 35, 60, 61, 0]],$
 $[[1, 2, 3, 4, 5, 6, 63, 62, 61, 0]], [[2, 3, 4, 17, 18, 19, 20, 45, 46, 1]],$
 $[[1, 2, 3, 4, 5, 40, 39, 68, 69, 0]], [[1, 46, 47, 48, 7, 6, 63, 62, 61, 0]],$
 $[[69, 28, 27, 8, 7, 6, 63, 62, 61, 0]], [[69, 28, 27, 8, 9, 34, 35, 60, 61, 0]],$
 $[[3, 2, 53, 52, 11, 10, 9, 34, 33, 32]], [[2, 53, 52, 11, 10, 19, 20, 45, 46, 1]],$
 $[[2, 53, 52, 11, 12, 13, 14, 47, 46, 1]], [[3, 4, 5, 40, 41, 12, 11, 52, 53, 2]],$
 $[[1, 46, 45, 44, 43, 26, 27, 28, 69, 0]], [[1, 46, 47, 14, 15, 36, 35, 60, 61, 0]],$
 $[[2, 3, 4, 17, 16, 15, 14, 47, 46, 1]], [[3, 4, 17, 16, 25, 24, 51, 52, 53, 2]],$
 $[[3, 4, 17, 18, 57, 56, 55, 54, 53, 2]], [[1, 46, 45, 20, 21, 38, 39, 68, 69, 0]],$
 $[[1, 46, 45, 20, 21, 22, 23, 62, 61, 0]], [[69, 28, 29, 30, 31, 22, 23, 62, 61, 0]],$
 $[[1, 2, 53, 54, 37, 36, 35, 60, 61, 0]], [[69, 28, 27, 26, 25, 24, 23, 62, 61, 0]],$
 $[[1, 46, 47, 48, 49, 50, 67, 68, 69, 0]], [[1, 2, 53, 54, 55, 56, 29, 28, 69, 0]],$
 $[[1, 2, 3, 32, 31, 30, 29, 28, 69, 0]], [[1, 2, 3, 32, 33, 66, 67, 68, 69, 0]],$
 $[[1, 2, 53, 54, 55, 64, 63, 62, 61, 0]], [[69, 68, 67, 66, 65, 64, 63, 62, 61, 0]],$
 $[[69, 68, 39, 40, 41, 42, 59, 60, 61, 0]], [[1, 46, 45, 44, 43, 42, 59, 60, 61, 0]],$
 $[[1, 46, 45, 44, 65, 66, 67, 68, 69, 0]], [[1, 46, 47, 48, 49, 58, 59, 60, 61, 0]],$
 $[[1, 2, 53, 52, 51, 50, 67, 68, 69, 0]], [[69, 28, 29, 56, 57, 58, 59, 60, 61, 0]]]$

- Vrcholy v grafe: 70 vrcholov

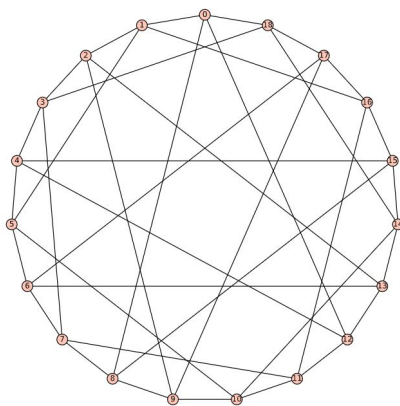
$[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13,$
 $14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28,$
 $29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41,$
 $42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54,$
 $55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69]$

- Hrany v grafe: 105 hrán

$[(0, 1), (0, 61), (0, 69), (1, 2), (1, 46), (2, 3), (2, 53), (3, 4),$
 $(3, 32), (4, 5), (4, 17), (5, 6), (5, 40), (6, 7), (6, 63), (7, 8),$
 $(7, 48), (8, 9), (8, 27), (9, 10), (9, 34), (10, 11), (10, 19), (11, 12),$
 $(11, 52), (12, 13), (12, 41), (13, 14), (13, 30), (14, 15), (14, 47), (15, 16),$
 $(15, 36), (16, 17), (16, 25), (17, 18), (18, 19), (18, 57), (19, 20), (20, 21),$
 $(20, 45), (21, 22), (21, 38), (22, 23), (22, 31), (23, 24), (23, 62), (24, 25),$
 $(24, 51), (25, 26), (26, 27), (26, 43), (27, 28), (28, 29), (28, 69), (29, 30),$
 $(29, 56), (30, 31), (31, 32), (32, 33), (33, 34), (33, 66), (34, 35), (35, 36),$
 $(35, 60), (36, 37), (37, 38), (37, 54), (38, 39), (39, 40), (39, 68), (40, 41),$
 $(41, 42), (42, 43), (42, 59), (43, 44), (44, 45), (44, 65), (45, 46), (46, 47),$
 $(47, 48), (48, 49), (49, 50), (49, 58), (50, 51), (50, 67), (51, 52), (52, 53),$
 $(53, 54), (54, 55), (55, 56), (55, 64), (56, 57), (57, 58), (58, 59), (59, 60),$
 $(60, 61), (61, 62), (62, 63), (63, 64), (64, 65), (65, 66), (66, 67), (67, 68), (68, 69)]$

