SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Evidenčné číslo: FEI-5382-80288

HUSTOTA INVERZIÍ RIEDKYCH CYKLICKÝCH MATÍC

BAKALÁRSKA PRÁCA

2018 **Branislav Boráň**

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Evidenčné číslo: FEI-5382-80288

HUSTOTA INVERZIÍ RIEDKYCH CYKLICKÝCH MATÍC

BAKALÁRSKA PRÁCA

Študijný program :	Aplikovaná informatika
Číslo študijného odboru:	2511
Názov študijného odboru:	9.2.9 Aplikovaná informatika
Školiace pracovisko:	Ústav informatiky a matematiky
Vedúci záverečnej práce:	Mgr. Tomáš Fabšič, PhD.

2018 **Branislav Boráň**

Slovenská technická univerzita v Bratislave
Ústav informatiky a matematiky

Fakulta elektrotechniky a informatiky
Akademický rok: 2017/2018
Evidenčné číslo: FEI-5382-80288

STU FEI

ZADANIE BAKALÁRSKEJ PRÁCE

Študent:	**Branislav Boráň**
ID študenta:	80288
Študijný program:	aplikovaná informatika
Študijný odbor:	9.2.9. aplikovaná informatika
Vedúci práce:	Mgr. Tomáš Fabšič, PhD.
Miesto vypracovania:	ÚIM

Názov práce: **Hustota inverzií riedkych cyklických matíc**

Jazyk, v ktorom sa práca vypracuje: slovenský jazyk

Špecifikácia zadania:

Medzi kandidátmi pre postkvantovú kryptografiu figurujú aj QC-MDPC McElieceov kryptosystém a QC-LDPC McElieceov kryptosystém. Významnú úlohu v týchto kryptosystémoch hrajú cyklické matice s nízkym počtom jednotiek v riadku. Takéto matice nazývame riedke cyklické matice. Okrem nich sa v spomínaných kryptosystémoch využívajú aj inverzné matice k riedkym cyklickým maticiam. Cieľom práce je vytvoriť program na generovanie a invertovanie riedkych cyklických matíc a následne skúmať, aký je počet jednotiek v inverzných maticiach k riedkym cyklickým maticiam. Nízky počet jednotiek v inverzných maticiach by totiž ohrozoval bezpečnosť spomínaných kryptosystémov.

Úlohy:
1. Naštudujte si, ako sa využívajú riedke cyklické matice v QC-MDPC McElieceovom kryptosystéme.
2. Vytvorte program na generovanie a invertovanie riedkych cyklických matíc.
3. Pomocou programu skúmajte, aký je počet jednotiek v inverzných maticiach k riedkym cyklickým maticiam.
4. Vyhodnoťte výsledky.

Zoznam odbornej literatúry:

1. Misoczki R., Tillich J-P., Sendrier N., Barreto P.S.L.M.: MDPC-McEliece: new McEliece variants from moderate density parity-check codes. In: IEEE International Symposium on Information Theory (ISIT'2013), pp. 2069-2073. Istanbul (2013)

Riešenie zadania práce od: 18. 09. 2017

Dátum odovzdania práce: 11. 05. 2018

Branislav Boráň
študent

prof. RNDr. Otokar Grošek, PhD.
vedúci pracoviska

prof. Dr. Ing. Miloš Oravec
garant študijného programu

SÚHRN

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Študijný program :	Aplikovaná informatika
Vyberte typ práce	Bakalárska práca
Autor:	Branislav Boráň
Vedúci záverečnej práce:	Mgr. Tomáš Fabšič, PhD.
Miesto a rok predloženia práce:	Bratislava 2018

V našej práci popisujeme lineárny kód, cyklické matice a ich využitie v QcMDPC McElieceovom kryptosystéme. Cieľom našej práce je skúmať hustotu inverzných matíc k riedkym cyklickým maticiam. Skúmame Hammingové váhy vektorov veľkosti 101, ktoré reprezentujú prvé riadky cyklických matíc v 4 experimentoch na základe vytvorených programov. V experimente číslo 1 skúmame hustoty náhodne generovaných matíc, ktorých prvé riadky majú ľubovoľnú Hammingovú váhu. V experimente číslo 2 skúmame hustoty náhodne generovaných invertovateľných matíc, ktorých prvé riadky majú ľubovoľnú Hammingovú váhu. V experimente číslo 3 skúmame a porovnávame hustoty inverzných cyklických matíc, ktoré vznikli z náhodne generovaných invertovateľných matíc a prvé riadky náhodne generovaných invertovateľných matíc majú danú nepárnu nízku Hammingovú váhu. V experimente číslo 4 skúmame a porovnávame hustoty takých cyklických matíc, ktoré už predstavujú samotné bloky generujúceich matíc lineárneho kódu v QC MDPC McElieceovom kryptosystéme. Nízke hustoty generujúcich matíc by mohli znamenať bezpečnostné riziko pre QC MDPC McElieceov kryptosystém.

Kľúčové slová: Cyklická matica, QC MDPC McElieceov kryptosystém, Hammingová váha vektora

ABSTRACT

SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA

FACULTY OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGY

Study Programme:	Applied Informatics
Bachelor Thesis:	Density of inverses of sparse circulant matrices
Autor:	Branislav Boráň
Supervisor:	Mgr. Tomáš Fabšič, PhD.
Place and year of submission:	Bratislava 2018

We describe the linear code, Hamming weights of vectors, cyclic matrices and their use in the McEliece cryptosystem in our work. The aim of our work is to investigate the density of inverse circulant matrices to sparse circulant matrices. We examine Hamming weights of vectors of size 101 that represent the first rows of cyclic matrices in 4 experiments based on the programs created. In Experiment number 1, we investigate densities of randomly generated matrices, the first rows of which have any Hamming weight. In Experiment number 2, we investigate densities of randomly generated invertible matrices whose first rows have any Hamming weight. In Experiment number 3, we investigate and compare the density of inverse cyclic matrices that originated from randomly generated invertible matrices, and the first rows of randomly generated invertible matrices have a given odd Hamming weight. In Experiment Number 4 we investigate and compare the densities of such cyclic matrices, which are already the blocks in generator matrices of the linear codes in the QC MDPC McEliece cryptosystem. Low density generating matrices could pose a safety risk for the QC MDPC McEliece cryptosystem.

Key words: Circulant matrix, QC MDPC McEliece cryptosystem, Hamming weight

Vyhlásenie autora

Podpísaný Branislav Boráň čestne vyhlasujem, že som Bakalársku prácu Hustota inverzií riedkych cyklických matíc vypracoval na základe poznatkov získaných počas štúdia a informácií z dostupnej literatúry uvedenej v práci.

Uvedenú prácu som vypracoval pod vedením Mgr. Tomáša Fabšiča.

V Bratislave dňa 01.06.2018

Boráň

.....

podpis autora

Poďakovanie

Chcel by som sa poďakovať svojmu vedúcemu práce Mgr. Tomášovi Fabšičovi, PhD. za odbornú pomoc a usmernenie pri písaní tejto práce, za materiály cenné rady, veľké množstvo informácií a za ochotu. V neposlednom rade by som sa chcel poďakovať aj svojej rodine a priateľom, ktorí ma celý čas podporovali.

Obsah

Zoznam obrázkov a tabuliek

Zoznam obrázkov:

Zoznam tabuliek:

Zoznam skratiek a značiek

č. – číslo

HW – hammingová váha vektora

HD – hammingová vzdialenosť

n – dĺžka vektora

k – pevná hammingová váha

E – stredná hodnota

D – rozptyl

S – smerodajná odchýlka

F – pole

G – generujúca matica lineárneho kódu

H – kontrolná matica lineárneho kódu

C – lineárny kód

LDPC kódy – low density parity check kódy

MDPC kódy - moderate density parity check code

QC- kvázicyklický

Úvod

Kryptosystémy delíme na symetrické a asymetrické. Symetrické kryptosystémy patria medzi historicky staršie. Na zašifrovanie správy v symetrických kryptosystémoch je možné použiť rovnaký kľúč ako k jej dešifrovaniu. Asymetrické kryptosystémy sa objavujú o niečo neskôr. Na zašifrovanie a dešifrovanie správy sú v nich používané rôzne kľúče. Jeden z problémov na ktorých sú založené asymetrické kryptosystémy sú problém faktorizácie a diskrétneho logaritmu. Použitím kvantového počítača by bolo možné riešiť problémy prvočíselnej faktorizácie a diskrétneho logaritmu v polynomiálnom čase. V prípade vytvorenia dostatočne výkonného kvantového počítača, už nebudú v súčasnosti používané asymetrické kryptosystémy považované za bezpečné a z tohto dôvodu sa časť výskumu v kryptografií sústreďuje na návrh nových asymetrických kryptosystémov odolných voči útokom kvantovými počítačmi. Takéto kryptosystémy musia byť založené na matematických problémoch, ktoré nie je možné efektívne riešiť ani pomocou kvantového počítača. Prvý asymetrický kryptosystém založený na probléme dekódovania náhodného lineárneho kódu je McElieceov kryptosystém. Jeho autorom je R. J. McEliece a do dnešného dňa nebol prelomený. QC MDPC McElieceov kryptosystém sa javí ako možná náhrada tohto problému. V kryptosystéme vystupujú cyklické matice, ktoré budeme v tejto práci skúmať. Našim cieľom bude skúmať hustotu inverzných matíc k riedkym cyklickým maticiam. Nízka hustota takých matíc by mohla znamenať bezpečnostné riziko pre QC-MDPC.(3)

1 Analýza problému

1.1 Lineárny kód

Lineárny kód (n, k) je k-rozmerný lineárny podpriestor priestoru F_2^n. F_2^n je priestor **n** – rozmerných vektorov, kde koordináty berieme z poľa F_2. K - rozmerný lineárny podpriestor obsahuje práve k lineárne nezávislých vektorov. (3) Ak by sme zobrali **k** takých vektorov, potom tieto vektory generujú daný k – rozmerný podpriestor a hovoríme, že tvoria bázu podpriestoru.(4,5)

1.1.1 Generujúca matica lineárneho kódu (G)

Generujúca matica lineárneho kódu je zostrojená z bázy lineárneho kódu tak, že riadky matice predstavujú prvky bázy. Riadky generujúcej matice sú lineárne nezávislé.(4,5)

Nech m je vstup, teda nekódované slovo, v je výstup, teda kódované slovo, C je označenie lineárneho kódu, G je označenie pre generujúcu maticu lineárneho kódu, potom platí:

$$C = \{m \times G: m \in F_2^k\} \quad (3)$$

Príklad: m = (1 0 0 0)

$$G = \begin{pmatrix} 0\,0\,0\,1\,1 \\ 0\,0\,1\,0\,1 \\ 0\,1\,0\,0\,1 \\ 1\,0\,0\,0\,1 \end{pmatrix}$$

$$m \times G = (0\ 0\ 0\ 1\ 1) = v$$

1.1.2 Kontrolná matica lineárneho kódu (H)

Ak máme k-rozmerný kód C v F_2^n potom existuje n-k lineárne nezávislých vektorov v F_2^n 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.(4,5)