- Počet grúp automorfizmov: 80

5.1.6 Robertsonov graf - cage(4,5)



Obr. 5.10: Robertsonov graf [The]

- Cykly formující graf:

$[[1, 2, 3, 18, 0]], [[8, 7, 11, 12, 0]], [[1, 16, 17, 18, 0]],$
 $[[1, 16, 11, 12, 0]], [[1, 2, 9, 8, 0]], [[1, 2, 13, 12, 0]],$
 $[[18, 3, 4, 12, 0]], [[18, 3, 7, 8, 0]], [[1, 5, 4, 12, 0]],$
 $[[8, 15, 4, 12, 0]], [[16, 17, 6, 5, 1]], [[2, 9, 10, 5, 1]],$
 $[[2, 13, 6, 5, 1]], [[3, 7, 6, 13, 2]], [[18, 14, 15, 8, 0]],$
 $[[18, 17, 9, 8, 0]], [[16, 11, 10, 5, 1]], [[9, 10, 14, 13, 2]],$
 $[[18, 14, 13, 12, 0]], [[1, 16, 15, 8, 0]]$

- Vrcholy v grafe: 19 vrcholov

$[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18]$

- Hrany v grafe: 38 hrán

$[(0, 1), (0, 8), (0, 12), (0, 18), (1, 2), (1, 5), (1, 16), (2, 3), (2, 9),$
 $(2, 13), (3, 4), (3, 7), (3, 18), (4, 5), (4, 12), (4, 15), (5, 6), (5, 10),$
 $(6, 7), (6, 13), (6, 17), (7, 8), (7, 11), (8, 9), (8, 15), (9, 10), (9, 17),$
 $(10, 11), (10, 14), (11, 12), (11, 16), (12, 13), (13, 14), (14, 15), (14, 18), (15, 16),$
 $(16, 17), (17, 18)]$

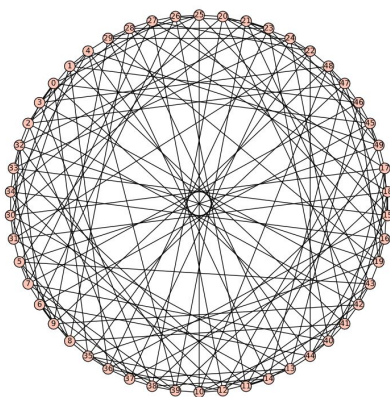
- Počet grup automorfizmov: 24

- Incidenčná matica:

[illegible]

Obr. 5.11: Incidenčná matica Robertsonovho grafu

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



Obr. 5.12: Hoffman - Singletonov graf [The]

- Cykly formující graf:
 $[[[28, 29, 24, 41, 8]], [[24, 37, 16, 34, 33]],$
 $[[24, 22, 35, 11, 33]], [[41, 24, 37, 36, 1]],$
 $[[45, 24, 21, 26, 6]], [[44, 22, 24, 45, 6]],$
 $[[33, 24, 45, 6, 32]], [[24, 45, 6, 38, 37]],$
 $[[45, 24, 41, 8, 6]], [[45, 24, 29, 9, 6]],$