Ľubovoľný vektor **v** je kódovým slovom práve vtedy, ak platí:

$$H \times v^T = 0^T$$

$$C = \{v \in F_2^n : Hv^T = 0\} \quad (3)$$

Príklad: H = (1 1 1 1 1)

$$v^T = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$H \times v^t = 0$$

1.1.3 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. Hlavnou nevýhodou väčšiny LDPC kódov je vysoká časová náročnosť ich kódovacieho algoritmu.(3) Kódy majú veľmi riedku kontrolnú maticu, pomocou ktorej sa dajú opraviť chyby v kódových slovách, ich kontrolná matica obsahuje menej ako 1% jednotiek.(5)

1.1.4 MDPC kódy

MDPC kódy (z angl. moderate density parity check code) sú lineárne samoopravné kódy, ktorých kontrolná matica môže byť trochu hustejšia(2%) ako pri LDPC kódoch.(5)

1.1.5 Hammingová vzdialenosť (HD)

Hammingová vzdialenosť 2 vektorov v ∈ F_2^n a u ∈ F_2^n je počet koordinátov, na ktorých sa vektor u a v líšia. (4,5)

Príklad: máme 2 zakódované slová:

u = (0101001101) v = (1001000110)

HD(u,v) = 1 + 1 + 0 + 0 + 0 + 0 + 1 + 0 + 1 +1 = 5

1.1.6 Hammingová váha (HW)

Hammingová váha jedného vektora v ∈ F_2^n vyjadruje počet jednotiek vektora v. (4,5)

Príklad: máme zakódované slovo:

v = (0101001101)

Hw(v) = 1 + 1 + 1 + 1 + 1 =5 Všeobecne platí: HD(u,v) = Hw(u + v)

1.1.7 Cyklická matica

Cyklická alebo Cirkulantná matica je štvorcová matica, ktorú možno vytvoriť z ľubovoľného náhodného vektora dĺžky n s HW k.

$$\begin{pmatrix} C_0 & C_1 & C_2 & \dots & \dots & \dots & C_{p-1} \\ C_{p-1} & C_0 & C_1 & C_2 & \dots & \dots & C_{p-2} \\ C_{p-2} & C_{p-1} & C_0 & C_1 & C_2 & \dots & C_{p-3} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ C_1 & C_2 & \dots & \dots & \dots & \dots & C_0 \end{pmatrix}$$

Obrázok 1 Cyklická matica

Prvý riadok matice je náhodný vektor dĺžky n. Každý ďalší riadok matice začína posledným prvkom predchádzajúceho riadku, kým sa nevystriedajú všetky prvky.(7)

1.1.8 Kvázicyklický kód

Lineárny kód C je kvázicyklický kód, ak existuje kontrolná matica H, ktorá má tvar $H=(H_0|H_1|...|H_{n0}^{-1})$ kde H_i sú cyklické matice.(3)

Príklad kontrolnej matice H, ktorej každý blok bude cyklický:

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{array}\right)$$

Ak sú LDPC a MDPC kódy zároveň kvázicyklické, nazývame ich QC-LDPC a QC-MDPC kódy.(5)

1.2 QC MDPC McElieceov kryptosystém

1.2.1 Popis a fungovanie QC MDPC McElieceovho kryptosystému

QC-MDPC kryptosystém je systém s verejným kľúčom (Public key system). Systém využíva 2 kľúče: verejný kľúč a súkromný kľúč. Verejný kľúč využíva na šifrovanie a súkromný kľúč na dešifrovanie. Princíp fungovania je, že si najprv vygenerujem verejný a súkromný kľúč, následne verejný kľúč zverejním. Súkromný kľúč si nechávam pre seba. Správy šifrované verejným kľúčom mi môže posielať hocikto, ale iba ja ich viem dešifrovať pomocou súkromného kľúču. (5)

1.2.2 Generovanie kľúčov v QC MDPC McElieceovom kryptosystéme

Náhodne si vygenerujeme kontrolnú maticu H, ktorá bude riedkou kvázicyklickou kontrolnou maticou pre QC-MDPC kód. Matica H bude súkromný kľúč. Verejný kľúč bude generujúca matica G popisujúca ten istý kód ako H. Chceme aby matica G bola QC (kvôli úspore pamäte).(5)

Ak $H=(H_0|H_1)$, G dostaneme ako:

$$G=(I\ |(H_1^{-1} \times H_0)^T) : \quad H \times G^T=0$$

Môžeme ľahko overiť, že platí:

$$(H_0|H_1) \times(T|H_1^{-1} \times H_0)^T = H_0 +H_1 \times H_1^{-1} \times H_0 = 2H_0 = 0$$

Maticu H nemožno zistiť z matice G. Dešifrovať viem iba pomocou riedkej matice H.(5)

Pre generujúcu maticu v QC-MDPC $G=(I\ |(H_1^{-1} \times H_0)^T)$ platí, že bloky H_0 a H_1 sú riedkymi cyklickými blokmi kontrolnej matice H. Z tohto tvrdenia vyplýva, že aj matica $(H_1^{-1} \times H_0)^T$ je cyklická. Na to aby bol QC-MDPC bezpečný by matica $(H_1^{-1} \times H_0)^T$ mala byť neodlíšiteľná od náhodnej cyklickej matice. V prípade, že má prvý riadok matice H^{-1} (vektor) malú Hammingovú váhu, tak malú Hammingovú váhu má aj prvý riadok matice $(H_1^{-1} \times H_0)^T$. V prípade nízkej Hammingovej váhy vektora matice sa $(H_1^{-1} \times H_0)^T$ líši od náhodne generovanej matice, pretože vektor náhodnej matice by mal mať približne polovičnú Hammingovú váhu.(5)

Nie je potrebné pracovať s celými maticami, ale iba s vektormi, ktoré reprezentujú prvý riadok matice. Je to z toho dôvodu, že samotná matica je tvorená cyklickými posunmi týchto vektorov a v každom riadku sa Hammingová váha nemení.(5)

1.2.3 Šifrovanie správy v QC MDPC McElieceovom kryptosystéme

Nech $e \in F_2^n$ je chybový vektor, ktorý musí mať dostatočne malú Hammingovú váhu aby sa dal odstrániť. Malé c predstavuje šifrovaný text. Správu $m \in F_2^k$ zašifrujeme na správu c nasledovne: $c = m \times G + e$(5)

1.2.4 Dešifrovanie správy v QC MDPC McElieceovom kryptosystéme

Na dešifrovanie správy použijeme dekódovací algoritmus pre MDPC kódy (algoritmus využíva maticu H) na odstránenie vektora e.(5)

1.3 Grupa, okruh a multiplikatívny rád

1.3.1 Grupa

Grupa je množina G spolu s binárnou operáciou * na G ak platia 3 vlastnosti:

1. * je asociatívna, pre všetky a, b, c z G

   $a*(b*c)=(a*b)*c$

2. Existuje identický element e v G pre všetky a z G

   $a*e = e*a=a$

3. Pre každé a z G existuje inverzný element a^{-1} z G ak platí

   $a*a^{1} = a^{-1}*a = e$

4. Pre všetky a, b z G platí a *b = b *a, potom je grupa nazývaná abelová alebo komutatívna (6)

1.3.2 Okruh

Okruh (R, +,.) je množina R, spolu s dvoma binárnymi operáciami označenými symbolmi + a . vtedy ak:

1. R je abelová grupa vzhľadom na operáciu sčítania
2. Je asociatívna- čiže$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ pre všetky a, b, c z R.

3. distribučné zákony: pre všetky a, b, c z R máme a.(b +c) = a.b + a.c a (b.c).a = b.a+ c.a

Okruh nazývame okruhom s identitou ak má multiplikatívnu identitu, čiže ak existuje element c , tak platí ac – ca = a pre všetky a z R
Okruh je nazývaný komutatívny ak . je komutatívna operácia (1,6)

V teórii okruhov je **homomorfizmus okruhov** funkciou medzi dvoma okruhmi, ktoré rešpektujú štruktúru. Ak R a S sú okruhy, potom homomorfizmus okruhov je takou funkciou f: R → S , že platí

$$f(a + b) = f(a) + f(b) \text{ pre všetky a a b} \in R$$

$$f(a \cdot b) = f(a) \cdot f(b) \text{ pre všetky a a b} \in R \qquad (6)$$

Izomorfizmus okruhov je bijektívne **homomorfné zobrazenie** z jednej algebrickej štruktúry do inej rovnakého typu. (2)

1.3.3 Multiplikatívny rád

V teórii čísel je dané celé číslo a a kladné celé číslo n, tak aby platilo gcd (a, n) = 1. Multiplikatívny rád modulo n je také najmenšie kladné celé číslo k, pre ktoré platí $a^k \equiv 1 \pmod n$. Multiplikatívny rád a modulo n je poradie a v multiplikatívnej skupine jednotiek v okruhu celých čísel modulo n. Multiplikatívny rád a modulo n označujeme $ord_n(a)$.

Poradie modulo n je zvyčajne napísané $ord_n(a)$, alebo $O_n(a)$. a a n môžu označovať aj polynómy, tak aby platilo gcd (a, n) = 1. (2,6)

2 Návrh riešenia

2.3 Spôsob invertovania cyklických matíc

Veta č.1

Zoberme do úvahy mapovanie τ, ktoré prevedie cyklickú binárnu (n × n) -maticu s prvým riadkom (c_0, c_1, c_2, ..., c_{n-1}) na polynóm $c(x) = c_0 + c_1x + c_2x^2 + \cdot\cdot + c_{n-1}x^{N-1}$. Potom je mapovanie τ izomorfizmom medzi okruhom cyklických binárnych (n × n) -matíc a okruhom $Z_2 [x] / (x^n +1)$.(8)

Nech τ je izomorfizmus. Majme cyklické matice A a B. Na základe tejto vety potom vieme povedať, že

$$\tau (A . B) = \tau (A) . \tau (B) \qquad => \qquad A . B = \tau^{-1} (\tau (A) . \tau (B))$$

Uvažujme, že matica B je inverznou maticou k matici A, potom platí:

$$\tau (A . A^{-1}) = \tau (A) . (\tau (A))^{-1}$$
$$\cancel{\tau (A)} . \tau (A^{-1}) = \cancel{\tau (A)} . (\tau (A))^{-1}$$
$$\tau (A^{-1}) = (\tau (A))^{-1}$$

Inverznú maticu A^{-1} vieme vyjadriť pomocou nasledujúceho vzťahu:

$$A^{-1} = \tau^{-1} (\tau (A))^{-1}$$

Nebude potrebné invertovať celé matice ale postačí nám prvý riadok z takýchto matíc na to aby sme určili či je daná matica invertovateľná a na zistenie inverznej matice k pôvodnej matici. (8)

Príklad:

Nech M je ľubovoľná cyklická matica rozmeru (n x n) nad poľom Z_2. Vektor v predstavuje prvý riadok takejto matice. Uvažujme pre tento príklad prvý riadok matice reprezentovaný vektorom v=(0 1 1 1 0). Z takéhoto vektora vieme získať polynóm

$p = 0*x^0 + 1*x^1 + 1*x^2 + 1* x^3 + 0*x^4 = x^3 + x^2 + x$. Keď už poznáme polynóm, dokážeme z neho zistiť inverzný polynóm pomocou rozšíreného euklidovho algoritmu. $p^{-1} \bmod x^n + 1$ existuje práve vtedy, keď $\gcd(p, x^n + 1) = 1$.