$[[24, 22, 20, 46, 45]], [[24, 45, 46, 7, 33]],$
 $[[46, 45, 24, 41, 1]], [[24, 29, 19, 46, 45]],$
 $[[24, 45, 46, 13, 37]], [[24, 21, 47, 46, 45]],$
 $[[45, 24, 37, 2, 0]], [[45, 24, 41, 40, 0]],$
 $[[45, 24, 29, 25, 0]], [[45, 24, 21, 30, 0]],$
 $[[45, 24, 22, 35, 0]], [[45, 24, 33, 3, 0]],$
 $[[24, 22, 27, 7, 33]], [[24, 37, 5, 7, 33]],$
 $[[24, 41, 40, 7, 33]], [[24, 21, 39, 7, 33]],$
 $[[24, 29, 9, 7, 33]], [[21, 24, 45, 18, 39]],$
 $[[39, 21, 24, 29, 4]], [[21, 24, 41, 10, 39]],$
 $[[24, 21, 39, 38, 37]], [[39, 21, 24, 22, 35]],$
 $[[10, 41, 24, 33, 32]], [[24, 41, 10, 13, 37]],$
 $[[24, 22, 48, 10, 41]], [[24, 29, 25, 10, 41]],$
 $[[24, 45, 12, 10, 41]], [[37, 24, 29, 25, 5]],$
 $[[24, 29, 28, 23, 21]], [[24, 37, 38, 3, 33]],$
 $[[24, 21, 30, 13, 37]], [[37, 24, 22, 27, 2]],$
 $[[24, 22, 20, 38, 37]], [[24, 41, 17, 38, 37]],$
 $[[24, 29, 14, 38, 37]], [[4, 29, 24, 41, 1]],$
 $[[21, 24, 29, 19, 43]], [[24, 29, 25, 15, 33]],$
 $[[29, 24, 21, 30, 9]], [[45, 24, 29, 14, 12]],$
 $[[25, 29, 24, 22, 20]], [[37, 24, 45, 49, 5]],$
 $[[24, 29, 25, 26, 21]], [[24, 22, 20, 42, 41]],$
 $[[24, 41, 42, 11, 33]], [[24, 45, 18, 42, 41]],$
 $[[37, 24, 41, 42, 2]], [[24, 21, 43, 42, 41]],$
 $[[24, 29, 9, 42, 41]], [[24, 29, 28, 27, 22]],$
 $[[47, 21, 24, 41, 8]], [[24, 29, 28, 13, 37]],$
 $[[24, 29, 28, 18, 45]], [[24, 29, 28, 3, 33]], [[2, 37, 24, 33, 32]],$

$[[37, 24, 21, 47, 2]], [[37, 24, 29, 4, 2]],$
 $[[24, 22, 48, 3, 33]], [[24, 21, 43, 3, 33]],$
 $[[3, 33, 24, 41, 1]], [[24, 21, 26, 16, 37]],$
 $[[24, 22, 48, 16, 37]], [[24, 41, 40, 16, 37]],$
 $[[24, 29, 19, 16, 37]], [[24, 45, 18, 16, 37]],$
 $[[26, 21, 24, 41, 1]], [[24, 22, 27, 26, 21]],$
 $[[24, 21, 26, 11, 33]], [[23, 21, 24, 33, 32]],$
 $[[33, 24, 22, 31, 32]], [[33, 24, 29, 19, 32]],$
 $[[37, 24, 21, 43, 5]], [[24, 45, 18, 15, 33]],$
 $[[24, 29, 14, 11, 33]], [[24, 21, 23, 49, 45]],$
 $[[37, 24, 41, 8, 5]], [[37, 24, 22, 31, 5]],$
 $[[24, 22, 48, 49, 45]], [[48, 22, 24, 21, 47]], [[29, 24, 22, 48, 9]],$
 $[[29, 24, 22, 44, 4]], [[29, 24, 45, 49, 4]],$
 $[[24, 29, 4, 34, 33]], [[37, 24, 21, 23, 36]],$
 $[[22, 24, 37, 36, 35]], [[24, 37, 36, 15, 33]],$
 $[[37, 24, 45, 12, 36]], [[37, 24, 29, 9, 36]],$
 $[[41, 24, 22, 31, 1]], [[24, 22, 31, 18, 45]],$
 $[[29, 24, 22, 31, 14]], [[24, 22, 31, 30, 21]],$
 $[[24, 22, 20, 34, 33]], [[24, 41, 8, 34, 33]],$
 $[[24, 21, 30, 34, 33]], [[24, 45, 12, 34, 33]],$
 $[[24, 29, 19, 17, 41]], [[24, 22, 27, 17, 41]],$
 $[[24, 45, 49, 17, 41]], [[24, 21, 30, 17, 41]],$
 $[[24, 41, 17, 15, 33]], [[24, 22, 44, 15, 33]],$
 $[[24, 21, 47, 15, 33]], [[24, 22, 44, 13, 37]],$
 $[[24, 37, 13, 11, 33]], [[45, 24, 22, 27, 12]],$
 $[[12, 45, 24, 21, 43]], [[14, 29, 24, 41, 40]],$
 $[[29, 24, 21, 47, 14]], [[41, 24, 21, 23, 40]],$

[[44, 22, 24, 21, 43]], [[19, 29, 24, 22, 35]],
 [[23, 21, 24, 22, 20]], [[8, 41, 24, 22, 35]],
 [[24, 45, 49, 11, 33]], [[41, 24, 22, 44, 40]]]

- Vrcholy v grafe: 50 vrcholov

[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18,
 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36,
 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49]