V QcMDPC sa n často volí ako prvočíslo také, že $ord_n(2) = n-1$. V takomto prípade môžeme testovať existenciu p^{-1} jednoduchšie, pretože platí Veta č. 2.
Následne už nebude problém previesť inverzný polynóm spätne na vektor, ktorý bude reprezentovať prvý riadok inverznej cyklickej matice.(8)

Veta č. 2

Nech n je prvočíslo a platí $ord_n(2) = n-1$. Každá cyklická matica C veľkosti n nad poľom Z_2 s párnym počtom jednotiek v riadku je singulárna a jej zodpovedajúci polynóm τ (C) má párnu Hammingovú váhu. Matica C je invertovateľna práve vtedy keď má jej zodpovedajúci polynóm τ (C) nepárnu hammingovú váhu, ktorá je zároveň menšia ako veľkosť samotného polynómu. (8)

2.4 Implementácia v programovacom jazyku

Experimenty vytvárame v programe Sage, ktorý je založený na programovacom jazyku Python. Zvolili sme ho, pretože ponúka veľké množstvo vopred naimplementovaných funkcií, ktoré nám podstatne uľahčia prácu. (10) Využili sme online aplikáciu CoCalc, 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. (9)

3 Všeobecný popis a výsledky experimentov

Pre všetky experimenty si zvolíme dĺžku jednotlivých vektorov, ktoré nám budú reprezentovať cyklické matice n = 101, pretože sa jedná o prvočíslo také, že platí:

$$ord_n(2) = n-1$$

Takýmto spôsobom sa často volí veľkosť bloku v QC-MDPC.(8) V niektorých experimentoch budeme meniť počet vektorov (počet opakovaní experimentu) , aby sme si overili správnosť výsledkov pre vyšší počet opakovaní experimentu a takisto budeme meniť aj nepárnu pevnú Hammingovú váhu náhodného vektora v takých experimentoch, v ktorých to bude potrebné. Nepárne Hammingové váhy budú mať hodnoty k=3, k=5 a k= 7. Hodnoty sme zvolili z toho dôvodu, aby sme zistili ako jednotlivé pevné Hammingové váhy k menia naše odhady pravdepodobnostných rozdelení.

3.4 Experiment č. 1

3.4.1 Cieľ experimentu

Nech C_1 je rovnomerne náhodne generovaná matica z priestoru všetkých binárnych cyklických matíc rozmeru n x n. Náhodná premenná X_1 predstavuje Hammingovú váhu prvého riadku cyklickej matice C_1. Cieľom experimentu je odhadnúť pravdepodobnostné rozdelenie náhodnej premennej X_1.

3.4.2 Popis experimentu

Rovnomerne náhodne si vygenerujeme vektor v_1 dĺžky n s ľubovoľnou Hammingovou váhou nad poľom Z_2 a zapamätáme si jeho Hammingovú váhu. Vektor v_1 reprezentuje prvý riadok cyklickej matice C_1. Experiment zopakujem 1000krát a 5000krát.

V grafoch skúmame odhad pravdepodobnostného rozdelenia náhodnej premennej X_1, ktorá nám znázorňuje jednotlivé Hammingové váhy náhodne generovaných vektorov v_1. Premenná X_1 bude mať binomické rozdelenie s parametrami (n,p_1), pričom $p_1 = 1/2$. Výsledky zobrazíme v 2 grafoch zvlášť pre 1000 opakovaní a 5000 opakovaní experimentu.

3.4.3 Dôležité Sage funkcie použité v experimente

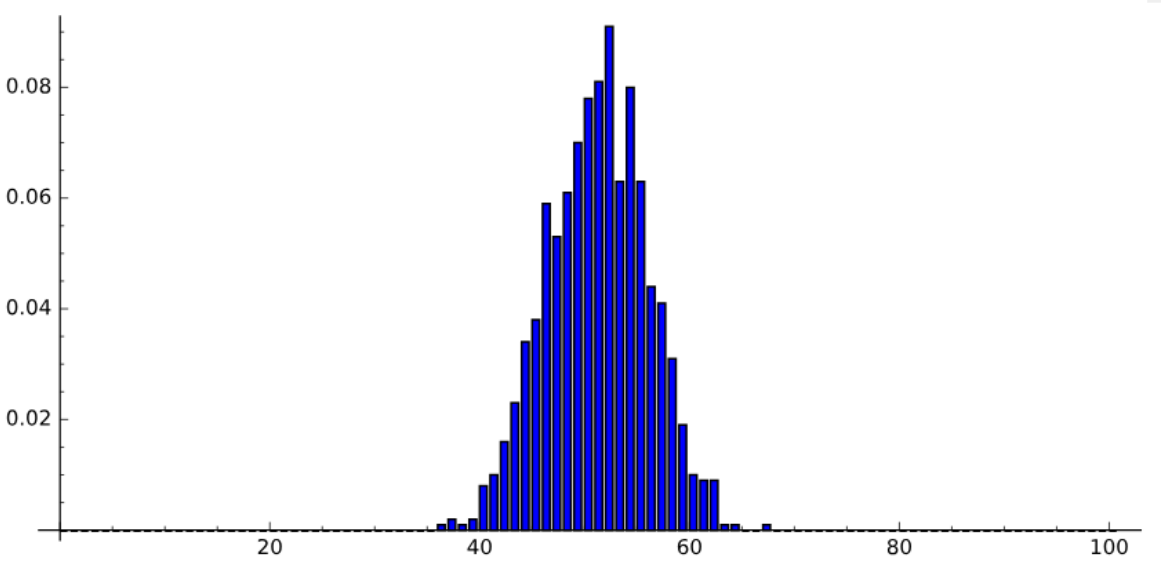
GF(2)^n a **random_element**() – vygenerujú náhodný vektor dĺžky n a naplnia ho hodnotami z poľa Z_2

hamming_weight() – vráti HW vektora

3.4.4 Vyhodnotenie výsledkov

V grafoch 1 a 2 skúmame odhad pravdepodobnostného rozdelenia náhodnej premennej X_1, ktorá nám znázorňuje jednotlivé Hammingové váhy náhodne generovaných vektorov v_1. Vektory v_1 reprezentujú prvé riadky cyklických matíc C_1. Os x predstavuje Hamingovú váhu vektorov v_1 a os y predstavuje pravdepodobnosť vygenerovania vektorov v_1 s danou Hamingovou váhou vektorov v_1.

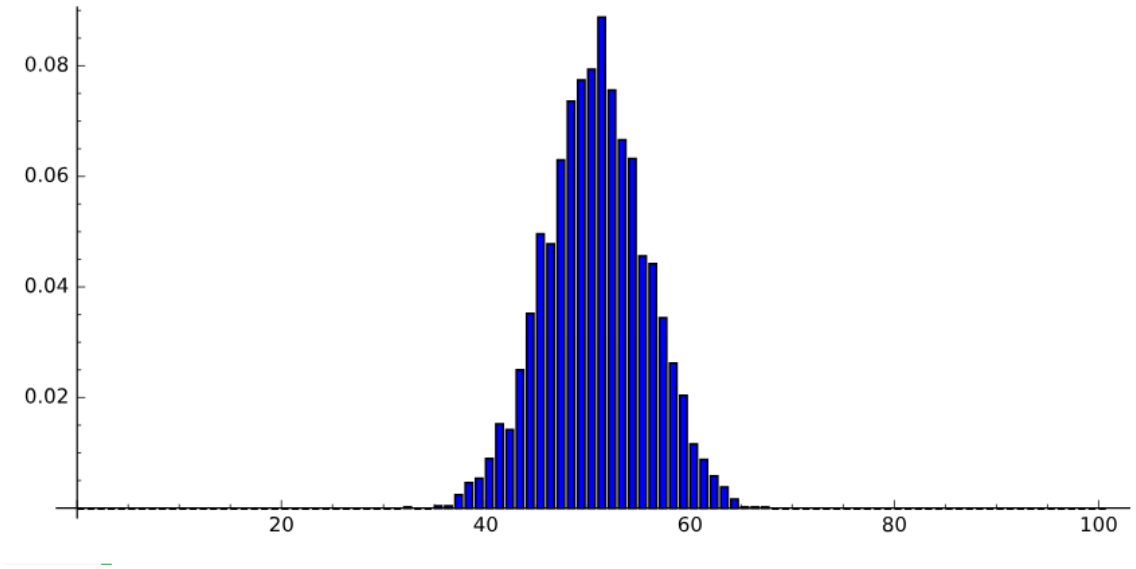
- Počet opakovaní: 1000krát



Graf 1

$E(X_1)$=50,894	**$D(X_1)$=22,81**	**$S(X_1)$=4,78**

- Počet opakovaní: 5000krát



Graf 2

E(X_1)=50,44	**D(X_1)=24,15**	**S(X_1)=4,91**

3.5 Experiment č. 2

3.5.1 Cieľ experimentu

Nech C_2 je rovnomerne náhodne generovaná matica z priestoru všetkých invertovateľných binárnych cyklických matíc rozmeru n x n. Náhodná premenná X_2 predstavuje Hammingovú váhu prvého riadku invertovateľnej cyklickej matice C_2. Cieľom experimentu je odhadnúť pravdepodobnostné rozdelenie náhodnej premennej X_2.

3.5.2 Popis experimentu

Rovnomerne náhodne si vygenerujeme vektor v_{2n} dĺžky n-1 s ľubovoľnou Hammingovou váhou nad poľom Z_2. Vektor v_{2n} reprezentuje neúplný prvý riadok neúplnej cyklickej matice C_{2n}. Zistíme si jeho Hammingovú váhu. Ak je jeho Hammingová váha párna, pridáme na koniec vektora v_{2n} číslo 1, ak je nepárna, tak pridáme na koniec vektora

v_{2n} číslo 0. Ošetríme si, aby bola Hammingová váha vektora v_2 menšia ako jeho veľkosť n. V prípade, že dostaneme vektor, kde sa jeho Hammingová váha v_2 rovná jeho veľkosti n musíme vygenerovať nový, pretože by nebol invertovateľný. Týmito krokmi sme získali úplný vektor v_2 dĺžky n, ktorý nám reprezentuje už úplný prvý riadok cyklickej matice C_2 a ošetrili sme aby boli všetky cyklické matice C_2 invertovateľné. Hammingová váha vektorov v_2 bude nepárna a menšia ako dĺžka n. Experiment opakujeme, kým nedostaneme 1000 a 5000 takýchto vektorov v_2.

V grafoch skúmame odhad pravdepodobnostného rozdelenia náhodnej premennej X_2, ktorá nám znázorňuje jednotlivé Hammingové váhy náhodne generovaných vektorov v_2, pričom vektory v_2 majú menšiu Hammingovú váhu ako je ich dĺžka n. Výsledky zobrazíme v 2 grafoch zvlášť pre 1000 a 5000 vektorov v_2.

3.5.3 Dôležité Sage funkcie použité v experimente

GF(2)^n a **random_element**() – vygenerujú náhodný vektor dĺžky n a naplnia ho hodnotami z poľa Z_2

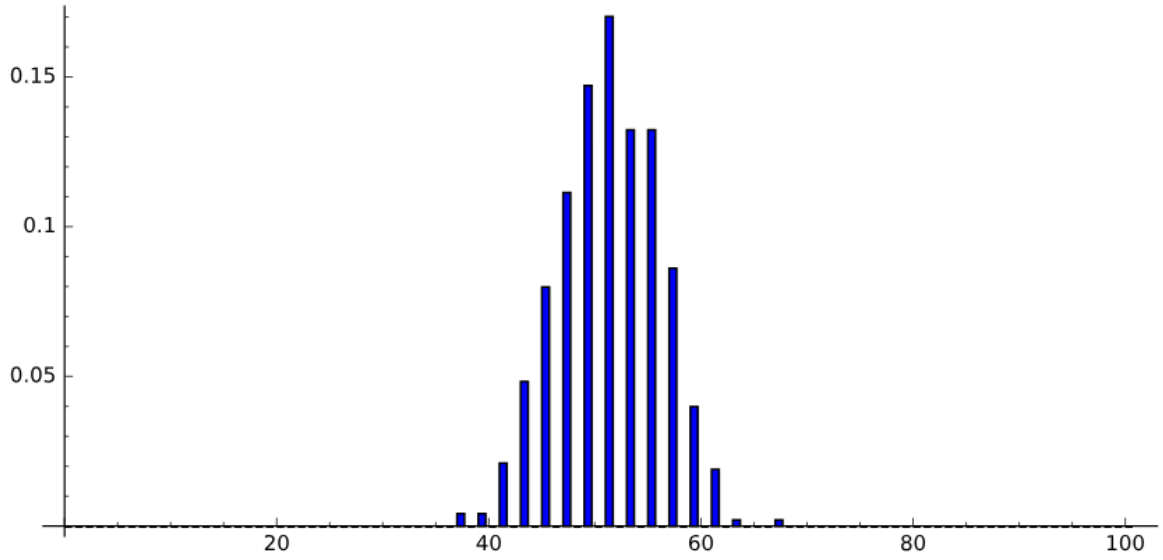
hamming_weight() – vráti HW vektora

3.5.4 Vyhodnotenie výsledkov

V grafoch 3 a 4 skúmame odhad pravdepodobnostného rozdelenia náhodnej premennej X_2, ktorá nám znázorňuje jednotlivé Hammingové váhy náhodne generovaných vektorov v_2, pričom vektory v_2 majú menšiu Hammingovú váhu ako je ich dĺžka n. Vektory v_2 reprezentujú prvé riadky cyklických matíc C_2. Os x predstavuje Hamingovú

váhu vektorov v_2 a os y predstavuje pravdepodobnosť vygenerovania náhodných vektorov v_2 s danou Hammingovou váhou menšou ako je ich dĺžka n.

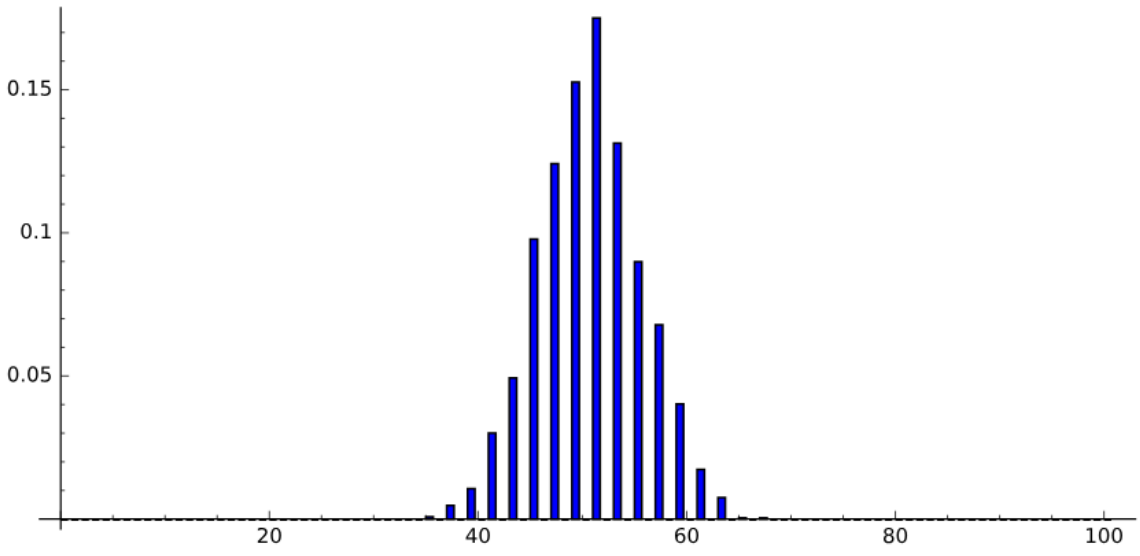
- Počet opakovaní: 1000krát



Graf 3

$E(X_2)=50,95$	**$D(X_2)=22,89$**	**$S(X_2)=4,78$**

- Počet opakovaní: 5000krát



Graf 4

$E(X_2)=50,34$	**$D(X_2)=24,46$**	**$S(X_2)=4,95$**

Grafy 3 a 4 sú takisto referenčné grafy. Budeme ich porovnávať s grafmi nasledujúcich experimentov.

3.6 Experiment č. 3

3.6.1 Cieľ experimentu

Nech C_3 je rovnomerne náhodne generovaná matica z priestoru všetkých binárnych cyklických matíc rozmeru n x n s Hammingovou váhou k. Nech C_3^{-1} je inverzná cyklická matica k matici C_3. Náhodná premenná $X_{3,k}$ predstavuje Hammingovú váhu prvého riadku inverznej cyklickej matice C_3^{-1}. Cieľom experimentu je odhadnúť pravdepodobnostné rozdelenie náhodnej premennej $X_{3,k}$.

3.6.2 Popis experimentu

Nech k je pevná nepárna Hammingová váha a n dĺžka vektora v_3, ktorý sa má vygenerovať.

Vektor a_1 je vektor samých jednotiek dĺžky k nad poľom Z_2. Vektor b_1 je vektor samých núl veľkosti n-k nad poľom Z_2. Vektory a_1 a b_1 spojíme do jedného vektora, ktorý následne pomocou funkcie numpy.random.shuffle() náhodne permutujeme a dostaneme rovnomerne náhodne vygenerovaný vektor v_3 dĺžky n s pevnou Hammingovou váhou k nad poľom Z_2, ktorý reprezentuje prvý riadok cyklickej matice C_3. Nech q_1 je polynóm, ktorý nám reprezentuje náhodný vektor v_3. Keďže vektor v_3 má nepárnu Hammingovú váhu, ktorá je menšia ako n, môžeme povedať, že jeho polynóm q_1 je invertovateľný. Vektor v_3 prevedieme na polynóm q_1, takým spôsobom, že indexy jednotiek náhodného vektora budú predstavovať exponenty jednotlivých členov polynómu. Pomocou funkcie na rozšírený euklidov algoritmus vieme zistiť inverzný polynóm q_1^{-1}. Funkcia nám vráti vektor r_1 s tromi prvkami. Ak sa na prvej pozícií vektora r nachádza číslo 1, tak na druhej pozícií vektora r_1 je inverzný polynóm q_1^{-1} . Inverzný polynóm q_1^{-1}si následne prevedieme napäť na vektor v_3^{-1}, ktorý nám bude reprezentovať prvý riadok inverznej cyklickej matice C_3^{-1}. Experiment zopakujeme 1000krát pre k=3, k=5, k=7 a aj 5000krát pre k=3, k=5, k=7. V grafoch skúmame odhad pravdepodobnostného rozdelenia náhodnej premennej $X_{3,k}$, ktorá nám znázorňuje jednotlivé Hammingové váhy vektorov v_3^{-1}. Výsledky zobrazíme v 6 grafoch zvlášť pre 1000 a 5000 vektorov v_3^{-1} a rôzne k.