- Hrany v grafe: 175 hrán

[(0, 2), (0, 3), (0, 25), (0, 30), (0, 35), (0, 40), (0, 45), (1, 3), (1, 4),
 (1, 26), (1, 31), (1, 36), (1, 41), (1, 46), (2, 4), (2, 27), (2, 32), (2, 37),
 (2, 42), (2, 47), (3, 28), (3, 33), (3, 38), (3, 43), (3, 48), (4, 29), (4, 34),
 (4, 39), (4, 44), (4, 49), (5, 7), (5, 8), (5, 25), (5, 31), (5, 37), (5, 43),
 (5, 49), (6, 8), (6, 9), (6, 26), (6, 32), (6, 38), (6, 44), (6, 45), (7, 9),
 (7, 27), (7, 33), (7, 39), (7, 40), (7, 46), (8, 28), (8, 34), (8, 35), (8, 41),
 (8, 47), (9, 29), (9, 30), (9, 36), (9, 42), (9, 48), (10, 12), (10, 13), (10, 25),
 (10, 32), (10, 39), (10, 41), (10, 48), (11, 13), (11, 14), (11, 26), (11, 33), (11, 35),
 (11, 42), (11, 49), (12, 14), (12, 27), (12, 34), (12, 36), (12, 43), (12, 45), (13, 28),
 (13, 30), (13, 37), (13, 44), (13, 46), (14, 29), (14, 31), (14, 38), (14, 40), (14, 47),
 (15, 17), (15, 18), (15, 25), (15, 33), (15, 36), (15, 44), (15, 47), (16, 18), (16, 19),
 (16, 26), (16, 34), (16, 37), (16, 40), (16, 48), (17, 19), (17, 27), (17, 30), (17, 38),
 (17, 41), (17, 49), (18, 28), (18, 31), (18, 39), (18, 42), (18, 45), (19, 29), (19, 32), (19, 35),
 (19, 43), (19, 46), (20, 22), (20, 23), (20, 25), (20, 34), (20, 38), (20, 42), (20, 46),
 (21, 23), (21, 24), (21, 26), (21, 30), (21, 39), (21, 43), (21, 47), (22, 24), (22, 27),
 (22, 31), (22, 35), (22, 44), (22, 48), (23, 28), (23, 32), (23, 36), (23, 40), (23, 49),
 (24, 29), (24, 33), (24, 37), (24, 41), (24, 45), (25, 26), (25, 29), (26, 27), (27, 28),
 (28, 29), (30, 31), (30, 34), (31, 32), (32, 33), (33, 34), (35, 36), (35, 39), (36, 37),

$(37, 38), (38, 39), (40, 41), (40, 44), (41, 42), (42, 43), (43, 44), (45, 46), (45, 49),$
 $(46, 47), (47, 48), (48, 49)]$

- Počet grúp automorfizmov: 252000

5.2 Generovanie incidenčných matíc, grúp automorfizmov zo zadaného zoznamu susedností

5.2.1 cage(3,11)

- Počet vrcholov v kletke: 112
- Počet hrán v kletke: 168
- Počet grúp automorfizmov: 64

5.2.2 cage(3,14)

- Počet vrcholov v kletke: 384
- Počet hrán v kletke: 576
- Počet grúp automorfizmov: 96

5.2.3 cage(3,16)

- Počet vrcholov v kletke: 960
- Počet hrán v kletke: 1440
- Počet grúp automorfizmov: 96

5.2.4 cage(3,17)

- Počet vrcholov v kletke: 2176
- Počet hrán v kletke: 3264
- Počet grúp automorfizmov: 544

5.2.5 cage(3,18)

- Počet vrcholov v kletke: 2560
- Počet hrán v kletke: 3840
- Počet grúp automorfizmov: 640

5.2.6 cage(3,20)

- Počet vrcholov v kletke: 5376
- Počet hrán v kletke: 8064
- Počet grúp automorfizmov: 2688

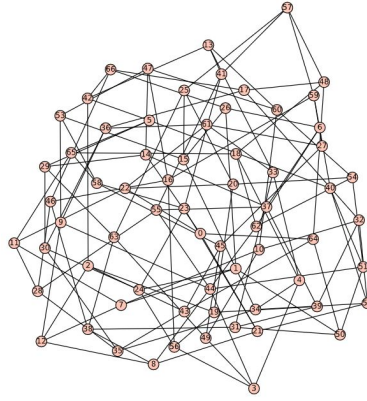
5.2.7 cage(3,23)

- Počet vrcholov v kletke: 49326
- Počet hrán v kletke: 73989
- Počet grúp automorfizmov: 1

5.2.8 $\text{cage}(3,25)$

- Počet vrcholov v kletke: 108906
- Počet hrán v kletke: 163359
- Počet grúp automorfizmov: —