3.6.3 Dôležité Sage funkcie použité v experimente

vector(GF(2), []) -inicializácia prázdneho vektora v poli Z_p

hamming_weight() – vráti HW vektora

numpy.random.shuffle(v) –premutácia prvkov vektora v

R.<x> = PolynomialRing(GF(2)) – inicializácia okruhu polynómov nad poľom Z_2

R(list(v)) – prevedie vektor na polynóm

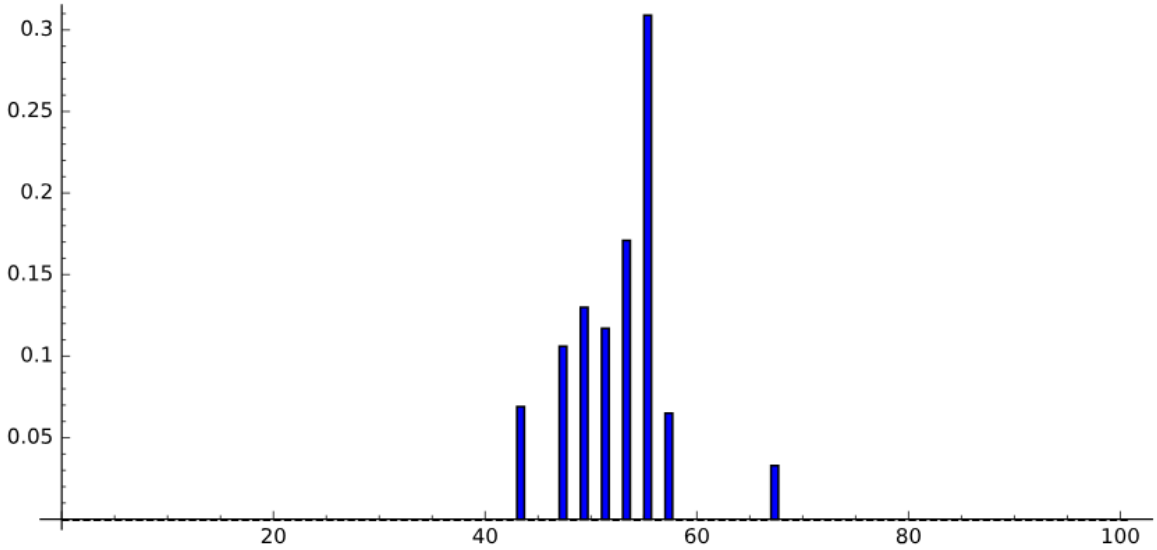
xgcd(q, (x^n)+1) – rozšírený euklidov algoritmus, vracia vektor 3 prvkov, v tomto experimente slúži na zistenie inverzného polynómu, ak je prvý prvok 1, q je vstupný polynóm, tak druhý prvok bude inverzným polynómom k polynómu q.

vector(v.list()) -slúži na prevod polynómu na vektor

3.6.4 Vyhodnotenie výsledkov

V grafoch 5, 6, 7, 8, 9, 10 skúmame odhad pravdepodobnostného rozdelenia náhodnej premennej $X_{3,k}$, ktorá nám znázorňuje jednotlivé Hammingové váhy vektorov v_3^{-1}. Vektory v_3^{-1} reprezentujú prvé riadky cyklických matíc C_3^{-1}. Os x predstavuje Hamingovú váhu vektorov v_3^{-1} a os y predstavuje pravdepodobnosť vygenerovania vektorov v_3^{-1} s danou Hammingovou váhou.

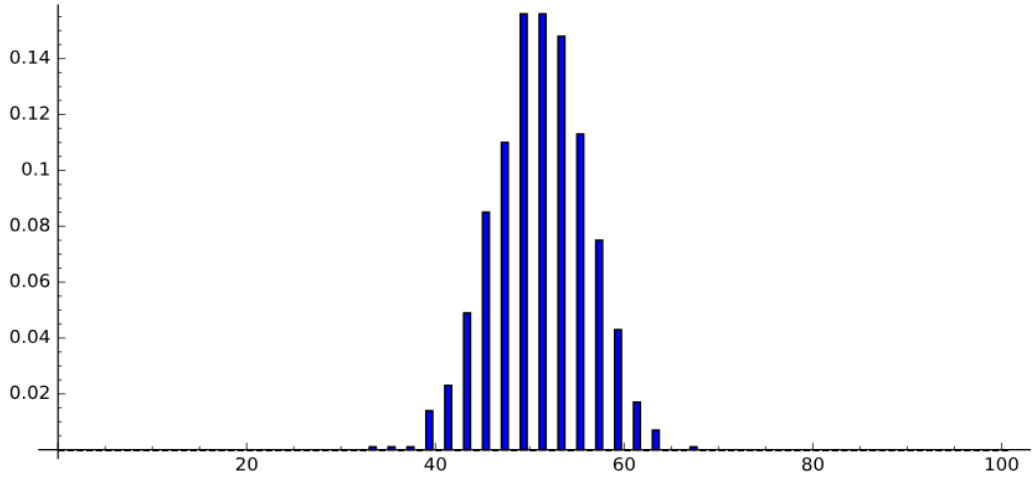
- Počet opakovaní: 1000krát
- k = 3



Graf 5

$E(X_{3,3})=52,26$	$D(X_{3,3})=21,46$	$S(X_{3,3})=4,63$

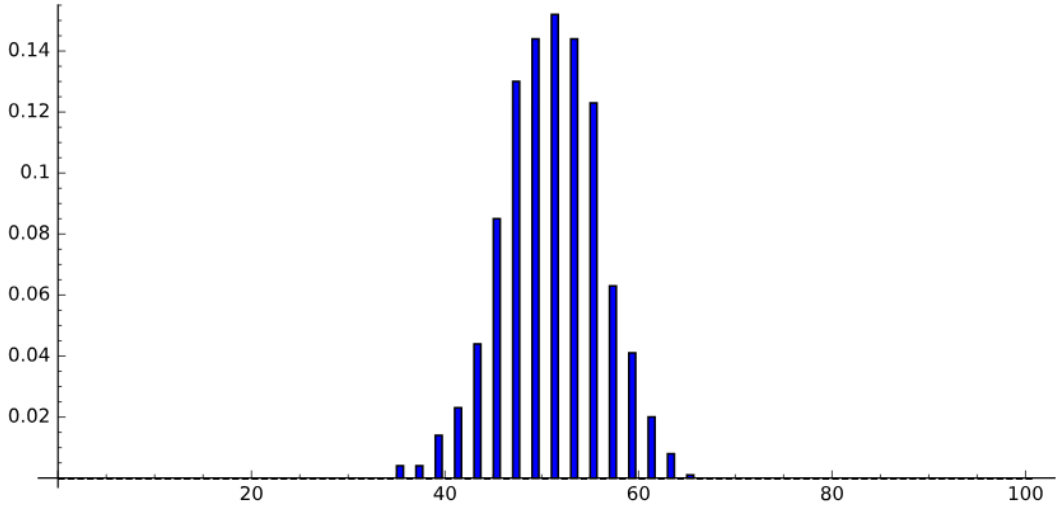
- Počet opakovaní: 1000krát
- k=5



Graf 6

$E(X_{3,5})=50,712$	$D(X_{3,5})=24,40$	$S(X_{3,5})=4,94$

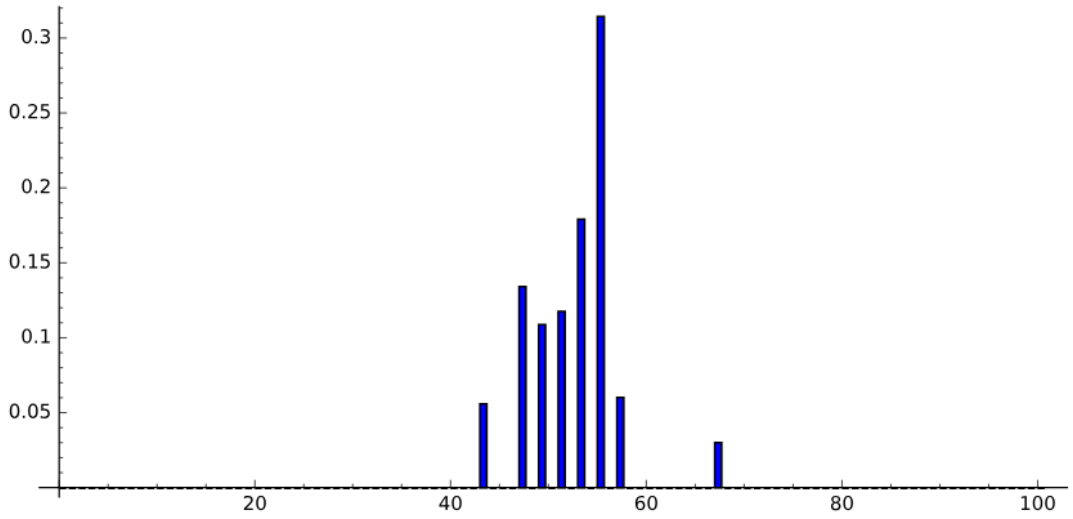
- Počet opakovaní: 1000krát
- k=7



Graf 7

$E(X_{3,7})=50,608$	$D(X_{3,7})=25,28$	$S(X_{3,7})=5,027$

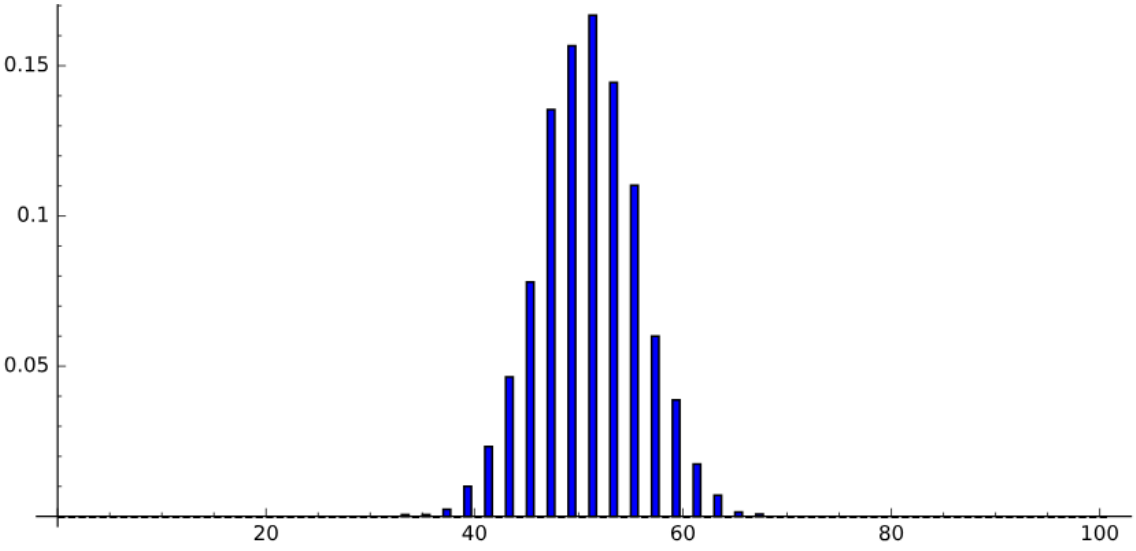
- Počet opakovaní: 5000krát
- k=3



Graf 8

$E(X_{3,3})=52,256$	**$D(X_{3,3})=20,17$**	**$S(X_{3,3})=4,49$**

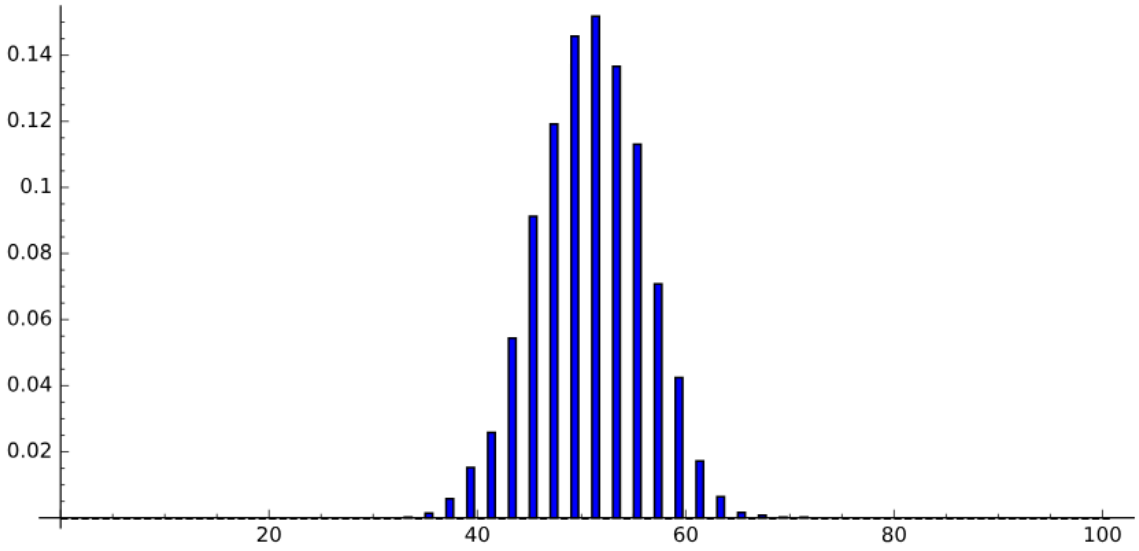
- Počet opakovaní: 5000krát
- k=5



Graf 9

$E(X_{3,5})=50,44$	**$D(X_{3,5})=25,31$**	**$S(X_{3,5})=5,03$**

- Počet opakovaní: 5000krát
- k=7



Graf 10

$E(X_{3,7})$=50,48	**$D(X_{3,7})$= 26,24**	**$S(X_{3,7})$=5,122**

Z porovnania odhadov pravdepodobnostných rozdelení náhodných premenných X_2 a $X_{3,k}$ pre 1000 opakovaní experimentu sme zistili, že pre k=3 má odhad pravdepodobnostného rozdelenia náhodnej premennej $X_{3,k}$ zvláštny tvar, ktorý nám nepripomína odhad pravdepodobnostného rozdelenia náhodnej premennej X_2. Odhad pravdepodobnostného rozdelenia premennej $X_{3,k}$ pre k = 3 nenadobúda všetky nepárne hodnoty Hammingových váh v intervale <43,67> ako je tomu pre odhad pravdepodobnostného rozdelenia premennej X_2 alebo pre nepárne Hammingové váhy k>3 odhadu pravdepodobnostného rozdelenia premennej $X_{3,k..}$ Odhad pravdepodobnostného rozdelenia premennej $X_{3,k}$ nenadobúda nepárne Hammingové váhy {43,59,61,63,65} v intervale <43,67> . Pravdepodobnosť vygenerovania inverznej cyklickej matice s Hammingovou váhou 55 je až 32%, čo je vysoká hodnota v porovnaní s ostatnými hodnotami. Správnosť týchto zistení potvrdzuje aj graf 8, kde bol zvýšený počet opakovaní experimentu na 5000 pre k=3 a dostali sme rovnaké výsledky. Pri porovnaní rozptylov platí, že pre k=3 je rozptyl podstatne menší ako pri ostatných grafoch experimentu číslo 3. Naopak, pre k=3 je väčšia je stredná hodnota ako pri ostatných grafoch experimentu číslo 3. Pre k=5 a k=7 môžeme pozorovať, že sa odhad pravdepodobnostného rozdelenia náhodnej

premennej $X_{3,k}$ podobá na odhad pravdepodobnostného rozdelenia náhodnej premennej X_2 a takisto nám tento výsledok potvrdil a väčší počet opakovaní.

3.7 Experiment č. 4

3.7.1 Cieľ experimentu

Nech H_0 je rovnomerne náhodne generovaná matica z priestoru všetkých binárnych cyklických matíc rozmeru n x n s pevnou Hammingovou váhou k. Nech H_1 je rovnomerne náhodne generovaná matica z priestoru všetkých binárnych cyklických matíc rozmeru n x n s pevnou Hammingovou váhou k. Matice H_0 a H_1 majú rovnakú Hammingovú váhu ale nie sú rovnaké. Nech H_1^{-1} je inverzná cyklická matica k matici H_1. Náhodná premenná $X_{4,k}$ predstavuje Hammingovú váhu prvého riadku matice (H_1^{-1} x H_0). Matica (H_1^{-1} x H_0) reprezentuje blok generujúcej matice lineárneho kódu. Cieľom experimentu je odhadnúť pravdepodobnostné rozdelenie náhodnej premennej $X_{4,k}$.

3.7.2 Popis experimentu

Nech k je pevná Hammingová váha a n dĺžka vektorov, ktoré sa majú vygenerovať. Vektor a_2 je vektor samých jednotiek dĺžky k nad poľom Z_2. Vektor b_2 je vektor samých núl veľkosti n-k nad poľom Z_2. Vektory a_2 a b_2 spojíme do jedného vektora, ktorý následne pomocou funkcie numpy.random.shuffle() náhodne permutujeme a dostaneme rovnomerne náhodne vygenerovaný vektor v_4 dĺžky n s pevnou Hammingovou váhou k nad poľom Z_2. Tie isté vektory a_2 a b_2 znova spojíme do jedného vektora, ktorý následne pomocou funkcie numpy.random.shuffle() náhodne permutujeme a dostaneme rovnomerne náhodne vygenerovaný vektor u dĺžky n s pevnou Hammingovou váhou k nad poľom Z_2. Vektor v_4 reprezentuje prvý riadok cyklickej matice H_0 a vektor u reprezentuje prvý riadok cyklickej matice H_1. Nech q_2 je polynóm, ktorý nám reprezentuje náhodný vektor u. Nech o je polynóm, ktorý nám reprezentuje náhodný vektor v_4. Vektory u a v4 prevedieme na polynómy q_2 a o, takým spôsobom, že indexy jednotiek náhodného vektora budú predstavovať exponenty jednotlivých členov polynómu. Pomocou funkcie na rozšírený

euklidov algoritmus vieme zistiť inverzný polynóm q_2^{-1}. Funkcia nám vráti vektor r_2 s tromi prvkami. Ak sa na prvej pozícií vektora r_2 nachádza číslo 1, tak na druhej pozícií vektora r_2 bude inverzný polynóm q_2^{-1} . Inverzný polynóm q_2^{-1} si následne prevedieme napäť na vektor, ktorý nám bude reprezentovať prvý riadok inverznej cyklickej matice H_1^{-1}. Vytvoríme polynóm z, ktorý je výsledkom súčinu polynómov q_2^{-1} a o. Polynóm z si následne prevedieme napäť na vektor h, ktorý nám bude reprezentovať prvý riadok cyklickej matice (H_1^{-1} x H_0). Experiment zopakujeme 1000krát pre k=3, k=5, k=7 a aj 5000krát pre k=3, k=5 k=7. V grafoch skúmame odhad pravdepodobnostného rozdelenia náhodnej premennej $X_{4,k}$, ktorá nám znázorňuje jednotlivé Hammingové váhy vektorov h. Výsledky zobrazíme v 6 grafoch zvlášť pre k=3, k=5, k=7,1000 opakovaní a pre k=3, k=5, k=7,5000 opakovaní experimentu.

3.7.3 Dôležité Sage funkcie použité v experimente

vector(GF(2), []) -inicializácia prázdneho vektora nad poľom Z_2

hamming_weight() – vráti HW vektora

R.<x> = PolynomialRing(GF(2)) – inicializácia okruhu polynómov nad poľom Z_2

R(list(v)) R(list(u)) – prevedie vektor na polynóm

numpy.random.shuffle(v) numpy.random.shuffle(u) – urobí premutáciu prvkov vektora v aj u

xgcd(q, (x^n)+1) – rozšírený euklidov algoritmus, vracia vektor 3 prvkov, v tomto experimente slúži na zistenie inverzného polynómu, ak je prvý prvok 1, a je vstupný polynóm, tak druhý prvok bude inverzným polynómom k polynómu q.

vector(v.list()) vector(u.list()) -slúži na prevod polynómu na vektor

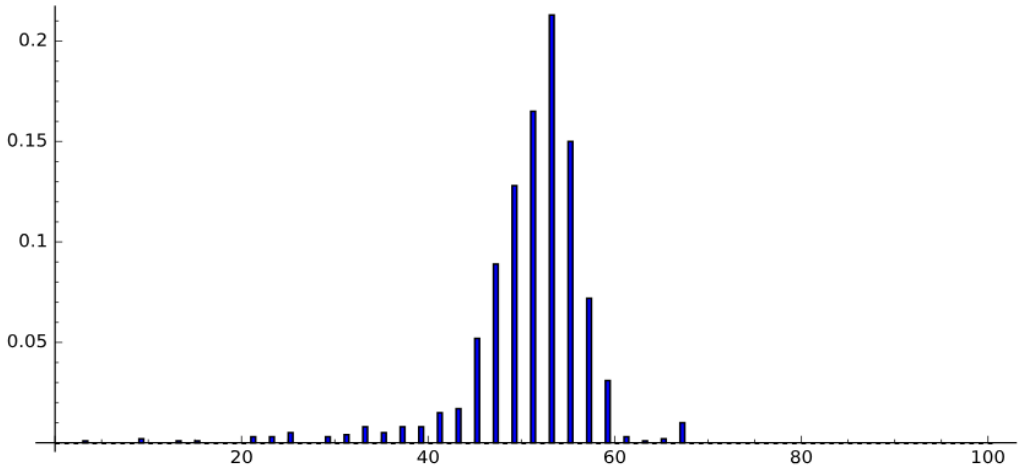
quotient() - zabezpečí aby exponenty neprekročili zvolenú dĺžku n

3.7.4 Vyhodnotenie výsledkov

V grafoch 11, 12, 13, 14, 15, 16 skúmame odhad pravdepodobnostného rozdelenia náhodnej premennej $X_{4,k}$, ktorá nám znázorňuje jednotlivé Hammingové váhy vektorov h. Vektory h reprezentujú prvé riadky cyklických matíc (H_1^{-1} x H_0). Os x predstavuje

Hamingovú váhu vektorov h a os y predstavuje pravdepodobnosť vygenerovania vektorov h s danou Hammingovou váhou.