5.2.9 $\text{cage}(4,7)$



Obr. 5.13: $\text{cage}(4,7)$

- Cykly formujúce kletku:
 $[[22, 11, 7, 12, 8, 21, 0]], [[22, 11, 28, 55, 37, 14, 0]],$
 $[[22, 20, 25, 63, 29, 14, 0]], [[22, 20, 54, 60, 47, 14, 0]],$
 $[[14, 29, 5, 40, 52, 21, 0]], [[12, 7, 11, 22, 20, 19, 2]],$
 $[[48, 17, 36, 61, 22, 0, 64]], [[50, 1, 7, 11, 22, 0, 64]],$
 $[[43, 45, 27, 61, 22, 0, 64]], [[50, 31, 33, 61, 22, 0, 64]],$
 $[[50, 1, 26, 66, 17, 48, 64]], [[24, 23, 21, 8, 12, 7, 1]],$
 $[[50, 51, 54, 20, 22, 0, 64]], [[26, 15, 53, 58, 23, 24, 1]],$
 $[[14, 47, 53, 15, 26, 6, 37]], [[29, 30, 24, 56, 16, 47, 14]],$
 $[[14, 29, 30, 24, 23, 21, 0]], [[48, 18, 65, 11, 22, 0, 64]],$

$[[11, 22, 20, 54, 60, 10, 7]], [[9, 12, 7, 11, 22, 61, 36]],$
 $[[43, 2, 19, 20, 22, 0, 64]], [[48, 17, 66, 42, 2, 43, 64]],$
 $[[43, 35, 28, 11, 22, 0, 64]], [[5, 42, 2, 12, 7, 11, 65]],$
 $[[42, 13, 60, 47, 14, 29, 5]], [[22, 20, 54, 62, 8, 21, 0]],$
 $[[4, 3, 44, 51, 50, 31, 33]], [[50, 51, 44, 3, 56, 24, 1]],$
 $[[24, 56, 3, 49, 10, 7, 1]], [[56, 24, 23, 58, 45, 49, 3]],$
 $[[49, 63, 29, 14, 47, 60, 10]], [[11, 22, 61, 33, 4, 18, 65]],$
 $[[4, 18, 62, 8, 21, 52, 34]], [[50, 51, 44, 9, 12, 7, 1]],$
 $[[14, 47, 53, 9, 44, 55, 37]], [[14, 47, 16, 56, 19, 39, 37]],$
 $[[22, 61, 27, 6, 37, 14, 0]], [[11, 22, 20, 54, 62, 18, 65]],$
 $[[29, 14, 47, 16, 59, 40, 5]], [[22, 11, 65, 5, 29, 14, 0]],$
 $[[50, 51, 40, 52, 21, 0, 64]], [[14, 37, 39, 32, 52, 21, 0]],$
 $[[11, 22, 61, 27, 45, 58, 65]], [[22, 20, 19, 39, 37, 14, 0]],$
 $[[27, 61, 22, 20, 54, 62, 6]], [[14, 29, 63, 38, 8, 21, 0]],$
 $[[10, 60, 47, 14, 37, 39, 32]], [[9, 53, 47, 14, 29, 30, 36]],$
 $[[14, 47, 53, 58, 23, 21, 0]], [[29, 63, 25, 15, 53, 47, 14]],$
 $[[13, 60, 54, 20, 22, 61, 33]], [[63, 29, 14, 47, 16, 46, 38]],$
 $[[48, 17, 32, 52, 21, 0, 64]], [[35, 30, 24, 23, 21, 52, 34]],$
 $[[28, 11, 22, 61, 36, 30, 35]], [[14, 47, 16, 46, 28, 55, 37]],$
 $[[14, 47, 60, 13, 41, 55, 37]], [[14, 37, 55, 41, 23, 21, 0]],$
 $[[48, 57, 41, 23, 21, 0, 64]], [[15, 53, 58, 23, 21, 52, 34]],$
 $[[27, 61, 22, 20, 25, 57, 59]], [[22, 61, 36, 30, 29, 14, 0]],$
 $[[14, 47, 16, 59, 27, 6, 37]], [[48, 57, 25, 20, 22, 0, 64]],$
 $[[26, 66, 46, 16, 56, 24, 1]], [[31, 39, 19, 20, 22, 61, 33]],$
 $[[22, 11, 65, 58, 23, 21, 0]], [[14, 29, 63, 38, 31, 39, 37]]]$

- Vrcholy v kletke: 67 vrcholov

$[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17,$

18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34,
 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52,
 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66]