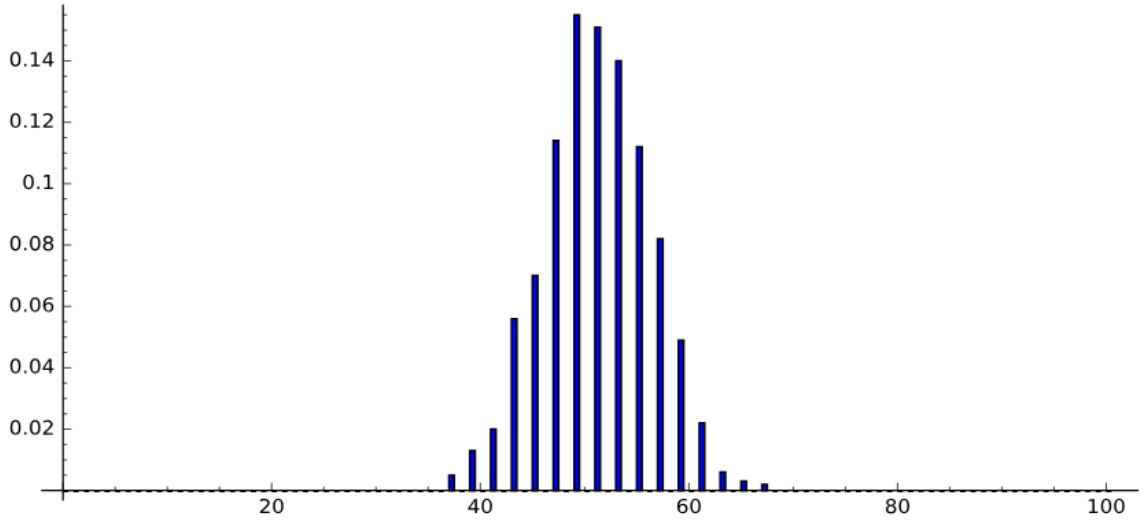
- Počet opakovaní: 1000krát
- k=3



Graf 11

$E(X_{4,3}) = 50,64$	**$D(X_{4,3}) = 44,14$**	**$S(X_{4,3})=6,64$**

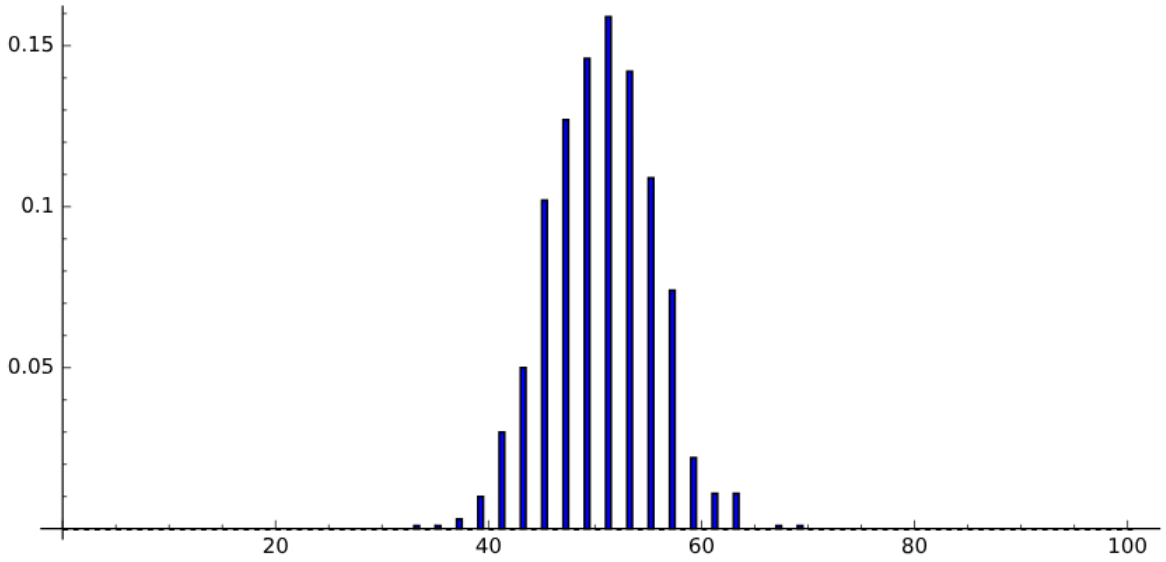
- Počet opakovaní: 1000krát
- k=5



Graf 12

$E(X_{4,5}) = 50,92$	$D(X_{4,5}) = 26$	$S(X_{4,5})=5,1$

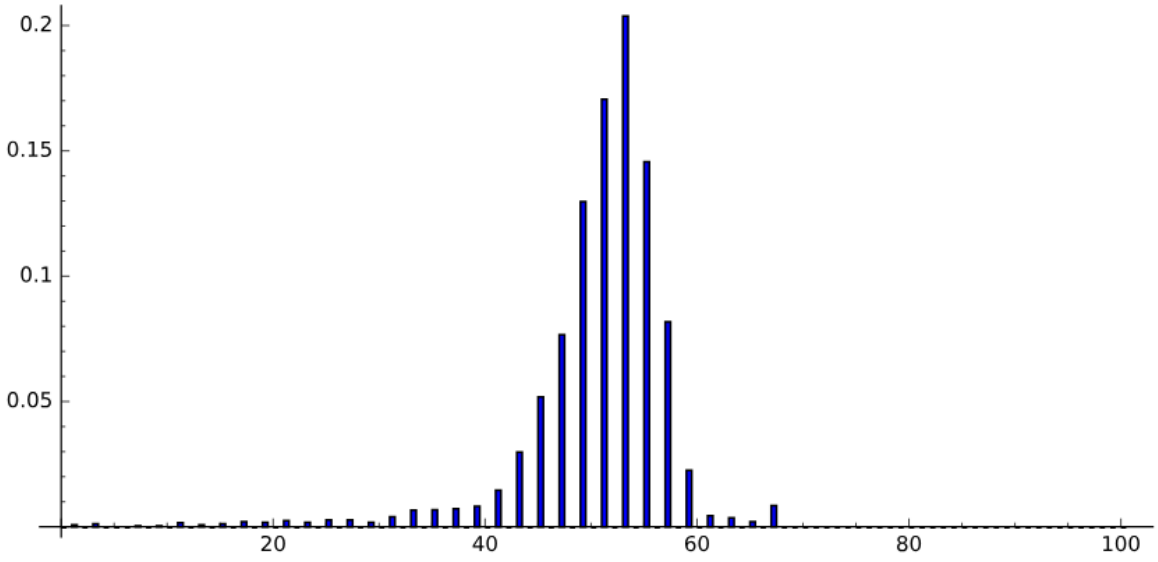
- Počet opakovaní: 1000krát
- k=7



Graf 13

$E(X_{4,7}) = 50,31$	$D(X_{4,7}) = 24,27$	$S(X_{4,7})=4,93$

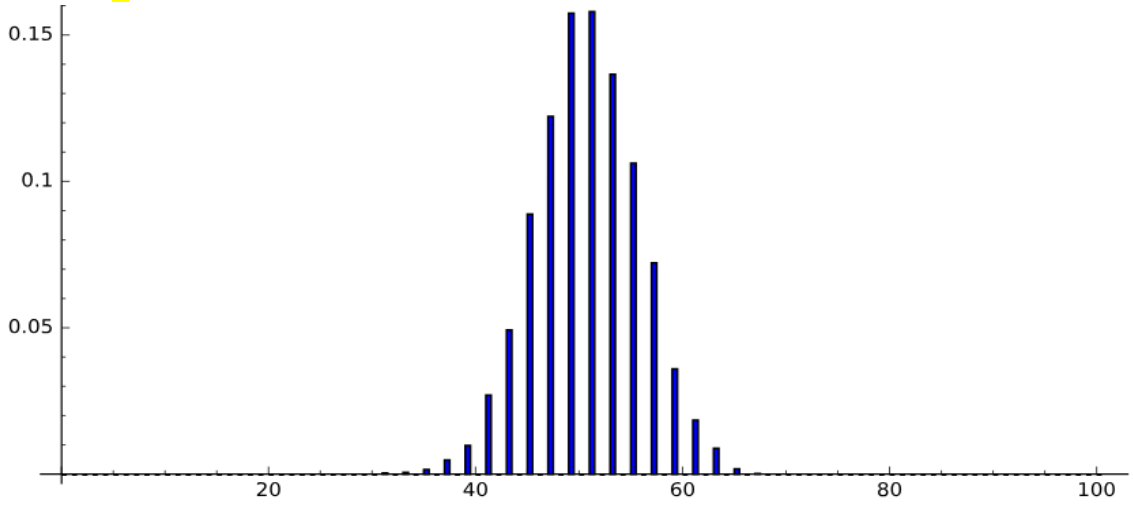
- Počet opakovaní: 5000krát
- k=3



Graf 14

$E(X_{4,3}) = 50,45$	$D(X_{4,3}) = 49,39$	$S(X_{4,3})=7,027$

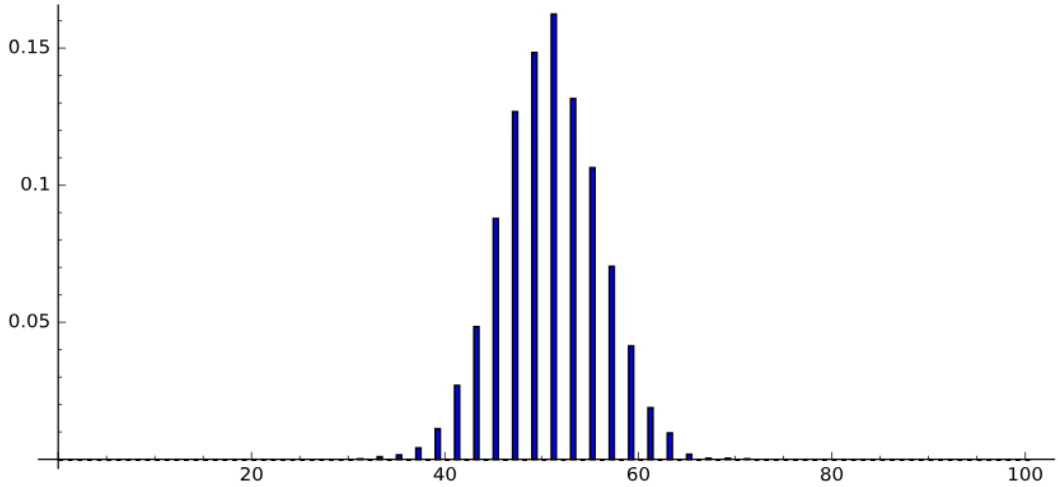
- Počet opakovaní: 5000krát
- k=5



Graf 15

$E(X_{4,5}) = 50,51$	$D(X_{4,5}) = 25,16$	$S(X_{4,5})=5,016$

- Počet opakovaní: 5000krát
- k=7



Graf 16

$E(X_{4,7}) = 50,38$	$D(X_{4,7}) = 25,59$	$S(X_{4,7})=5,059$

Z porovnania odhadov pravdepodobnostných rozdelení náhodnej premennej $X_{4,k}$ a X_2 pre 1000 opakovaní experimentu sme zistili, že pre k=3 má odhad pravdepodobnostného rozdelenia náhodnej premennej $X_{4,k}$ opäť zvláštny tvar, ktorý nám nepripomína odhad pravdepodobnostného rozdelenia náhodnej premennej X_2.

Na rozdiel od odhadu pravdepodobnostného rozdelenia premennej X_2 vidíme častejší výskyt matíc s Hammingovou váhou < 40%. Pravdepodobnosť vygenerovania cyklickej matice s Hammingovou váhou 55 je až 22%, čo je vyššia hodnota v porovnaní s ostatnými hodnotami odhadov pravdepodobnostných rozdelení náhodných premenných $X_{4,k}$ pre k>3 a X_2 (pre 1000 opakovaní).

Pri porovnaní rozptylov pre k=3 a 1000 opakovaní je rozptyl podstatne väčší ako pri všetkých ostatných grafoch experimentu č.4 aj v porovnaní s odhadom pravdepodobnostného rozdelenia náhodnej premennej X_2. Pre k=5 a k=7 môžeme pozorovať, že sa odhad pravdepodobnostného rozdelenia náhodnej premennej $X_{4,k}$ podstatne viac podobá na odhad pravdepodobnostného rozdelenia náhodnej premennej X_2.

Pre overenie správnosti výsledkov sme experiment zopakovali 5000krát pre k=3, k=5 a k=7 aby sme potvrdili naše zistenia pre 1000 opakovaní experimentu. Vo všetkých prípadoch môžeme pozorovať, že sa výsledky pre odhad pravdepodobnostného rozdelenia náhodnej premennej $X_{4,k}$ potvrdili.

3.8 Zhrnutie štatistických výsledkov

Všetky štatistické výsledky sú zobrazené v nasledujúcej tabuľke

Názov grafu	**Experiment**	**Počet opakovaní**	**Pevná HW** (pri generovaní n. vektora) **(k)**	**Stredná hodnota**	**Rozptyl**	**Smer. odchýlka**
Graf 1	Experiment č.1	1000	-	50,89	22,81	4,78
Graf 2	Experiment č.1	5000	-	50,44	24,15	4,91
Graf 3	Experiment č.2	1000	-	50,95	22,89	4,78
Graf 4	Experiment č.2	5000	-	50,34	24,46	4,95
Graf 5	Experiment č.3	1000	3	52,26	21,46	4,63
Graf 6	Experiment č.3	1000	5	50,712	24,40	4,94
Graf 7	Experiment č.3	1000	7	50,61	25,28	5,03
Graf 8	Experiment č.3	5000	3	52,26	20,17	4,49
Graf 9	Experiment č.3	5000	5	50,44	25,31	5,03
Graf 10	Experiment č.3	5000	7	50,48	26,24	5,12
Graf 11	Experiment č.4	1000	3	50,64	44,14	6,64
Graf 12	Experiment č.4	1000	5	50,92	26	5,1
Graf 13	Experiment č.4	1000	7	50,31	24,27	4,93
Graf 14	Experiment č.4	5000	3	50,45	49,39	7,03
Graf 15	Experiment č.4	5000	5	50,51	25,16	5,02
Graf 16	Experiment č.4	5000	7	50,38	25,59	5,06

Tabuľka č.1 Štatistické výsledky

Záver

V našej práci sme skúmali cyklické matice, ktoré vystupujú v QC MDPC McElieceovom kryptosystéme. Cieľom našej práce bolo skúmať hustotu inverzných matíc k riedkym cyklickým maticiam. Pozorovania sme uskutočnili v 4 experimentoch. Výsledky experimentov sme zobrazili v jednotlivých grafoch. V grafoch sme skúmali odhad pravdepodobnostného rozdelenia náhodných premenných, pre ktoré sme zisťovali aj strednú hodnotu, rozptyl a smerodajnú odchýlku. Pre všetky experimenty sme si zvolili dĺžku jednotlivých vektorov, ktoré nám budú reprezentovať cyklické matice n = 101. Nepárne Hammingové váhy niektorých náhodných vektorov sme zvolili k=3, k=5 a k= 7.

V experimente č.1 sme skúmali odhad pravdepodobnostného rozdelenia náhodnej premennej X_1, ktorá nám znázorňovala jednotlivé Hammingové váhy náhodne generovaných vektorov v_1, pričom vektory v_1 reprezentovali prvé riadky cyklických matíc C_1. Experiment sme opakovali 1000 a 5000 krát. Grafy experimentu č.1 nám slúžili len ako referenčné grafy.

V experimente č.2 sme skúmali odhad pravdepodobnostného rozdelenia náhodnej premennej X_2, ktorá nám znázorňovala jednotlivé Hammingové váhy náhodne generovaných vektorov v_2. Vektory v_2 reprezentovali prvé riadky cyklických matíc C_2, ktoré boli invertovateľné. Experiment sme opakovali, kým sme nedostali 1000 a 5000 takýchto vektorov v_2. Grafy experimentu č.2 boli takisto referenčné grafy.

V experimente č.3 sme skúmali odhad pravdepodobnostného rozdelenia náhodnej premennej $X_{3,k}$, ktorá nám znázorňovala jednotlivé Hammingové váhy vektorov v_3^{-1}. k bola pevná nepárna Hammingová váha vektora v_3, ktorý reprezentuje prvý riadok cyklickej matice C_3. Vektory v_3^{-1} reprezentovali prvé riadky cyklických matíc C_3^{-1}. Experiment sme opakovali 1000krát pre k=3, k=5, k=7 a 5000krát pre k=3. Z porovnania experimentov č.2 a 3 pre 1000 opakovaní sme zistili, že pre k=3 mal odhad pravdepodobnostného rozdelenia náhodnej premennej $X_{3,k}$ neočakávaný zvláštny tvar. Odhad pravdepodobnostného rozdelenia premennej $X_{3,k}$ pre k = 3 nenadobúdal všetky nepárne hodnoty Hammingových váh v intervale <43,67>. Hodnoty ktoré premenná $X_{3,k}$ nenadobudla sú hammingové váhy {43,59,61,63,65} Pravdepodobnosť vygenerovania inverznej cyklickej matice s Hammingovou váhou 55 bola až 32% a $X_{3,k}$ mala menší rozptyl a väčšiu strednú hodnotu

v porovnaní s ostatnými grafmi experimentu č.3 pre 1000 opakovaní. Správnosť našich zistení nám potvrdil vyšší počet opakovaní experimentu.

V experimente č.4 sme skúmali odhad pravdepodobnostného rozdelenia náhodnej premennej $X_{4,k}$, ktorá nám znázorňovala jednotlivé Hammingové váhy vektorov h. k bola pevná Hammingová váha prvého riadku matíc H_0 a H_1. Vektory h reprezentovali prvé riadky cyklických matíc (H_1^{-1} x H_0). Matica (H_1^{-1} x H_0) nám predstavovala blok generujúcej matice. Experiment sme zopakovali 1000krát pre k=3, k=5, k=7 a 5000krát pre k=3, k=7. Z porovnania experimentu č.4 a experimentu č.2 pre 1000 opakovaní experimentu sme zistili, že pre k=3 mal odhad pravdepodobnostného rozdelenia náhodnej premennej $X_{4,k}$ opäť neočakávaný zvláštny tvar. Na rozdiel od odhadu pravdepodobnostného rozdelenia premennej X_2 sme videli častejší výskyt matíc s Hammingovou váhou < 40%. Odhad pravdepodobnostného rozdelenia premennej $X_{4,k}$ Rozptyl pre k=3 bol podstatne väčší ako pri všetkých ostatných grafoch aj v porovnaní s odhadom pravdepodobnostného rozdelenia náhodnej premennej X_2. Experiment sme zopakovali 5000krát, pre k=3 a k=7. Výsledky a zistenia sme väčším počtom opakovaní experimentu potvrdili.

Matica (H_1^{-1} x H_0), ktorá predstavuje blok generujúcej matice, mala v niektorých prípadoch nízku hustotu a mohla by znamenať bezpečnostné riziko pre QC-MDPC. Vlastnosti blokov (H_1^{-1} x H_0) generujúcich matíc by bolo zaujímavé ďalej skúmať, či umožnia útoky na QC MDPC McElieceov kryptosystém.

Zoznam použitej literatúry

1. **Anton, Howard, Bivens, Irl C. a Davis, Stephen (2012),** *Calculus Single Variable*, John Wiley & Sons, p. 31, ISBN 9780470647707.

2. **Eric Weisstein,** *Wolfram Math World*, http://mathworld.wolfram.com/

3. **Fabšič, Tomáš,** *Contributions to the analysis of the QC-LDPC McEliece Cryptosystem.* Dizertačná práca, Slovak University of technology in Bratislava Faculty of electrical engineering and information technology, 2017.

4. **Huffman, W., & Pless, V. (2003),** *Fundamentals of Error-Correcting Codes*. Cambridge: Cambridge University Press. doi:10.1017/CBO9780511807077.

5. **R. Misoczki, J. P. Tillich, N. Sendrier and P. S. L. M. Barreto,** "*MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes,"* 2013 IEEE International Symposium on Information Theory, Istanbul, 2013, pp. 2069-2073.

6. **Rudolf Lidl, Harald Niederreiter,** *Introduction to finite fields and their applications.* New York : Cambridge University Press, 1986. ISBN 0-521-30706-6.

7. **Davis, Philip J.,** *Circulant Matrices,* Wiley, New York, 1970 ISBN 0471057711.

8. **Tomáš Fabšič, Otokar Grošek, Karol Nemoga & Pavol Zajac.** *On generating invertible circulant binary matrices with a preescribed number of ones,* Cryptography and Communications Discrete Structures, Boolen Functions and Sequences. Springer US, 2017. ISSN 1936-2447.

9. *Cocalc* https://cocalc.com

10. *Sage documentation* http://doc.sagemath.org/

Prílohy

Príloha A: Štruktúra elektronického nosiča

K projektu je priložený elektronický nosič CD, so spustiteľným programom, potrebnými súbormi, ako aj s dokumentáciou.

Štruktúra elektronického CD nosiča je nasledovná:

- \Dokumentácia - dokumentácia k bakalárskej práci
- \Zdrojové kódy - každý experiment je samostatne vypracovaný v kóde, parametre, ktoré je potrebné meniť sú popísané v komentári zdrojových kódov
- \Zdrojové kódy\záloha - záložné textové súbory obsahujúce zdrojové kódy