- Hrany v kletke: 134 hrán

$[(0, 14), (0, 21), (0, 22), (0, 64), (1, 7), (1, 24), (1, 26), (1, 50), (2, 12),$
 $(2, 19), (2, 42), (2, 43), (3, 4), (3, 44), (3, 49), (3, 56), (4, 18), (4, 33),$
 $(4, 34), (5, 29), (5, 40), (5, 42), (5, 65), (6, 26), (6, 27), (6, 37), (6, 62),$
 $(7, 10), (7, 11), (7, 12), (8, 12), (8, 21), (8, 38), (8, 62), (9, 12), (9, 36),$
 $(9, 44), (9, 53), (10, 32), (10, 49), (10, 60), (11, 22), (11, 28), (11, 65), (13, 33),$
 $(13, 41), (13, 42), (13, 60), (14, 29), (14, 37), (14, 47), (15, 25), (15, 26), (15, 34),$
 $(15, 53), (16, 46), (16, 47), (16, 56), (16, 59), (17, 32), (17, 36), (17, 48), (17, 66),$
 $(18, 48), (18, 62), (18, 65), (19, 20), (19, 39), (19, 56), (20, 22), (20, 25), (20, 54),$
 $(21, 23), (21, 52), (22, 61), (23, 24), (23, 41), (23, 58), (24, 30), (24, 56), (25, 57),$
 $(25, 63), (26, 66), (27, 45), (27, 59), (27, 61), (28, 35), (28, 46), (28, 55), (29, 30),$
 $(29, 63), (30, 35), (30, 36), (31, 33), (31, 38), (31, 39), (31, 50), (32, 39), (32, 52),$
 $(33, 61), (34, 35), (34, 52), (35, 43), (36, 61), (37, 39), (37, 55), (38, 46),$
 $(38, 63), (40, 51), (40, 52), (40, 59), (41, 55), (41, 57), (42, 66), (43, 45), (43, 64),$
 $(44, 51), (44, 55), (45, 49), (45, 58), (46, 66), (47, 53), (47, 60), (48, 57), (48, 64),$
 $(49, 63), (50, 51), (50, 64), (51, 54), (53, 58), (54, 60), (54, 62), (57, 59), (58, 65)]$

- Počet grúp automorfizmov: 4

5.2.10 cage(4,9)

- Počet vrcholov v kletke: 270
- Počet hrán v kletke: 540
- Počet grúp automorfizmov: 90

5.2.11 cage(4,10)

- Počet vrcholov v kletke: 384
- Počet hrán v kletke: 768
- Počet grúp automorfizmov: 768

5.2.12 cage(5,10)

- Počet vrcholov v kletke: 1296
- Počet hrán v kletke: 3240
- Počet grúp automorfizmov: 3888

5.2.13 cage(7,7)

- Počet vrcholov v kletke: 640
- Počet hrán v kletke: 2240
- Počet grúp automorfizmov: 320

5.2.14 cage(7,8)

- Počet vrcholov v kletke: 672
- Počet hrán v kletke: 2352
- Počet grúp automorfizmov: 14112

5.2.15 cage(10,5)

- Počet vrcholov v kletke: 124
- Počet hrán v kletke: 620
- Počet grúp automorfizmov: 1

5.2.16 cage(11,5)

- Počet vrcholov v kletke: 154
- Počet hrán v kletke: 847
- Počet grúp automorfizmov: 1

5.2.17 cage(12,5)

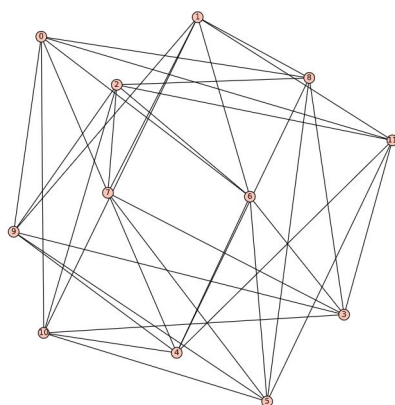
- Počet vrcholov v kletke: 203
- Počet hrán v kletke: 1218
- Počet grúp automorfizmov: 203

5.2.18 cage(13,5)

- Počet vrcholov v kletke: 230
- Počet hrán v kletke: 1495
- Počet grúp automorfizmov: 1

5.3 Generovanie kletky a následne incidenčných matíc, grúp automorfizmov

5.3.1 $\text{cage}(6,4)$



Obr. 5.14: $\text{cage}(6,4)$

- Cykly formujúce kletku:

[[[7, 3, 10, 0]], [[9, 5, 10, 0]], [[7, 3, 8, 0]], [[9, 2, 11, 0]], [[7, 1, 11, 0]], [[8, 1, 9, 0]],
 [[7, 1, 8, 0]], [[7, 1, 10, 0]], [[6, 1, 11, 0]], [[6, 2, 8, 0]], [[7, 2, 11, 0]], [[6, 4, 11, 0]],
 [[8, 2, 10, 0]], [[8, 2, 11, 0]], [[6, 3, 9, 0]], [[6, 5, 7, 0]], [[8, 5, 9, 0]], [[6, 3, 8, 0]],
 [[6, 3, 11, 0]], [[6, 4, 7, 0]], [[6, 4, 9, 0]], [[8, 4, 9, 0]], [[7, 4, 10, 0]], [[10, 5, 11, 0]],
 [[7, 5, 11, 0]]]

- Vrcholy v kletke: 12 vrcholov

[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11]

- Hrany v kletke: 36 hrán

[(0, 6), (0, 7), (0, 8), (0, 9), (0, 10), (0, 11), (1, 6), (1, 7), (1, 8),
 (1, 9), (1, 10), (1, 11), (2, 6), (2, 7), (2, 8), (2, 9), (2, 10), (2, 11), (3, 6),

(3, 7), (3, 8), (3, 9), (3, 10), (3, 11), (4, 6), (4, 7), (4, 8), (4, 9),
 (4, 10), (4, 11), (5, 6), (5, 7), (5, 8), (5, 9), (5, 10), (5, 11)]

- Počet grúp automorfizmov: 1036800
- Incidenčná matica:

```
[1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1]
[1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0]
[0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 0]
[0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 1 0]
[0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0]
[0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0]
[0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0]
[0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0]
[0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1]
```

Obr. 5.15: Incidenčná matica kletky $cage(6, 4)$

5.4 Vyhodnotenie výsledkov generovania incidenčných matíc z kliebok a grúp automorfizmov

V nasledovnej tabuľke si zobrazíme dosiahnuté výsledky a porovnáme ich s vypočítaným Moorovým ohraňčením pre povolený počet vrcholov

cage(k,g)	M(k,g)	Počet vrcho- lov	Počet hrán	Rozmer matice	Grupy auto- morfiz- mov
cage(3,5)	10	10	15	10×15	120
cage(3,6)	14	14	21	14×21	336
cage(3,7)	22	24	36	24×36	32
cage(3,8)	30	30	45	30×45	1440
cage(3,10)	62	70	105	70×105	80
cage(3,11)	94	112	168	112×168	64
cage(3,14)	254	384	576	384×576	96
cage(3,16)	510	960	1440	960×1440	96
cage(3,17)	766	2176	3264	2176×3264	544
cage(3,18)	1022	2560	3840	2560×3840	640
cage(3,20)	2046	5376	8064	5376×8064	2688
cage(3,23)	6142	49326	73989	49326×73989	1
cage(3,25)	12286	108906	163359	108906×163359	-
cage(4,5)	17	19	38	19×38	24
cage(4,7)	53	67	134	67×134	4
cage(4,9)	161	270	540	270×540	90
cage(4,10)	242	384	768	384×768	768
cage(5,10)	682	1296	3240	1296×3240	3888
cage(6,4)	12	12	36	12×36	1036800
cage(7,5)	50	50	175	50×175	252000
cage(7,7)	302	640	2240	640×2240	320
cage(7,8)	518	672	2352	672×2352	14112
cage(10,5)	101	124	620	124×620	1
cage(11,5)	122	154	847	154×847	1
cage(12,5)	145	203	1218	203×1218	203
cage(13,5)	170	230	1495	230×1495	1

Tabuľka 5.1: Tabuľka overenia dosiahnutých výsledkov

Vo všetkých prípadoch bola splnená podmienka Moorovho ohraničenia zaručujúca existenciu uvažovaných kliebok. Vo všetkých prípadoch sa nám

podarilo zistiť vrcholy, hrany, rozmer incidenčnej matice ako aj incidenčnú maticu spolu s grupami automorfizmov. Správnosť počtu grúp automorfizmov sme overili aj pomocou teórie, kde je tento údaj pre uvažované kliecky známy ako aj údaj o počte vrcholov. Dalším krokom bude preskúmať prepojenie incidenčných matíc a lineárnych LDPC kódov ako aj proces samotného kódovania.

5.5 Experimentálne Generovanie incidenčných matíc

5.5.1 Generovanie Incidenčnej matice, ktorej výsledkom bude $\text{cage}(6,4)$

Pokus č. 1

- Parametre: počet vrcholov = 12,
počet hrán = 36, stupeň vrcholov $k = 6$
- Výsledná incidenčná matica:

[illegible]

Obr. 5.16: Experimentálne vygenerovaná incidenčná matica 1 $cage(6, 4)$

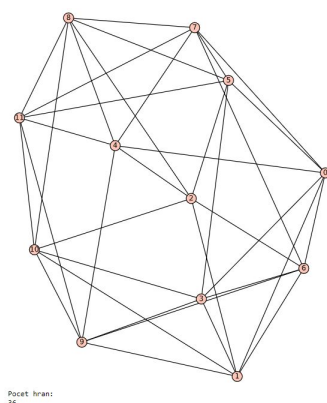
-

Obr. 5.17: Experimentálne vygenerovaný graf 1 $cage(6, 4)$

- Parametre: počet vrcholov = 12,
počet hrán = 36, stupeň vrcholov $k = 6$
- Výsledná incidenčná matica:

[illegible]

- Graf z experimentálnej incidenčnej matice s kontrolou počtu hrán:

Obr. 5.19: Experimentálne vygenerovaný graf 2 $cage(6, 4)$

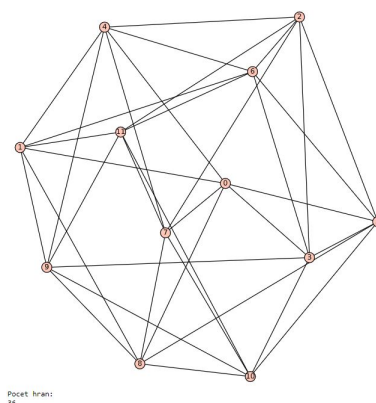
Pokus č. 3

- Parametre: počet vrcholov = 12,
počet hrán = 36, stupeň vrcholov $k = 6$
- Výsledná incidenčná matica:

```
[0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 1 0 0 0 1 1 1 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 1 0 0 0 0 1 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 1 0 0 0 0 1 0]
[0 0 1 0 0 1 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0]
[0 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 1 0 1 1 0 0 0]
[0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0]
[0 1 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1]
[1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0]
```

Obr. 5.20: Experimentálne vygenerovaná incidenčná matica 3 $cage(6, 4)$

- Graf z experimentálnej incidenčnej matice s kontrolou počtu hrán:

Obr. 5.21: Experimentálne vygenerovaný graf 3 $cage(6, 4)$

5.6 Vyhodnotenie výsledkov experimentálneho generovania incidenčných matíc

Vo všetkých prípadoch sa nám nepodarilo vygenerovať incidenčnú maticu kletky $cage(6, 4)$ nakoľko z obrázkov pri vizuálnej kontrole môžeme vidieť, že graf neobsahuje iba cykly dĺžky 4. Incidenčnú maticu sa nám síce podarilo vygenerovať, ale správne dĺžky cyklov nie sú zachované. Okrem toho, že už takýto spôsob generovania incidenčných matíc je príliš výpočtovo náročný, pomocou náhodného generovania je veľmi obtiažne dostať sa k želanému výsledku. Z tohto dôvodu je potrebné pre problematiku opačného generovania zvoliť iný postup, alebo sa zamerať na niektoré také skupiny kletiek, ktoré sa generujú rovnakým, poprípade podobným spôsobom na základe informácií, ktoré sú už o nich známe.

Kapitola 6

Záver

xxxxxxx

Literatúra

- [CoC] Cocalc.
- [EJ13] Geoffrey Exoo and Robert Jajcay. Dynamic cage survey. 2013.
- [Exo] Geoffrey Exoo. Regular graphs of given degree and girth.
<http://cs.indstate.edu/ge/CAGES/index.html>.
- [HP03] W Cary Huffman and Vera Pless. *Fundamentals of error-correcting codes*. Cambridge Univ. Press, Cambridge, 2003.
- [Mal07] Gabofestwe Alafang Malema. *Low-Density Parity-Check Codes: Construction and Implementation*. School of Electrical and Electronic Engineering, Faculty of Engineering, Computer and Mathematical Sciences The University of Adelaide, Australia, 2007.
- [MTSB13] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S. L. M. Barreto. Mdpc-mceliece: New mceliece variants from moderate density parity-check codes. In *ISIT*, pages 2069–2073. IEEE, 2013.
- [The] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version x.y.z)*. <https://www.sagemath.org>.

Zoznam obrázkov

3.1	Vztah medzi grafom a maticou [Mal07]	5
3.2	Petersenov graf [EJ13]	8
3.3	Heawoodov graf [EJ13]	8
3.4	McGeeho graf [EJ13]	9
3.5	Tutte-Coxeterov graf [EJ13]	9
3.6	Robertsonov graf [EJ13]	10
5.1	Petersenov graf [The]	15
5.2	Incidenčná matica Petersenovho grafu	16
5.3	Heawoodov graf [The]	17
5.4	Incidenčná matica Heawoodovho grafu	18
5.5	McGeeho graf[The]	18
5.6	Incidenčná matica McGeeho grafu	19
5.7	Tutte-Coxeterov graf [The]	20
5.8	Incidenčná matica Tutte - Coxeterovho grafu	21
5.9	Balabanov(10) graf[The]	21
5.10	Robertsonov graf [The]	23
5.11	Incidenčná matica Robertsonovho grafu	25
5.12	Hoffman - Singletonov graf [The]	25
5.13	$cage(4, 7)$	31

5.14	$cage(6, 4)$	36
5.15	Incidenčná matica kletky $cage(6, 4)$	37
5.16	Experimentálne vygenerovaná incidenčná matica 1 $cage(6, 4)$.	39
5.17	Experimentálne vygenerovaný graf 1 $cage(6, 4)$	40
5.18	Experimentálne vygenerovaná incidenčná matica 2 $cage(6, 4)$.	40
5.19	Experimentálne vygenerovaný graf 2 $cage(6, 4)$	41
5.20	Experimentálne vygenerovaná incidenčná matica 3 $cage(6, 4)$.	41
5.21	Experimentálne vygenerovaný graf 3 $cage(6, 4)$	42